Global Investigations Review

The Guide to Cyber Investigations

Editors
Benjamin A Powell and Jason C Chipman

Second Edition

The Guide to Cyber Investigations

Editors:

Benjamin A Powell

Jason C Chipman

Reproduced with permission from Law Business Research Ltd
This article was first published in June 2021
For further information please contact Natalie.Clarke@lbresearch.com

GIR
Global Investigations Review

Published in the United Kingdom
by Law Business Research Ltd, London
Meridian House, 34-35 Farringdon Street, London, EC4A 4HL, UK

www.globalinvestigationsreview.com

ISBN 978-1-83862-595-5

Printed in Great Britain by
Encompass Print Solutions, Derbyshire
Tel: 0844 2480 112

Acknowledgements

The publisher acknowledges and thanks the following for their assistance throughout the preparation of this book:

ANDERSON MORI & TOMOTSUNE

BAKER MCKENZIE

BCL SOLICITORS LLP

CLIFFORD CHANCE US LLP

COVINGTON & BURLING LLP

CRAVATH, SWAINE & MOORE LLP

RICHARD DENATALE

HUGHES HUBBARD & REED

K&L GATES LLP

KROLL, A DIVISION OF DUFF & PHELPS

BRIAN MCDONALD

QUINN EMANUEL URQUHART & SULLIVAN, LLP

ROPES & GRAY LLP

WILMER CUTLER PICKERING HALE AND DORR LLP

Publisher's Note

The Guide to Cyber Investigations is published by Global Investigations Review – the online home for all those who specialise in investigating and resolving suspected corporate wrongdoing.

It aims to fill a gap in the literature and provide an in-depth guide to every aspect of preparing for and dealing with data breaches and other cyber incidents. These incidents can be challenging, to say the least.

As such it is a companion to GIR's larger reference work, *The Practitioner's Guide to Global Investigations* (now in its fifth edition), which walks readers through the issues raised, and the risks to consider, at every stage in the life cycle of a corporate investigation, from discovery to resolution.

The Guide to Cyber Investigations takes the same holistic approach, going through everything to think about before, during and after an incident. We suggest both books be part of your library – *The Practitioner's Guide* for the whole picture and *The Guide to Cyber Investigations* as the close-up.

The Guide to Cyber Investigations is supplied to all GIR subscribers as a benefit of their subscription. It is also available to non-subscribers in online form only, at www.globalinvestigationsreview.com.

The publisher would like to thank the editors for their energy and vision. We collectively welcome any comments or suggestions on how to improve it. Please write to us at insight@globalinvestigationsreview.com.

Contents

Introduction: Preventing, Mitigating and Responding to Data Breaches

Benjamin A Powell[1]

Today, it is almost impossible to open a newspaper without seeing an article about another data breach. Attackers of various motivations – from nation states and criminals to terrorists and hactivists – have targeted and successfully breached government entities, private individuals and companies in all sectors of the economy and around the globe. As then-FBI Director Robert Mueller observed in 2012: '[T]here are only two types of companies: those that have been hacked and those that will be. And even they are converging into one category: companies that have been hacked and will be hacked again.'

In recent years, this has become even more apparent. According to Kroll's 2019/2020 Global Fraud and Risk Report, nearly every industry ranked cyberthreats and data leaks as a top security risk facing their economic sector.[2] And, underscoring the evolving nature of attacks facing business, according to FireEye Mandiant's M-Trends 2021 report, ransomware groups have evolved to pursue multifaceted extortion schemes that accounted for a large percentage of cyber intrusion activity in 2020.[3]

As data breaches and ransomware events increase in frequency, boards of directors, management, employees, customers and regulators across the globe are increasing their expectations for companies to take information security and breach preparedness seriously. Preventing, preparing for and (inevitably) responding to breaches is no longer seen as an IT issue, but rather as a significant risk area that cuts across areas including legal and compliance, human resources, audit, vendor management, insurance and communications.

In the wake of a data breach, companies may need to conduct internal investigations; engage external specialists, including law firms, forensic investigators and public relations

1 Benjamin A Powell is a partner at Wilmer Cutler Pickering Hale and Dorr LLP.

2 Kroll, 'Global Fraud & Risk Report: 10th Annual Edition – 2019/2020, www.kroll.com/en/insights/publications/global-fraud-and-risk-report-2019.

3 FireEye Mandiant Services, Special Report, 'M-Trends 2021, https://content.fireeye.com/m-trends/rpt-m-trends-2021.

experts; implement crisis management plans; assess breach notification requirements, regulatory obligations (such as data protection authority and securities disclosure requirements), contractual issues, litigation exposure and compliance improvement efforts; and respond to requests, enquiries and actual or threatened enforcement or litigation from customers, government agencies, payment card brands, insurance companies, auditors and the media.

Understanding and preparing for each of these workstreams is fundamental to a successful cybersecurity investigation and incident response. To that end, this book – with chapters addressing key topics authored by leading authorities and informed by their broad experience in handling data incidents – is intended to provide companies and counsel with an overview of the key cyberthreats and legal, strategic, tactical and reputational considerations and risks that companies may need to assess in preparing for and responding to a data security incident, including how these considerations vary in certain jurisdictions around the world.

Fundamentally, as regulators and industry groups across the globe have recognised, effectively managing any company's exposure to cybersecurity threats and liabilities requires taking a risk-based approach.[4]

As such, the guidance in this book is not intended to be one-size-fits-all. For example, as recognised throughout the book, regulatory obligations and risk mitigation strategies may vary based on sector, geographical location and the nature of a company's critical data assets. Therefore, to successfully prevent, mitigate and respond to a data breach, each company should assess and understand its risk profile; develop a system of overlapping data security controls and risk mitigation strategies tailored to its threat profile and critical assets; and prepare an incident response plan that is appropriate for the company's size, organisational structure, culture and risks.

Assessing risk

To properly prevent and prepare for breaches and to otherwise assess and mitigate cyber risk, a company first needs to understand the nature of its cyber risk. This means not only understanding the organisation's threat profile (from both external and internal threats) but also having a firm grasp on what the critical data is and where it is stored. Armed with these key pieces of information, an organisation can allocate IT resources and personnel, tailor

4 See, e.g., Appendix B to 12 CFR Part 30, Section III.C (requiring national banks and federal savings associations in the United Sates to design information security schemes to 'control the identified risks, commensurate with the sensitivity of the information as well as the complexity and scope' of the entity's activities); 45 CFR Section 164.306 (requiring 'covered entities' and 'business associates' under the Health Insurance Portability and Accountability Act, as amended, to utilise security measures to protect electronic protected health information, based upon, in part, '[t]he probability and criticality of potential risks to electronic protected health information'); Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Section 2, Art. 32 ('Taking into account the . . . risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk . . .'); Group of 7 Cyber (G7) Cyber Experts Group, 'G7 Fundamental Elements of Cybersecurity for the Financial Sector', https://www.ecb.europa.eu/paym/pol/shared/pdf/G7_Fundamental_Elements_Oct_2016.pdf (noting that financial institutions should '[e]stablish and maintain a cybersecurity strategy and framework tailored to specific cyber risks . . .').

security controls and make informed strategic decisions to balance risk minimisation with operational needs.

Chapter 1 of this book, for example, provides an overview of the different types of threats and threat actors, ranging from nation-state actors to cybercriminals and company insiders. While the types of controls a company may need to implement may not vary, for example, as between nation state-associated actors and cybercriminals, it will be important for companies to understand the types of risks they face from both internal and external actors and their most vulnerable attack vectors so that they can control for each of these risk areas. Understanding when, for example, certain company actions might increase the likelihood of a nation-state actor being driven to attack may drive the company to enhance monitoring for a time around that activity.

In addition to understanding a company's threat profile, it is perhaps even more critical for a company to identify its key data assets, often referred to as its 'crown jewels', and knowing where those data assets reside. As the US Federal Trade Commission (FTC) advised in its 2016 Protecting Personal Information: A Guide for Business, 'effective data security starts with assessing what information you have[,] identifying who has access to it . . . [and] how [it] moves into, through, and out of your business', because this information is 'essential to assessing security vulnerabilities'.[5] Crown jewels can include commercial proprietary information, intellectual property or trade secrets (belonging to the company or its enterprise customers); sensitive personal, health or financial information (belonging to the company's employees or customers); classified or other controlled information (e.g., export-controlled information); or other internal documents (e.g., email files). 'Tak[ing] stock' of how a business maintains sensitive information, as the FTC suggests, includes understanding who sends sensitive information to the business, how the business receives that information, what kind of information is collected at each entry point, and where the information collected at each entry point is kept.[6]

Understanding a company's threat profile and identifying its critical data assets often go hand in hand. For example, if a company processes payment card data as a core component of its business, cyber criminals may be one of its biggest cyberthreats. Or, if a company is a government contractor, it may be targeted by nation states seeking government information. But sometimes the picture is less clear. For example, a hospital's most valuable data to an external party may be health insurance information, social security numbers and other information that enables identity theft. But ensuring the availability, integrity and security of other data or systems – such as patient allergy information or the continued functionality of life-saving medical devices – may be just as critical.

While described in the context of cyber due diligence, the guidance provided in Chapter 7 for preparing for a diligence and scoping of potential risk areas can be helpful for a company conducting its own internal risk assessment as well.

5 US Federal Trade Commission [FTC], 'Protecting Personal Information: A Guide for Business' 2, October 2016, www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf. While this and other FTC data security guidance is directed at the protection of US consumer personal information – in view of the FTC's jurisdictional authority (see Chapter 11) – its guidance is nonetheless helpful in identifying foundational security practices for the protection of sensitive information more broadly.

6 id., at 3 to 5.

Protecting assets

Once a company identifies the nature and location of its most sensitive assets, it should then design and implement a system of controls appropriate to protecting those assets. For example, in June 2015, the FTC issued a guidance document as part of its Start with Security initiative, which focused on encouraging small and medium-sized businesses to embrace 'security-by-design' principles. In the guidance document, Start with Security: A Guide for Business,[7] the FTC drew what it considered to be lessons learned from its 54 data security enforcement actions.[8]

Based on a review of these cases, the FTC advised companies to incorporate a series of 10 lessons learned:

- develop an appropriate, proactive cybersecurity plan;
- control access to data sensibly;
- require secure passwords and authentication;
- store sensitive information securely and protect it during transmission, including through the use of strong cryptography for data in transit and at rest;
- segment networks and monitor egress and ingress through tools such as firewalls and intrusion detection and prevention tools;
- secure remote access to networks;
- apply sound security practices (e.g., secure coding, security testing and vulnerability assessments) when developing new products;
- keep a watchful eye on service providers (e.g., diligence, contractual requirements and performance oversight) to ensure they implement reasonable security measures;
- keep security current and address any vulnerabilities; and
- secure paper, physical media and devices.[9]

Many of these recommendations may sound obvious. However, time and again, failings in fundamental security practices, similar to many of those identified by the FTC, often are the apparent cause or a substantial contributing factor to a significant breach.

Forensics, security and consulting firms agree. In its 2018 X-Force Threat Intelligence Index annual report, IBM said that human error, such as misconfigured cloud servers, unsecured cloud databases and improperly secured backups, were responsible for 43 per cent of publicly disclosed misconfiguration incidents in 2018, up from only 17 per cent in 2017.[10] Meanwhile, Verizon's 2018 annual 'Payment Security Report' found a decrease in

7 FTC, 'Start with Security: A Guide for Business', June 2015, www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

8 As at the end of 2018, the FTC has brought 65 cases against companies based on allegations of unfair or deceptive practices involving inadequate protection of consumers' personal data. FTC, 'Privacy & Data Security: Update 2018', www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2018/2018-privacy-data-security-report-508.pdf.

9 In 2017, the FTC published a series of blog posts titled 'Stick with Security' as a 'deeper dive' follow-up to the Start with Security guidance. The blog series includes a separate in-depth blog post on each of the 10 'lessons learned'. FTC, 'Stick with Security: A Business Blog Series' (2017), www.ftc.gov/tips-advice/business-center/guidance/stick-security-business-blog-series.

10 IBM Security, 'X-Force Threat Intelligence Index' (2019), https://xforceintelligenceindex.mybluemix.net/?cm_mc_uid=22606977992415547523155&cm_mc_sid_50200000=30533621554752315552&cm_mc_sid_5264

the percentage of companies fully compliant with the Payment Card Industry Data Security Standards (PCI-DSS) during interim assessments – the first time Verizon has seen a decrease in the percentage of compliant companies since 2012.[11] Verizon further noted that 'no organization affected by payment card data breaches was found to be in full compliance with the PCI[-]DSS during a subsequent Verizon PCI forensic investigator . . . inquiry'.[12]

Prepare, plan, practise and manage a coordinated response

Once a company is armed with an understanding of its risk profile and crown jewels, and has endeavoured to implement controls (appropriate in light of the risks) to prevent, detect and quickly mitigate an attack, the company should be in a position that successful, significant attacks on its data assets are unlikely. Nevertheless, companies cannot and should not rest on their laurels, or be comforted by the strength of their security scheme alone. New vulnerabilities and attack methods are being identified and exploited daily. A common maxim in the security community is that the attackers only have to 'get it right' once – find one vulnerability on one system to exploit – while security personnel need to 'get it right' every time to definitively prevent a breach from occurring. Another maxim is that the most secure system is the least usable – one that is locked in an impenetrable safe and disconnected from the internet.

Because neither perfection nor total non-usability are desirable or appropriate, companies should ensure that they are prepared to respond to an incident if necessary. Companies can use this book to help them in those efforts and to guide their response efforts should they ever face a significant security incident. Whether it be identifying the internal team and external resources who should be at the table during an incident response, planning a realistic table-top exercise that will reasonably cover the types of issues a company may face in an incident response, identifying relevant regulators and law enforcement with whom companies should establish relationships before an incident occurs, planning for various workstreams, or assessing options for insurance cover, this book is intended to provide a legal framework, supplemented by practical and tactical guidance, to support these efforts.

0000=63000101554752315557.

11 Verizon, '2018 Payment Security Report', https://enterprise.verizon.com/resources/reports/2018_payment_security_report_en_xg.pdf.

12 ibid.

Part I

A 'Typical' Cyber Investigation

1

The Cyberthreat Landscape

Jason Smolanoff, Alan Brill and Andrew Beckett[1]

Introduction

Hackers, cybercriminals, ransomware, cyberterrorism, state-sponsored cyberespionage, hacktivism: we hear these terms constantly. Cyber incidents have become newsworthy because virtually everyone's personal data has been compromised in one or more of the thousands of incidents that have occurred over the years, only some of which have been made public.

Every system that uses digital technologies – whether it involves centralised servers with immense processing power and storage capabilities or information we store and transact on our smartphones – has vulnerabilities associated with it. Some of these are well known and understood; others are constantly emerging. The reality is that a system that was considered secure yesterday may be insecure this morning because a new, previously unknown hardware or software issue (called a zero-day vulnerability) has been identified.

Systems are compromised by attackers for many reasons. A disgruntled current or former employee with a grudge wipes out a key file or program. A nation-state actor compromises a company's competitive bidding system and provides its forthcoming bid to a competitor in its country. A hacker compromises huge numbers of payment card accounts and offers them for sale on the dark web. A criminal tricks someone at a help desk into providing them with access codes. A misconfigured system allows an intruder to go from a portion of a system that monitors environmental conditions in one location to one that stores sensitive financial information. These all have happened and continue to happen.

In this chapter, we share our collective insight spanning the public and private sectors, different parts of the world, and diverse industry backgrounds and experience of more than 40 years investigating and responding to cyber incidents.

1 Jason Smolanoff and Alan Brill are senior managing directors and Andrew Beckett is a managing director at Kroll, a division of Duff & Phelps. The information in this chapter is accurate as at May 2019.

The questions we cover are: Who are the suspects? What kinds of threat-actors are out there targeting our systems? Is there some logic in how they select victims? In how they attack? Why are so many attacks successful?

Breaking down the problem

Cyber incident actors: who are they?

Who are the actors behind cyber incidents? While there is no universally accepted list, and while a perpetrator can be part of multiple groups (however those groups are defined), experience indicates that there is a broad taxonomy we can use to bring some ordered thinking to the question of who is carrying out attacks and why they select their particular targets.

Nation-state actors

Nation states have recognised that cyber is a domain of warfare that is inherently asymmetric; that is, a small number of talented people can have a huge effect. In the Ukraine, for example, Russian hacking was believed to be responsible for substantial power outages. A nation state can act directly or indirectly.

Direct actions of nation states

This is the case when a government is directing the actions of people carrying out an attack. Examples of agencies believed to have offensive cyber capabilities include the US National Security Agency, the Russian Main Intelligence Directorate (GRU), the People's Liberation Army of China, and governments as diverse as North Korea (Democratic People's Republic of Korea) and Israel. They have employed cyber operators who act for the nation state under the direction of their superiors.

Outsourced actions of nation states

A nation state may lack capacity in terms of qualified hackers but still want to carry out offensive cyber operations. In these cases they may decide to outsource the work and can consider a range of possible actors. They may contract with civilian criminal hacking groups with the requisite capabilities or work through an allied country that has the capabilities. They may also act through a non-government group. For example, it has been reported that during the 2016 US presidential campaign, Russian organisations hacked the Democratic National Committee, but used the Wikileaks organisation to release and distribute the stolen material.

Non-state or quasi-state actors

There is also a range of non-government organisations (NGOs) that may be behind offensive cyber activities.

Terrorist activities

Terrorist groups have become sophisticated users of cyber capabilities. They may use the internet for recruiting, financing, information theft or distribution. They may carry out operations to confuse their enemy, appearing to have greater or fewer numbers of personnel than they really do. Cyberterrorism has become a field of study in itself.

Information anarchists

We have seen the growth of organisations (some loosely organised) that believe no information should be secret, or at the very least, those they target should have no secrets. They may steal emails or other information and post it publicly. They may strike out in various ways, including distributed denial of services (DDoS) attacks designed to take a target website out of operation.

NGOs who share a common cause with state actors

Do not think that every attack can be attributed to one of the aforementioned types of operators. Just as threats can involve multiple risks, multiple actors can operate in concert (either formally or informally). They may share a target (but operate independently) or may coordinate their efforts; for example, a nation-state actor steals the data, but an NGO distributes it.

Organised cybercriminal organisations

Organised cybercriminal organisations can, aside from their own for-profit operations (e.g., stealing sensitive personal information, credit card data, health insurance data and the like), be the source of malware or they may provide malware as a service offering. They may also engage in other forms of attack (e.g., DDoS). They will provide their services to anyone who pays them. We are seeing an increase in the use of 'professional' malware in attacks. This makes it hard to determine attribution because, while the attack may have been seen before, it does not tell you who the attacker is. It also puts sophisticated attacks in the hands of , or at the direction of , less sophisticated attackers; what looks like organised crime may still actually be attributable to a disgruntled employee or a nation state. There have also been reports of groups such as street gangs or criminal motorcycle gangs turning to cybercrime as a source of funds.

Individual cybercriminals

Individual criminal actors can carry out attacks that may be indistinguishable from those of organised criminal gangs. They may also offer their services to others (malware as a service, DDoS as a service, etc.) in return for a fee. The availability of pre-packaged attack software (i.e., ransomware toolsets) makes today's cybercriminal far more dangerous than those of former years.

Investigative journalists

In the past, journalists used hacking techniques to pursue stories, but the spread of cybersecurity and anti-hacking laws has made this practice dangerous. Particularly in the United Kingdom, the phone intrusion trials that resulted in journalists and editors being convicted and sentenced to prison have curtailed these practices.

Insiders

Disrupters

There are insiders who are on a mission to cause problems for a company. It could be a disgruntled current or former employee. It could be someone who gets themselves hired (or

assigned as a temporary employee) to gain access for the purpose of causing problems. A motivated disrupter with appropriate access can cause tremendous damage. For example, a disrupter who is in an IT position could cause backup files to be replaced with useless files, and could then damage live files that have no usable backup. This is why monitoring software that can detect suspicious or unauthorised activities is so important.

IP compromiser

An IP compromiser has a mission of stealing intellectual property (IP). IP can be valued at millions or even billions of dollars. Stealing a software source code can jump-start a foreign competitor's capabilities.

Data compromiser

Like an IP compromiser, a data compromiser is up to no good. He or she wants to steal data that can either be turned into money (for example, by selling it to a credit card number distributor) or released, directly or indirectly, to embarrass a target organisation.

Unintentional

Insiders can also be responsible for incidents without intending to do so. They can also be divided into two broad groups: victim and error maker.

Victim

An insider can be targeted by a perpetrator to take an action to help carry out an attack without realising that they are doing so.

Phishing: Phishing emails have become ubiquitous. They have the objective of getting the recipient to either click on a link within an email that leads to the deployment of malware, or to give up log-in credentials, credit card numbers or other valuable data. Even though some organisations offer anti-phishing training to employees, this scheme still works on a small percentage of the targeted population.

Social engineering. Criminals will use the phone to induce an insider to reveal non-public information. In one method, the caller pretends to be from the company's IT department and needs to log in remotely to fix a problem, which requires getting the employee's log-in credentials. Some people fall for it and provide the information.

Business email compromise. A perpetrator sends an email to a targeted employee, sometimes using an email address very similar to that of the targeted organisation, pretending to be a senior executive. The bogus senior executive needs the employee to help with a secret deal by wiring funds (sometimes millions of dollars, or the equivalent) to a specific account. Most people now recognise this for the fraud that it is, but sometimes it works, and the funds are transferred.

Work-at-home dupe. An individual can be induced to take part in what they believe to be a work-at-home opportunity that turns out to be part of a sophisticated theft scheme. The work-at-home worker may turn out to be supporting money laundering, sanctions evasion or other crimes.

Error maker

Sometimes, an individual simply makes a mistake that leads to a data compromise. For example, a systems developer may inadvertently misconfigure a cloud-based storage container and leave it open to access through the internet, leading to the data stored in the digital container being compromised. Similarly, something as simple as an email sent to an incorrect address (or a fax message sent to the wrong fax number) can cause the compromise of highly sensitive information. This can be caused by accidentally entering the wrong email address, or deliberately (but unknowingly) directing an email to an address set up by an adversary with a very similar address to that of the real organisation.

Scanners

It is important to point out that cyber perpetrators may also use automated tools to look for companies whose systems exhibit particular vulnerabilities that leave them open to attack. Thus, a company may be targeted simply because the attacker has the capability to successfully carry out an attack. These attacks use tools called scanners that, in effect, test sites for the presence of specific weaknesses that render the site vulnerable to penetration.

Cyber incident methods

High-tech, low-tech and blended attacks

It might be easy to throw up one's hands and say that data breaches are inevitable and, to an extent, that is true. There is no such thing as 100 per cent security but that is not an excuse to give up. Any meaningful study of threats recognises that some are high-tech. They rely on vulnerabilities in software or in cybersecurity operations. Others are low-tech, relying on human error. Still others combine multiple vectors of attack into blended threats. Consider the following examples.

Vault 7

Vault 7 is the name given by Wikileaks to its trove of cybersecurity information apparently stolen from the US Central Intelligence Agency. Vault 7 material included what were previously unreported methods for compromising multiple types of systems. Suddenly, with the release of Vault 7 material, nation states and cybercriminals had access to world-class hacking tools. This is one reason for so many attacks being successful. They employed methods that the perpetrators would have never had access to if it were not for the release of CIA materials through Vault 7.

Polymorphic malware

When malware was first developed, defensive systems were developed that could recognise the specific signature of particular pieces of malware. But malware writers understood this and developed what is called polymorphic malware, which modifies itself every time it is duplicated, without the changes affecting the functionality of the malware. Once each copy is unique, traditional pattern-based detection systems cannot see it. Newer defensive tools had to be developed to recognise the actions of the malware. Adversaries continue to develop malware with more advanced detection-avoidance capabilities, so anti-malware vendors are always in a race to keep pace.

Malware (and malware as a service)

Tens of thousands of pieces of malware are developed every day. Malware can be aimed at an operating system or a particular application. The proliferation of malware makes it vital to maintain up-to-date patching. Patches are software modifications developed by manufacturers to counter specific threats, including those associated with malware. Additionally, as a business feature, some malware writers, rather than selling a piece of malware to a buyer, operate it for them, and this is known as malware as a service.

Ransomware (and ransomware as a service)

In the past couple of years, a new form of malware called ransomware has emerged and been the cause of tremendous problems for both public and private sector organisations. When it enters a system, ransomware encrypts storage devices that it can control, leaves behind a notice that the software has encrypted stored documents and files, and informs system owners that upon payment of a ransom (often to be paid in a cryptocurrency such as bitcoin or monero), the perpetrator will send a decryption key. While initial ransomware usually asked for a few hundred dollars, ransomware today is often targeted at enterprises, and ransom payments ranging from tens of thousands to hundreds of thousands of dollars may be demanded. High ransom payments are often demanded if the ransomware has the capability of encrypting cloud-based backup copies of files. Unfortunately, many companies feel they have no alternative but to pay the ransom and have to hope that the criminals will actually provide a working decryption key. Note also that some ransomware is provided to criminals as a service operated by other criminals. Some are so sophisticated as to provide detailed instructions for the victim to use in purchasing cryptocurrency. Some even provide a customer service phone number for victims to call for payment assistance.

Denial of service attacks

Websites can be overwhelmed by receiving millions of messages per second. This is how DDoS attacks work. Most often operated by criminals as a service, these attacks take advantage of thousands of computers that have been infected with malware that enables them to be commanded to send large numbers of messages to a target. With hundreds or thousands of computers sending large numbers of messages to the target, the website can be disabled. These DDoS attacks can be combined with a blackmail demand ('Pay me and I will stop the attack') or may be conducted for political or ideological purposes. Fortunately, internet service providers have become good at defeating these attacks.

Social engineering

Social engineering attacks focus on making people do what the attacker wants. The many forms include the following:

- Business email compromise, as discussed earlier.
- Credential compromise. This is a scheme designed to get a targeted individual to reveal system credentials, such as user ID and password. One way of reducing the chance of a successful credential compromise is to use what is called two-factor authentication (or 2FA), whereby a user ID and password is not sufficient to gain access to a system. The

second factor could be a message sent to a smartphone, or a fingerprint, or any number of other means.

- Dropping infected drives. Perpetrators have been known to leave a thumb drive containing malware where it can be readily found. For example, it might be left attached to a key ring in a public toilet, or in a company car park. The hope is that it will be found and the drive plugged into a computer in an attempt to identify the owner (perhaps by finding a picture or document with a clue as to the person's identity). Once plugged in, the drive injects the malware into the system, where it is designed to spread. An alternative is for someone with access to the premises, such as a janitor, to plug an infected drive into multiple computers.

Automated attacks

One method that perpetrators use to identify potential victims is an automated attack, in which the perpetrator uses software that runs tests against target systems to identify those with specific vulnerabilities. In some cases, the objective is to identify a vulnerable system for infection at a later stage. In other cases, identification of the vulnerability is combined with exploitation of the vulnerability.

The life cycle of an attack

Attackers must overcome a lot of challenges before their efforts can be considered successful. Of course, this involves some understanding of the objectives of the perpetrators. For example, if the objective is to render a given website or internet-connected access point unavailable, the attacker does not have to figure out how to access, collect and extract data from the target. Rather, the attacker needs to know only how to either block access to the site or cause it to fail. For example, if a site's manager has not taken simple (but vital) steps to prevent unauthorised changes to the internet registration of a domain (e.g., sampledomain.com), an attacker can initiate a transaction that could associate that domain name with an internet protocol address controlled by the attacker. When someone enters the domain name, they end up somewhere else. Once the objective of the attack is known, the elements of information needed to understand the attack become evident.

While attacks against cyber infrastructures have been going on for more than 50 years in various forms, there are many published standard ways of defining how incidents occur. Some, we have found, oversimplify an attack and do not result in the depth of understanding needed to understand why an attack was successful, what worked (and did not work) for the attackers, and what you need to know to effectively strengthen your cyber defence measures. In developing this chapter, we decided to use the MITRE ATT&CK™ model,[2] which is the result of contributions from many experienced practitioners as a way of describing attacker behaviours in a consistent way.

The ATT&CK model suggests that to fully understand an incident, an organisation should try to understand the following characteristics of attacker behaviour. Our experience

2 The MITRE ATT&CK model is both a database and a model for understanding the ways in which cyberattackers operate. It is available for use without charge. See https://attack.mitre.org/resources/getting-started/.

indicates that it is unlikely that all these characteristics will be known, particularly at the initial stage of an incident response and investigation, but it is a very useful model for reminding the investigators of the diverse avenues they need to pursue.

Initial behaviour

How was the attack initiated? Did it involve removable media? Was it a 'drive-by' (a visit to a website that automatically downloads malware)? The result of a phishing email? Social engineering? Additionally, attackers may carry out pre-attack activities such as surveillance (i.e., determining what tools are in use within a network and testing to determine whether common exploitable vulnerabilities exist). Recognising these indicators of an attack that is in the planning stage can help an organisation to prevent it, or at least to mitigate the damage. Note that pre-attack activities can be either focused on a specific target or carried out by automated systems to create a list of vulnerable sites to be exploited in the future. This element of the incident includes what some other models refer to as 'reconnaissance activities'. To the extent that a network can detect these types of activities, that can be an early indicator of a potential attack on the network, and can provide the information needed to prevent or mitigate a successful attack and exfiltration of data.

Execution

What was the technology used to initiate the compromise? Was it a compiled HTML file? Did it use a dynamic data exchange? Was PowerShell used?[3]

Persistence

In previous decades, the attack model was to get in, steal data, cover your tracks and get out quickly. Today, the model has morphed to one in which the attacker aims to establish a long-term stealthy presence in the target network. This characteristic describes the means used to support persistence of an attack.

Privilege escalation

Once an attacker enters a system, they may well need to gain additional capabilities to do things like getting to valuable data, moving to other parts of the system, establishing persistence or being able to remove data from a network. How they go about doing this is described in this characteristic.

Defence evasion

Once in a system, attackers do not want to be noticed, caught or prevented from carrying out their plans. They understand not only that their targets will put defences in place to prevent them from being successful, but what those defences are likely to be. There are many ways in which an attacker can bypass or otherwise evade these defensive measures; understanding how they carried out the evasion is an important part of understanding the attack as a whole.

3 PowerShell is an automation engine and scripting language with an interactive command-line shell that Microsoft developed to help IT professionals configure systems and automate administrative tasks.

Credential access

How did the attacker get the credentials used in an attack? Did they find the information in an insufficiently protected file? Was a known vulnerability used to gain access to a valid credential? Was the attacker able to cause the creation of a credential that was not supposed to exist?

Discovery

How did the target discover the attack? For example, did they notice a strange device on their network? An unusual file? An anomalous movement of data out of the system? Unfortunately, the discovery process may not start until the victim organisation is notified of the attack by a third party (e.g., by law enforcement agencies or a payment card issuer).

Lateral movement

Once an attacker has gained access to a network, how do they navigate from one part of that network to another part of the network, or to a connected network? As an example, in the well-known 2013 attack against the retailer Target, the cybercriminals first entered the system through a vendor responsible for store heating and cooling systems; they were then able to move laterally through the network to gain access to the payment card information of tens of millions of customers. Moving from the environmental systems part of the network to the payment card portion of the network represents lateral movement.

Collection

What techniques were used by the attackers to collect the data that they intended to move out of the system? Were they able to access shared drives? Did they use screen captures? Did they access information stored on a remote system (i.e., cloud storage)? Understanding this is key to developing more effective defensive measures.

Extraction

How did the criminals get the data from your network to the site or email address that they control? Did your data leakage control system fail (if you have one)? Were there unprotected endpoints? In one case, we discovered that an organisation that believed it had 14 points of connection to the global internet actually had more than 70!

Command and control

There are a number of ways in which an attacker can monitor and direct an attack against an organisation. As with other categories, understanding how they achieved command and control helps with strengthening defences.

In looking at this list, you may notice that there was no specific element focused on the identity of the perpetrator of the incident. There are several reasons for that. First, once it is determined, for example, that the attack was designed to steal credit card information and that the stolen information was transmitted to a site in Asia, there may be little or no value in spending time and money in what may well be a fruitless search for the identity of those responsible. The chance of actually catching them and bringing them to justice is low, and

an insurer or managers may not want to incur that expense. Second, there are many ways in which a perpetrator can obfuscate its connection to your data. You may believe you know who the perpetrator is, but that may not be sufficient to support a prosecution or to result in an international extradition.

Monitoring the threat environment

Is there a requirement to monitor the threat environment? We believe that organisations have an obligation to understand the risks they face. Without such an assessment, an organisation cannot effectively target the resources available to them to maximise their protection, and some may require assistance in monitoring for threat intelligence and active threats. There are many sources – commercial, government, academic and not-for-profit – that may be able to provide assistance in this regard.

Threats are constantly evolving along with technology. Business risks that were acceptable yesterday may be unacceptable today. New threats are constantly arising. Simply carrying out a threat assessment is not enough; the process must be constantly reviewed to take into account threat evolution. But in addition to threats posed by nation-state actors, NGO actors, insiders and hacker groups, an organisation's freedom of action in regard to self-defence may also be affected by laws, regulations, contract provisions and self-interest. These may require or prohibit certain actions by an organisation to accomplish cybersecurity goals.

Law

Governments worldwide are recognising the risks associated with cyber operations in their public and private sectors, and passing laws to criminalise certain actions. These laws may extend to movement (or limitation of movement) of data across national borders. Organisations are responsible for maintaining knowledge of laws in countries in which they operate or in which their customers or data reside.

Regulation

Regulations, like laws, can affect decisions about how systems are structured and protected. As with laws, it is incumbent on companies to maintain knowledge of applicable regulations. Note that regulations can be promulgated by or limited to a single nation, or may be associated with a multinational organisation. For example, the EU General Data Protection Regulation has effect throughout the European Union.

Contractual

Some cybersecurity requirements can be the result of a contractual relationship. For example, on a global basis, those organisations accepting payment cards (debit and credit cards) are obliged by contract to protect card information using the Payment Card Industry Data Security Standard.

Self-interest

An organisation may set rules that are more strict than those required by law, regulation or contract. Having more limitations on data protection and movement than are required by external factors may be important in some industries, and companies are free to self-impose

restrictions as long as those restrictions are compatible with laws, regulations and contractual requirements.

How to accomplish monitoring the threat environment

Obviously, organisations differ in size, technological capability, size of legal staff and needs. While some may have the in-house capability to monitor the nature of threats that they face, others may not. Regardless of these factors, the need to monitor the threat environment, to carry out risk assessment and to design, implement and maintain a commercially reasonable and effective cybersecurity program is incumbent on all organisations. Any organisation that lacks the capabilities to do so must seek assistance. In some cases, organisations may turn to government agencies for help with monitoring threats and developing and implementing an effective cybersecurity program, or they may seek help from academic institutions or not-for-profit organisations. But in many cases, the most cost-effective alternative is to work with a commercial vendor that can provide a continuing service to carry out monitoring, leveraging updated indicators of compromise and real-time notifications of problems.

Why are so many attacks successful?

We have been fighting challenges to our computer systems for almost 50 years, and challenges to our financial systems, intellectual property and informational targets with value for centuries. But it seems that as quickly as we develop defences, the criminals develop new ways of defeating them. Can we change that paradigm? And if we can, will we?

The root cause of the problem starts with the fact that the internet, as we know it, was never designed to be secure. It permits users to hide their identities. It allows for the creation of regions such as the deepnet or the darknet, which are invisible to most users and are employed in many cases for nefarious purposes.

We don't believe that the internet was created as it was with the intention of facilitating misuse. Rather, we believe that many – perhaps most – of the problems we face are a result of what is known as The Law of Unanticipated Consequences. This concept states that there can be results of actions we take that are not what we intended, and they can be either positive or negative. An unanticipated consequence can be the result of insufficient testing or simply not thinking in terms of negative (or positive) ways in which a piece of software could be used or abused.

Cyber investigations often involve identifying root causes that are unanticipated consequences. This should not be surprising. This aim of this book is to provide guidance in initiating, carrying out and reporting on investigations of cyber incidents. While most of the steps in an investigation are quite logical, sometimes investigative success involves thinking outside the box. In fact, it is the inability to think broadly that can be the cause of an investigative failure. Keep this in mind as you read and use this book.

2

Preparedness for a Cyber Incident: Developing an Incident Response Plan, Identifying the Team and Practising

David C Lashway and John W Woods, Jr[1]

General overview

Why preparation, stakeholder identification and practice is important

No organisation of any scale presently operates without substantial reliance on information technology – servers, desktops, mainframes, cloud computing infrastructure, supervisory control and data acquisition systems, programmable logic controllers and internet of things devices are but a few of the technologies and systems used in the modern IT environment. Unfortunately, these systems constantly face a range of internal and external cybersecurity threats – from the routine to the advanced nation state. When threats to these systems manifest as events or incidents, organisational capability to react appropriately to minimise the effects almost always will depend on successful advance planning and preparation as codified in a written incident response plan that is developed and tested for effectiveness well before the incident arises.

In preparing to respond to a cyber incident, a plan is a necessary, but alone insufficient, element of incident preparedness for an organisation. To use a well-worn military phrase, 'no plan survives first contact with the enemy'.[2] This short statement brings to the fore two of the most important lessons that experienced cyber incident response professionals observe. No plan can foresee every eventuality that will arise in a given incident. As such, the incident response plan must be flexible and agile enough to respond to a variety of

1 David C Lashway and John W Woods, Jr are partners at Baker McKenzie.

2 This quote derives from Prussian General Helmuth von Moltke the Elder. See Helmuth Karl Bernhard von Moltke, *Über Strategie* (Mittler, 1891) ('The material and moral consequences of every major battle are so far-reaching that they usually bring about a completely altered situation, a new basis for the adoption of new measures. One cannot be at all sure that any operational plan will survive the first encounter with the main body of the enemy. Only a layman could suppose that the development of a campaign represents the strict application of a prior concept that has been worked out in every detail and followed through to the very end.').

unforeseen circumstances, not wooden and overly cumbersome with internal requirements that are impossible to meet in actual operation. The second lesson, derived from the first, is that testing the plan under a variety of circumstances is a critical element of executing and achieving the central mission of any plan – to mitigate the consequences of an event or incident when one emerges.

This chapter addresses strategic and tactical considerations in formulating an incident response plan and the need for, and benefit from, practising a plan before an incident emerges.

Development of incident response plans

Overview

The European Union Agency for Network and Information Security provides a succinct summary of the definition and purpose of the incident response plan:

> *Incident response and management is the protection of an organisation's information by developing and implementing an incident response process (e.g., plans, defined roles, training, communications, management oversight) in order to quickly discover an attack and then effectively contain the damage, eradicate the attacker's presence, and restore the integrity of the network and systems.*[3]

While incident response planning traditionally has focused heavily on IT security processes and procedures, as the legal and operational risks arising from incidents continue to increase due to the proliferation of operationally impactful malware, there is a commensurate need to develop a 'whole business' approach to planning for incident response. In this section, we address certain strategic considerations when formulating a plan to address current risks – legal considerations regarding the need for an incident response plan and how that plan is structured and executed, and governance considerations related to staffing the plan. Finally, there is an outline of specific tactical elements and components of a plan.

Legal considerations

An important starting point for the structure and execution of an incident response plan is the legal backdrop against which the plan will be executed. There are two overlapping but distinct legal elements: (1) the direct or indirect regulation that informs the content or timing relating to the incident response plan; and (2) issues relating to the structure of the investigation that can affect legal privilege and the discoverability of information generated during an investigation.

Regulatory considerations

With increasing regulation in the area of information security, a fundamental element of any plan is that it will satisfy the basic legal requirements imposed by relevant regulators. This can include direct regulation regarding the requirement to have a plan, such as the US Health Insurance Portability and Accountability Act (HIPAA) Security Rule, which requires

3 European Union Agency for Network and Information Security, 'Strategies for Incident Response and Cyber Crisis Cooperation' 7 (ver. 1.1 2016) (citing SANS Critical Security Control 18).

certain entities to have the ability to identify and respond to security incidents and to have contingency plans in place.[4] In addition, regulator notification, reporting requirements and other legal obligations can materially affect how a plan is structured and implemented. The most prominent example of this arises out of the breach notification requirements of the EU General Data Protection Regulation (GDPR). Under Article 33(1) of the GDPR, entities may have as little as 72 hours after becoming aware of a breach of personal information to satisfy certain notification obligations.[5] The Information Commissioner's Office (ICO) – the data protection enforcement authority in the United Kingdom under the UK Data Protection Act 2018 – has published guidance establishing that subject organisations must have an incident response plan that covers the following checklist to ensure GDPR compliance:

- allocating responsibility for managing breaches to a dedicated person or team;
- escalating a security incident to the appropriate person or team to determine whether a breach has occurred;
- assessing the likely risk to individuals as a result of a breach;
- notifying the ICO of a breach as necessary; and
- informing affected individuals of a breach as necessary.[6]

Additionally, a number of regulators and other government departments have issued legal guidance regarding incident handling that should be considered in the context of developing an incident response plan. The ability to map the steps in a plan to these guidance documents provides a strong basis to assert that the plan and response are legally well founded. Examples of guidance used in the United States to inform the content of incident response plans include the Federal Trade Commission's 'Data Breach Response: A Guide for Business'[7] and the US Department of Justice Criminal Division guidelines, titled 'Best Practices for Victim Response and Reporting of Cyber Incidents'.[8]

Finally, one notable regulatory development that needs to be factored into any response plan is related to ransomware incidents and the increased focus being paid to money laundering and terrorism financing risks due to the uptick in size of reported ransom payments.[9]

---

4 The US Health Insurance Portability and Accountability Act of 1996 [HIPAA] Security Rule requires covered entities and business associates to: identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes. 45 CFR Section 164.308(a)(6). The HIPAA Security Rule also requires HIPAA-covered entities and business associates to establish and implement contingency plans, including data backup plans, disaster recovery plans and emergency mode operation plans. 45 CFR Section 164.308(a)(7).

5 General Data Protection Regulation [GDPR], Article 33.

6 Information Commissioner's Office, 'Guide to the General Data Protection Regulation (GDPR)' (August 2018), at 233, available at https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf.

7 US Federal Trade Commission, 'Data Breach Response: A Guide for Business' (September 2016), available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0154_data-breach-response-guide-for-business.pdf.

8 US Department of Justice, 'Best Practices for Victim Response and Reporting of Cyber Incidents' (version 2.0 September 2018), available at https://www.justice.gov/criminal-ccips/file/1096971/download.

9 An overview of the ransomware payment market and increase in payments is found at the CNBC Article 'The extortion economy: Inside the shadowy world of Ransomware payouts' (6 April 2021). Available at www.cnbc.

On 1 October 2020, the US Department of the Treasury (the Treasury) issued a pair of advisories to alert companies about risks associated with ransomware.[10] The first advisory from the Treasury's Financial Crimes Enforcement Network (FinCEN) provides general information on the role of financial intermediaries in the processing of ransomware payments, and a list of ransomware-related financial red flags, including instances in which organisations in high-risk sectors (e.g., government, financial, educational, healthcare) engage in transactions with companies known to facilitate ransomware payments. The second advisory from the Treasury's Office of Foreign Assets Control (OFAC) highlights the sanctions risks associated with facilitating ransomware payments on behalf of victims targeted by malicious cyber-enabled activities. Taken together, these guidance documents should be factored into a response plan, with a key planning consideration being the identification of a vendor that has robust procedures in place to mitigate OFAC-related risk in the event an organisation is faced with a decision of whether to pay a ransom.

At bottom, legal and regulatory issues related to an organisation's incident response processes are evolving rapidly, and it is important to track these legal requirements and understand how they may have a material effect on the resources, structure and language used to describe an incident in response planning.

Legal privilege issues

A consideration in forming an incident response team is the extent to which certain legal privileges may be implicated in aspects of the response. As a general proposition, an incident response plan should provide guidelines for identifying incidents that present material legal, regulatory, operational, commercial or reputational risk and, for such incidents, structuring the incident response team in a way that maximises the ability to assert applicable legal privileges, as appropriate.

While it is beyond the scope of this chapter to discuss the complex nuances of global privilege law,[11] a critical action that needs to occur at the outset of a response is determining whether the organisation will seek to assert privilege over communications and documents created during the response and investigation, and the scope of such privilege. As described in more detail in Chapter 3 of this book, in the US a number of courts have recognised and protected the privilege of the work of internal teams during incident response intrusion investigations when the direction of that work was properly structured.[12] In 2020, two decisions

com/2021/04/06/the-extortion-economy-inside-the-shadowy-world-of-ransomware-payouts.html.

10 See Department of the Treasury Office of Foreign Asset Control, 'Advisory on Potential Sanctions Risks for Facilitating Ransomware Payment' (1 October 2020) (OFAC Advisory) available at https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions/20201001; Department of the Treasury Financial Crimes Enforcement Center, 'Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments', FIN-2020-A006 (Oct. 1, 2020) available at www.fincen.gov/resources/advisories/fincen-advisory-fin-2020-a006 (FinCen Advisory).

11 A helpful overview of privilege law across certain key jurisdictions can be found at the Baker McKenzie Global Privilege Center. Available at https://globalprivilege.bakermckenzie.com/.

12 *See, e.g., In re Premera Blue Cross Customer Data Sec. Breach Litig.*, 296 F. Supp. 3d 1230 (D Or 2017); *In re Experian Data Breach Litig.*, Case No.15-mdl-1592, 2017 WL 4325583, 2017 US Dist LEXIS 162891 (CD Cal 18 May 2017); *In re Target Corp. Customer Data Sec. Breach Litig.*, MDL No. 14-2522, 2015 WL 6777384, 2015 US Dist LEXIS 151974 (D Minn 23 Oct 2015); *Genesco, Inc. v. Visa U.S.A., Inc.*, 302 FRD

from the same US court addressing privilege issues involving a single data security incident that reached different outcomes provides some insight on consideration of how to structure engagements to maximise that ability to assert privilege. The decisions were issued in a case arising from a 2019 incident involving a large banking entity that allegedly impacted the information of 100 million consumers.[13] Plaintiffs in the case were seeking access to various vendor reports about the incident. In the first decision, the court disallowed a claim of privilege over the work of the forensic vendor that conducted the incident response investigation, with the opinion highlighting the fact that the vendor retention leveraged a pre-existing agreement with the company, as opposed to a bespoke agreement to support legal counsel. The vendor's report was shared for business reasons both internally and with its auditor, and the forensic vendor was not paid out of the legal budget.[14] In the second opinion, the work of a different consultant was deemed protected from disclosure, with the court matter highlighting certain specific legal considerations that drove the consultant's retention, the fact that the retention agreement was bespoke to the engagement, and that circulation of the report was significantly circumscribed.[15] While only a single decision from one US court, these procedural considerations are notable to contemplate as a plan is developed.

Governance considerations

The first two elements of the ICO checklist (see 'Regulatory consideration') touch on the need to allocate responsibility within an organisation and ensure that the right levels of an organisation are notified when an incident occurs.[16] These governance considerations are at the foundation of any incident response plan. The US National Institute of Standards and Technology (NIST) Computer Security Incident Handling Guide highlights the fact that an organisation's overall management structure and size can affect the management model employed, highlighting that in some instances a centralised team is best while in others a distributed or coordinating model can work.[17] Regardless of the model, most well-formed incident response teams either explicitly or implicitly follow the Gold-Silver-Bronze, or Strategic-Tactical-Operational, command structure developed by the United Kingdom Metropolitan Police Service in 1980 and currently codified in the London Emergency

168 (M.D. Tenn 2014); *In re TJX Cos. Retail Sec. Breach Litig.*, Case No. 1:07-cv-10162 (D. Mass. 9 Nov 2007) (Minute Order).

13 Rachel Sandler, 'Capital One Says Hacker Breached Accounts Of 100 Million People; Ex-Amazon Employee Arrested', *Forbes* (29 July 2019) available at www.forbes.com/sites/rachelsandler/2019/07/29/capital-on e-says-hacker-breached-accounts-of-100-million-people-ex-amazon-employee-arrested/?sh=4da880fd41d2.

14 See *In re Capital One Customer Data Security Breach Litigation*, 2020 U.S. Dist. LEXIS 91736, Case No. 1:19-md-02915 (E.D. Va. May 26, 2020) (Anderson M.J.) Docket Entry 490 *affirmed by In re Capital One Customer Data Security Breach Litigation*, 1:19-md-02915 (E.D. Va. June 25, 2020) (Trenga J.) Docket Entry 641.

15 See *In re Capital One Customer Data Security Breach Litigation*, 1:19-md-02915 (E.D. Va August 24, 2020) (Anderson M.J.) Docket Entry 804.

16 Guide to the GDPR (footnote 6), at 233.

17 National Institute of Standards and Technology [NIST], Spec. Pub. 800-61, 'Computer Security Incident Handling Guide' 13 (revised 2 August 2012), available at https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf.

Services Liaison Panel's Major Incident Procedure Manual.[18] This crisis management framework generally has three management tiers:

- Strategic or Gold Commanders are responsible for preparing the strategy for their organisation's role in the incident. He or she retains overall command of resources but delegates tactical decision making to a Silver Commander.[19]
- Tactical or Silver Commanders are responsible for planning the tactics to be adopted to achieve the strategy set up by a Gold Commander. Silver Commanders should be located where they can most effectively carry out their responsibilities but should be distanced from the immediate response activities.[20]
- Operational or Bronze Commanders control and utilise the resources of their respective service within a specific area to implement the tactics prepared by a Silver Commander.[21]

It is important to note that under this structure, competency and experience drives the leadership designation, not title.

Both NIST and the International Organization for Standardization (ISO) adopt this pyramid governance structure in practice through the designation of incident response leads and the recognition that, in many instances, these leaders will not perform any actual incident handling.[22] The core benefit of a plan that is consistent with these standards is that it enhances the ability to ensure that appropriate individuals are part of the response leadership, that they are engaged at the right time in the response, and that operational and crisis management responsibilities are aligned.

In developing the governance framework of a response plan, and the general roles and responsibilities of its strategic, tactical and operational teams and their individual members, an organisation should consider its business structure and identify, assess and prioritise the various risks to the organisation that can arise from a security incident:

- the nature of the business and its operations (e.g., whether the business is consumer-facing or business-to-business, provides network, data or professional services, or manufactures and sells goods or connected devices, and the sensitive customer, employee or organisational information or other assets that require protection);
- the structure of the organisation, including size and complexity (e.g., whether it has global operations, geographically disparate functions, a parent-subsidiary relationship that must be aligned, or a segmented or third party-hosted computing infrastructure); and
- risks related to a declared security incident, which may be reputational, commercial, legal (contractual/regulatory) or operational, and may affect the physical safety of customers or employees, or the security, privacy, confidentiality, integrity or availability of sensitive data under the control or in the possession or custody of the organisation.

---

18 London Emergency Services Liaison Panel, Major Incident Procedure Manual (9th ed. 2015), available at https://www.met.police.uk/SysSiteAssets/media/downloads/met/about-us/major-incident-procedure-manual-9th-ed.pdf.

19 ibid., at Section 6.5.1.

20 ibid., at Section 6.4.1.

21 ibid., at Section 6.3.1.

22 NIST Spec. Pub. 800-61 (footnote 17), at 13. ISO/IEC 27001 establishes that organisations 'should ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses'. ISO/IEC, No. 27001, Information Security Management, at A.16.1. (2013).

Components of an incident response plan

A comprehensive framework of the individual components of an incident response plan is available in the form of guidance issued to its examiners by the US Federal Financial Institutions Examination Council (FFIEC), which is a council of US financial regulators whose responsibilities include setting the information security standards of federally chartered financial institutions:

> *The institution's program should have defined protocols to declare and respond to an identified incident. More specifically, the incident response program should include, as appropriate, containing the incident, coordinating with law enforcement and third parties, restoring systems, preserving data and evidence, providing assistance to customers, and otherwise facilitating operational resilience of the institution. . . .*
>
> *Preparation determines the success of any intrusion response. Such preparation involves defining the policies and procedures that guide the response; assigning responsibilities to individuals; providing appropriate training; formalizing information flows; and selecting, installing, and understanding the tools used in the response effort. Additionally, management should define thresholds for reporting significant security incidents, and consider developing processes for when the institution should notify its regulators of incidents that may affect the institution's operations, reputation, or sensitive customer information.*[23]

In light of the FFIEC guidance, and similar guidance released by NIST,[24] the US Federal Trade Commission[25] and the US Department of Justice,[26] among other incident response guidelines, an incident response plan should address the following elements:

- what constitutes an incident as opposed to a security event;
- the process for formally declaring an incident;
- the make-up of and process for assembling the incident response team;
- guidance for management's handling of incidents, including roles and responsibilities, span of authority and span of control;
- guidance on operational handling of incidents, including evidence preservation and containment;
- guidance for information sharing, both internally and externally;
- authority to declare an incident a breach, or other legally significant designation;
- considerations for determining whether to engage external support parties and contact information for those parties (e.g., specialised computer forensics, legal consultants, credit monitoring and a call centre);
- guidance for engaging law enforcement agencies; and
- guidance for remediating incidents and conducting post-incident reviews.

23 The Federal Financial Institutions Examination Council, IT Examination Handbook for Information Security, Section III.D (September 2016).

24 NIST Spec. Pub. 800-61 (footnote 17).

25 'Data Breach Response: A Guide for Business' (footnote 7).

26 'Best Practices for Victim Response and Reporting of Cyber Incidents' (footnote 8).

The elements outlined above reflect regulatory and industry guidance relating to incident response plans. Generally, these plans have a strong focus on managing a breach of confidential information, particularly personally identifiable information, protected health information or other sensitive data. As noted above, incidents are occurring that affect the operational functionality of the systems and may render an organisation incapable of performing almost any function that relies on IT systems. For example, based on public reports, the NotPetya malware that struck major companies around the world functionally rendered several Fortune 1000 companies inoperable.[27] Moreover, this was not a one-off event – for example, in 2021, major global corporations such as CNA Insurance and Honeywell experienced significant operationally impactful events due to ransomware.[28]

Unfortunately, the lessons of these operational incidents have not yet been fully incorporated into the regulation, literature and guidance, and are not fully considered in many incident response plans. Based on direct experience in advising organisations following malware incidents that have severely affected business operations, including the NotPetya event, organisations would be well served by reviewing their existing incident response plans with the following questions in mind:

- Does the current incident response plan integrate with the organisation's business continuity and disaster recovery plan from both an operational and management perspective?
- How will the incident response plan be carried out if all the communications infrastructure owned and managed by the organisation is inoperable?
- Has the organisation identified and mapped its critical business services to understand what systems need to be brought online, and in what order, in the aftermath of an operationally major event?
- Many organisations have in place incident response retainers with third parties; has the organisation assessed and identified a third-party vendor to assist with the provision of surge IT capacity to assist in restoring the computing environment after an operational event?
- Does the organisation understand key external dependencies and how to restore them in the aftermath of an operationally major event?

The law, regulation and guidance will continue to reflect the growing threat presented by these operational events. One recent example is the October 2020 guidance issued by the FFIEC, directly addressing operational resilience and specifically discussing resilience considerations for operationally impactful cyber events.[29]

---

27 See Andy Greenberg, 'The Untold Story of NotPetya, the Most Devastating Cyberattack in History', *Wired Magazine*, September 2018, available at www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

28 See Eduard Kovacs, 'Honeywell Says Malware Disrupted IT Systems', Security Week (March 24, 2021) available at www.securityweek.com/honeywell-says-malware-disrupted-it-systems; Alicia Hope, CPO Magazine, 'Cyber Insurance Firm Suffers Sophisticated Ransomware Cyber Attack; Data Obtained May Help Hackers Better Target Firm's Customers' (April 5, 2021) available at www.cpomagazine.com/cyber-security/cyber-insurance-firm-suffers-sophisticated-ransomware-cyber-attack-data-obtained-may-help-hackers-better-target-firms-customers/.

29 See Press Release, *Agencies release paper on operational resilience* (Oct. 30, 2020), www.federalreserve.gov/newsevents/pressreleases/bcreg20201030a.htm.

Another consideration for an incident response plan is the identification of the relevant stakeholders within the organisation as an incident can implicate potentially all aspects of an organisation and thinking through the multidimensional team is important. An incident response plan should identify the strategic or tactical leads for each potentially relevant function within the organisation. These functions will vary depending on the organisation's complexity and mission, but could include the following:

- Operations. The business units within the organisation are generally responsible for understanding and mitigating the operational effects on the organisation, including outcomes that may result from impairment to affected IT systems and capabilities, as well as any loss of goodwill.
- Legal. The legal staff are generally responsible for identifying and mitigating legal risks associated with the incident, including ensuring compliance with relevant regulatory obligations, privacy and securities laws, interfacing with regulators, and managing or avoiding potential disputes and litigation. As noted above, under precedent such as *In re KBR*, to maximise claims of legal privilege, the general counsel or other legal leadership must direct and control the investigation into the incident.
- Communications. The communications staff are generally responsible for ensuring consistent messaging that complies with business requirements, including with respect to the public, investors, affected individuals or customers, and in certain employee communications within the organisation. Fulfilling this function will usually require coordination with the legal function to ensure that communications comply with applicable legal requirements and otherwise consider post-breach legal risks.
- Technical. The technical team will typically include members of the information security function as well as the operational IT groups. The security team members will typically focus on investigating the incident and formulating an appropriate containment strategy. IT staff will need to assist the investigators while also remediating the incident as appropriate. This may include a range of possible responses, from restoring a handful of affected systems to implementing the disaster recovery protocol.
- Sales/Account Management: In incidents involving business to business relationships, sales and account teams with the direct client relationships can prove instrumental to navigating and communicating with customers. Training sales personnel on the basics of incident response and what to say and not to say while an incident is occurring is key, as customers will be reaching out to the account representatives directly and demanding answers.
- Finance. The finance team will generally be responsible for mitigating any financial effects an incident might have, including planning around lost revenue and securing necessary funding for external costs. The finance team may also be responsible for insurance recovery.
- Human resources (HR). The HR team will generally be responsible for ensuring the incident response complies with applicable employment policies (such as overtime rules). HR may also be implicated to the extent that employee malfeasance is found to be a contributing factor to the incident, employee personal information may have been compromised, or employee morale may need to be managed as part of the response efforts.[30]

30 See also NIST Spec. Pub. 800-61 (footnote 17), at 17 (identifying functional areas typically called upon in an incident response).

The plan also should identify key external advisers who would be called upon during a response, such as a cyber incident response firm, crisis communications firm and legal counsel. By identifying and establishing engagement terms with these third-party vendors, the organisation's response can be significantly streamlined and more efficacious.

Finally, many organisations find it constructive to build relationships with third parties such as law enforcement, cybersecurity-focused government stakeholders and key regulators in advance of an incident. When an event happens, established relationships that facilitate the disclosure of the incident to a government stakeholder can go a long way towards mitigating the overall organisational risk to that sometimes key constituency. And a response itself can be materially assisted by information flow to and from the government, be it law enforcement such as the US Federal Bureau of Investigation or government programmes specifically designed to reduce cybersecurity risk, such as the UK's Government Communications Headquarters – National Cyber Security Centre public-private information sharing programme.

Practising the incident response plan

A growing component of the cyber programme for organisations with a relatively mature cybersecurity capability is the regular mandatory testing of their incident response plans. The US Department of Homeland Security Exercise Evaluation Program has developed a robust programme to test incident response plans and identified seven types of exercises that can facilitate their adoption and execution.[31] The first four are discussion-based exercises, each with a different focus and rules, but all exercises usually include a facilitator who leads the discussion and records input and responses:

- Seminar: An informal discussion, designed to orient participants to new or updated plans, policies or procedures.[32] In the information security context, a seminar could be scheduled to facilitate a cross-organisational discussion regarding how, for example, information security and IT management interpret aspects of the span of control provisions within an information response plan.
- Workshop: Similar to a seminar, but more focused on forward-looking risks or changes.[33] An example of a workshop might be how the incident response team may incorporate the growing risk of operationally high-risk malware into the incident response policy.
- Tabletop exercise: Involves key personnel discussing simulated situations in an informal setting.[34] These situations are designed to assess plans, policies and procedures on a given set of facts and to discuss the different perspectives of the participants.
- Games: Offers a simulation of operations. It can often involve two or more teams, usually in a competitive environment, using rules, data and procedures designed to depict an actual or assumed real-life situation.[35] Games require significantly more investment of time and effort, as the facilitator must react to responses by the game participants within

31 US Department of Homeland Security, Homeland Security Exercise and Evaluation Program (April 2013), available at https://www.fema.gov/media-library-data/20130726-1914-25045-8890/hseep_apr13_.pdf.

32 ibid., at 2 to 4.

33 ibid., at 2 to 5.

34 ibid.

35 ibid.

the rules established for the game. An example of a game would be one in which management must decide whether to pay a ransom in a ransomware situation and a discussion is facilitated to bring varying considerations to the fore.

Operations-based exercises validate plans, policies, agreements and procedures, clarify roles and responsibilities, and identify resource gaps in an operational environment. Types of operations-based exercises include the following:

- Drill: A coordinated, supervised activity focused on a single specific operation or function within an organisation.[36] A drill might entail an information security 'red team' operating within carefully prescribed parameters attempting to penetrate a network without triggering alerts so as to test intrusion detection tools and personnel.
- Functional exercise (FE): Similar to a game but can occur over a longer period and is designed to test coordination, command and control between various areas of the organisation.[37] As in a game, facts relating to a hypothetical incident are presented to participants, but there is less discussion and more real-time decision-making among the stakeholders. An example again could be similar to the game situation of a ransomware attack, but the FE involves less discussion and more structure to emulate the organisation's decision-making process.
- Full-scale exercise: A multi-stakeholder exercise involving functional areas.[38] In the information response planning context, such an exercise might involve engaging with key third-party vendors as participants in the exercise. Other options include retaining former regulators or reporters to simulate third-party reaction to decisions made by the incident response team.

At its broadest, exercises can touch on all aspects of the incident response plan and all relevant stakeholders can participate, including business unit leaders, communications, legal, the executive management team, the board and external stakeholders. Capturing and incorporating feedback and the lessons learned to improve the response plan is an important aspect. Each participant should provide feedback not only on the exercise itself, but also on whether the existing response plan adequately informed them of their roles and responsibilities and provided sufficient guidance to execute their roles.

In essence, the most carefully drafted and considered plan on paper is worthless if, during a crisis, those charged with executing it fail to know and understand their responsibilities within a well-considered framework. The best-prepared organisations exercise their plans regularly in different ways and with different methods for continuous improvement.

36 ibid., at 2 to 6.
37 ibid.
38 ibid.

3

The 'Art' of Investigating: Responding and Investigating at the Same Time and Overseeing a Privileged Forensic Investigation

Benjamin A Powell and Jason C Chipman[1]

Incident response requires an immediate, coordinated effort to gather the facts and execute an incident response plan that enables a company reacting to a data breach to address multiple work streams simultaneously. All at once, the company will need to manage, and be prepared to tackle, various work streams, including, but not limited to:

- conducting a forensic investigation to understand what has occurred, how it occurred and what, if any, damage was caused to the confidentiality, availability or integrity of company systems or data;
- preserving evidence;
- containing and remediating the incident;
- preparing for and complying with any notice requirements to regulators, consumers or other third parties;
- preparing for and responding to formal and informal regulatory or legislative enquiries;
- coordinating with law enforcement;
- developing and, where necessary, deploying contingency planning, messaging strategies and communications to in-house and external audiences;
- preparing and monitoring for possible litigation, including preserving documents and monitoring dockets;
- briefing insurance carriers; and
- assuring auditors that IT controls remain sound.

The details of these specific work streams, and considerations for each, are detailed later in this chapter and in subsequent chapters of this book. In this chapter, we begin by highlighting some of the tactical processes, deliverables and tools that should be launched immediately, as they facilitate an effective, strategic and forward-leaning incident response, rather

1 Benjamin A Powell and Jason C Chipman are partners at Wilmer Cutler Pickering Hale and Dorr LLP.

than a reactive and chaotic one. We then discuss two work streams in which companies can be particularly proactive: managing the forensic investigation and coordinating with law enforcement.

Launching an incident response

An effective incident response requires an organised process, regular communication, a single consolidated understanding of the facts, and a system for tracking key communications and events. Specifically, the following steps and documents should be initiated immediately and regularly updated or reassessed, as appropriate, throughout the incident response:

- Assembling the team. The first step is identifying which in-house personnel and external vendors (e.g., law firms, forensic vendors) should form the core incident response team. Ideally, this should be addressed in the company's incident response policy (as discussed in Chapter 2) but some incident response teams may reasonably include 'optional' members depending on the circumstances (such as the head of a particular affected business unit, or the head of human resources if the breach has affected a large number of employees). Companies should quickly identify which incident response team members are relevant for a particular incident and continue to reassess whether additional members should be engaged.
- Assigning tasks. Each work stream should be assigned to designated in-house and external personnel, such as through a matrix identifying each work stream, point of contact, action item, status and expected completion date. This should include work streams for incident response, forensics, communications with key in-house and external audiences, and legal and regulatory analysis and coordination.
- Scheduling calls and meetings. The incident response team should meet regularly to ensure that messaging, goals and developments remain coordinated across work streams. For example, those developing communications documents will need to be aware of new forensic developments, and those coordinating regulatory communications will need to be aware of any developments in messaging strategy. Regular communication will also ensure that company priorities potentially affecting or affected by the incident response (e.g., regularly scheduled filings to the Securities and Exchange Commission) can be synchronised with the incident response efforts. Typically, we recommend at least two daily calls or meetings: (1) a strategy and update meeting with the incident response team leadership (including external counsel) to review the current status, recent developments and next steps, and to open questions for each work stream; and (2) a technical update with the forensic team, internal IT or information security and external counsel to discuss forensic developments, resolve technical challenges and prioritise tasks.
- Maintain a detailed chronology. All key events and communications should be tracked in a centralised, detailed chronology, preferably prepared and maintained by external counsel. The chronology should include minute details in a straightforward factual manner, including key in-house and external communications (e.g., board briefings, updates to insurance carriers, productions to law enforcement), investigation and remediation updates, and key forensic details. This will allow the company to cross-correlate events from different work streams and respond in the future to specific detailed questions regarding the incident, the investigation or the company's response.

- Draft a centralised narrative. Information known about the incident, when it was identified and what key questions remain should be drafted in a centralised narrative, again preferably prepared and maintained by external counsel. To the extent known, it should describe the initial point of entry and how it was leveraged, key instances of lateral movement and potential data compromise. The narrative should be high level and clear about outstanding strategic considerations. This document should be used as a starting point for all external communications to ensure consistency and accuracy in messaging.

While these processes and documents are under way, the forensic work will begin in earnest, proceeding with four primary objectives: (1) preserving potentially relevant evidence in a forensically sound manner; (2) investigating what happened; (3) containing the incident to prevent further exposure and remove the threat actor; and (4) remediating identified vulnerabilities.

Many companies understandably prioritise containment and remediation. However, to successfully mitigate the incident and prevent potential further exposure, evidence preservation and a preliminary investigation must often be completed first. Before an incident can be safely contained, the company must have a sufficiently complete understanding of the vulnerabilities leveraged by the threat actor; otherwise, containment efforts may miss potential areas of exposure or back doors installed by the hacker, allowing the hacker to maintain a low profile and continue its attack. Appropriate evidence preservation is also key to fully understanding an attack's life cycle.

Managing a third-party forensic investigation

Most companies engage third-party forensic investigators to assist in responding to a breach. In virtually all significant incidents that may involve regulatory enquiries, customer concerns or other significant issues, having a third-party expert perform the forensic analysis provides necessary resources,[2] gives assurance to regulators and customers that an incident has been examined by an independent party [3] and brings in additional expertise to examine a problem.

In addition to these advantages, using a third-party forensic investigator, and particularly one engaged by external counsel, can be critical to maximising privilege protections for forensic analysis, work-product and working papers. In the event of a cyber incident,

2 See, e.g., Paul Cichonski, Tom Millar, Tim Grance, Karen Scarfone, US Department of Commerce, National Institute of Standards and Technology, Special Publication 800-61 Revision 2, 'Computer Security Incident Handling Guide', 14 to 15 (August 2012), http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf ('Incident response work is very stressful, as are the on-call responsibilities of most team members. This combination makes it easy for incident response team members to become overly stressed. Many organizations will also struggle to find willing, available, experienced, and properly skilled people to participate, particularly in 24-hour support. Segregating roles, particularly reducing the amount of administrative work that team members are responsible for performing, can be a significant boost to morale.').

3 See, e.g., Federal Trade Commission [FTC], 'Data Breach Response: A Guide for Business', 1 (September 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0154_data-breach-response-guide-for-business.pdf (encouraging companies to '[c]onsider hiring independent forensic investigators to help you determine the source and scope of the breach. They will capture forensic images of affected systems, collect and analyze evidence, and outline remediation steps').

the breached company may face a variety of legal risks, as discussed elsewhere in this book. In such situations, customers, regulators or class action plaintiffs would undoubtedly seek discovery of written materials relating to a forensic investigation. Materials created at the direction of legal counsel to enable external counsel to advise the company may be protected under privilege and help to ensure the company is given effective legal advice.

The best way to mitigate these risks – and the path pursued in virtually every significant cybersecurity incident to date – is to ensure the forensic investigation is conducted under legal privilege. In this section, we describe key considerations for conducting the investigation in a manner that maximises privilege protection. We then briefly discuss other considerations in overseeing an investigation being conducted by an external firm, including ensuring appropriate and efficient coordination between external forensic vendors and in-house IT staff, reviewing deliverables from the forensic vendors and, in the case of a payment card breach for which a payment card industry (PCI) forensic investigator (PFI) is engaged, navigating that investigation alongside the privileged investigation.

Protecting privilege over forensic work

In the United States, the attorney–client privilege protects confidential communications between clients (including employees and former employees of corporate clients) and their lawyers relating to the provision of legal advice. This privilege also applies to consultants retained by attorneys to help provide legal advice.[4] Separately, the work-product doctrine protects documents and working papers prepared by lawyers, clients and their consultants and experts in anticipation of litigation.[5]

While the forensic facts of an incident alone may not be privileged, and may ultimately need to be disclosed to third parties, maintaining attorney–client and work-product privilege protections over the underlying investigatory documents would allow a breached company to proceed in a manner that minimises its legal exposure.

A key enquiry into whether communications or work-product are privileged is determining whether the communication occurred or the work-product was generated for the purpose of providing legal advice or in anticipation of litigation – rather than in the ordinary course of business. Generally, this is a far more straightforward enquiry in the case of an independent forensic investigator (particularly one engaged and supervised by external counsel)[6] than in the case of in-house IT and IT security staff. A court may determine that the business role of IT and IT security staff is to investigate cybersecurity incidents for the sake of the

4 *United States v. Kovel*, 296 F.2d 918, 921 (2d Cir 1961).

5 Privilege law may vary from jurisdiction to jurisdiction. We encourage those conducting breach response investigations outside the United States to further assess how applicable privileges may apply in this context in other jurisdictions.

6 While some organisations rely on in-house counsel to run breach responses and engage or oversee forensic investigations, the argument that privilege applies in those cases can be more complicated than in the case of external counsel. This is because in-house lawyers may have a dual business and legal role, such that a company 'may face more difficulty showing that in-house counsel communications deserve privilege protection than showing that communications of outside lawyers who predominantly provide legal advice deserve protection'. Margaret A Dale and Yasmin M Emrani with Practical Law Institute Intellectual Property & Technology, 'Data Breaches: The Attorney-Client Privilege and the Work Product Doctrine', 3, Thomson Reuters (2017), www.proskauer.com/insights/download-pdf/4949.

business (e.g., to remediate the breach), irrespective of legal or litigation considerations, such that no legal privilege protects underlying investigative material, even if the in-house staff report their findings to counsel.

Several cases have affirmed the privilege protections applicable to third-party forensic consultants after a breach.

Genesco, Inc v. Visa USA, Inc

In this case, the court found that the attorney–client privilege and work-product doctrine protected communications between Genesco's general counsel and Genesco's third-party forensic investigator, Stroz Friedberg, because the retainer agreement, an affidavit and other documents showed that the general counsel engaged Stroz Friedberg in anticipation of litigation to assist him in providing legal advice.[7] Specifically, the general counsel's affidavit explained that he retained Stroz Friedberg after (1) the PFI had identified evidence of an intrusion; (2) he had conversations with external counsel regarding the legal ramifications of the intrusion (including the likelihood of litigation); (3) the company determined that he should conduct an investigation into the incident 'separate and apart from the investigation already being conducted by [the PFI] on behalf of [the card brands] for the purpose of providing legal advice to Genesco regarding the intrusion and in anticipation of litigation . . .'; and (4) counsel identified the need to retain a computer security consultant to assist in this investigation.[8]

In re Target Corporation Customer Data Security Breach Litigation

Target engaged two teams from Verizon to conduct forensic investigations: (1) a team to advise the data breach task force, which was established at the direction of in-house and external counsel after a public announcement of the breach and after several class action lawsuits had been filed against Target, to 'educate Target's attorneys about aspects of the breach' so that counsel 'could provide Target with informed legal advice'; and (2) a team of investigators engaged in a PFI role.[9] Target limited its privilege claims to the first team, which, per the engagement letter between external counsel and Verizon, was engaged to 'enable counsel to provide legal advice to Target, including legal advice in anticipation of litigation and regulatory inquiries'.[10] The plaintiffs had argued that communications and documents prepared by Verizon were not privileged because 'Target would have had to investigate and fix the data breach regardless of any litigation, to appease its customers and ensure continued sales, discover its vulnerabilities and protect itself against future breaches'.[11] The court agreed with Target, finding that the data breach task force 'was focused not on remediation of the breach . . . but on informing Target's in-house and outside counsel about the

7 *Genesco, Inc. v. Visa U.S.A., Inc.*, 302 FRD 168, 180 to 181 (MD Tenn 2014).

8 ibid., at 180.

9 *In re Target Corp. Customer Data Sec. Breach Litig.,* No. 14-2522, 2015 WL 6777384, at *1 (D Minn 23 October 2015).

10 ibid., at *1 (internal citations omitted).

11 ibid.

breach so that Target's attorneys could provide the company with legal advice and prepare to defend the company in [pending and reasonably anticipated] litigation'.[12]

In re Experian Data Breach Litigation

Experian's external counsel retained the forensic firm Mandiant.[13] Experian said that 'the only purpose of [Mandiant's] report [wa]s to help [external counsel] provide legal advice to Experian regarding the attack'.[14] The Mandiant report, which was finalised after Experian publicly announced the breach and the first claims against Experian had been filed, was provided by Mandiant to Experian's external counsel, who then provided it to in-house counsel.[15] The plaintiffs argued that the report was not protected by the work-product doctrine because 'Experian had independent business duties to investigate any data breaches and it hired Mandiant to do exactly that after realizing its own experts lacked sufficient resources'.[16] While the court agreed Experian had those obligations, it found that the 'record . . . makes it clear that Mandiant conducted the investigation and prepared its report for [external counsel] in anticipation of litigation, even if that wasn't Mandiant's only purpose'.[17] The court emphasised that the full report was not given to Experian's in-house incident response team, that external counsel instructed Mandiant to conduct the investigation and that the report would not have been prepared in substantially the same form or with the same content but for the anticipated litigation.[18]

In each of the above cases, the court found that privilege protections applied for reasons that would generally not be applicable to an in-house forensics team – because (1) the scope or purpose of work in the engagement letter emphasised that the work was being conducted to provide legal advice; (2) the forensic investigator reported to counsel; and (3) the work was performed not as part of the ordinary course of business investigation but to provide legal advice.

The holding in *In re Premera Blue Cross Customer Data Security Breach Litigation* was generally consistent with these principles, but reached the opposite conclusion. The company asserted attorney–client or work-product privilege over several categories of documents, including reports issued by a forensic investigator under the supervision of Premera's external counsel.[19] Mandiant had been hired by Premera, prior to the discovery of the breach, to review the company's systems. During this investigation, Mandiant discovered malware. Premera then hired external counsel and, subsequently, Premera and Mandiant amended the statement of work (SOW) to shift supervision of Mandiant's work to external counsel but without changing the description of Mandiant's scope of work.[20]

12 ibid., at *3.
13 *In re Experian Data Breach Litig.*, No. 15-01592, 2017 WL 4325583, at *2 (CD Cal 18 May 2017).
14 ibid.
15 ibid.
16 ibid.
17 ibid.
18 ibid.
19 *In re Premera Blue Cross Customer Data Sec. Breach Litig.*, 296 F Supp 3d at 1230 (D Or 2017).
20 ibid., at 1245.

While Premera argued that the situation changed after discovery of the breach, the court found that the unchanged scope of work in the SOW did not support the assertion. The court found that 'change of supervision, by itself, is not sufficient to render all the later communications and underlying documents privileged or immune from discovery as work-product'.[21] Because Premera did not meet its burden to show that either (1) 'Mandiant changed the nature of its investigation at the instruction of outside counsel and that Mandiant's scope of work and purpose became different in anticipation of litigation' or (2) 'all of the underlying documents relating to the Mandiant reports were created because of anticipated litigation and "would not have been created in substantially similar form but for the prospect of litigation"', it could not assert privilege over the reports.[22] However, specific documents or portions of documents could be withheld if they (1) were prepared to communicate with an attorney for the provision of legal advice, (2) contained counsel's own impressions in anticipation of litigation, (3) communicated factual information to counsel to prepare for litigation, or (4) involved a factual investigation done solely at the behest of counsel for the purpose of litigation and not under the original work scope.[23]

A Virginia court reached a similar conclusion in *In Re: Capital One Consumer Data Security Breach Litigation*, MDL No. 1:19md2915 (AJT/JFA)(ED VA)). In that case, a magistrate judge held that a forensic report drafted by Mandiant – a consulting firm retained by Capital One's counsel – was not protected under the work product doctrine.[24] In assessing whether the work product privilege applied, the judge examined whether *Capital One* would have prepared the Mandiant report in question in a similar form but for the litigation. The court concluded the report did not meet the 'but for' test because Capital One had a pre-existing relationship with Mandiant through which Mandiant conducted substantially similar work for Capital One business units. The Magistrate Judge declined to address whether Capital One waived any privilege by providing the Mandiant report to regulators (Office of the Comptroller of the Currency, Consumer Financial Protection Bureau).

Some parties have attempted to avoid the outcome from Capital One by creating a dual-track approach to incident response investigations. This approach calls for an organisation's internal cybersecurity team to conduct its own investigation of an incident, with a forensic vendor engaged to support the business while a legally privileged investigation is pursued with an outside vendor engaged by counsel. In practice, it remains unclear whether such an approach strengthens a litigant's privilege claim. In *Wengui v. Clark Hill PLC*, No. 19-3195 (DDC, 12 January 2021), the US District Court for the District of Columbia concluded that a forensic report commissioned by outside counsel was not privileged, and not subject to the work product doctrine, because it would have been commissioned by the business in any event. The defendant in *Wengui* argued that the business had a separate forensic vendor engaged, although the Court noted that the factual record showed that the business unit actually relied upon the work commissioned by outside counsel.

Premera also helps shed some light on how courts may view the privilege status of other documents, beyond forensic investigators' reports and working papers, created in the course

21 ibid.

22 ibid., at 1245 to 1246.

23 ibid., at 1246.

24 The only issue in the *Capital One* case was whether the report was protected under the work product doctrine.

of a privileged breach response. Premera asserted privilege over a number of documents, including (1) drafts of documents written or edited by counsel, and (2) documents drafted by non-legal personnel at the request of counsel but not created by or sent to counsel. The first category included documents that were drafted by and sent to or from non-attorneys but included edits from counsel, or drafted by counsel and incorporated edits from non-attorneys.[25] For some, Premera asserted privilege only over the drafts. The second category included documents with information relating to 'technical aspects of the breach and its mitigation, company policies, public relations and media matters, and remediation activities' and were prepared either by Premera personnel or third-party vendors retained by external counsel.[26]

The court found that only some of these documents were protected by attorney–client privilege.[27] For example, documents containing edits by an attorney communicating legal advice would be protected attorney–client communications, as long as the edit was not done solely with a business purpose in mind.[28] Similarly, communications relating to these documents sent to or from counsel seeking or providing actual legal advice, such as about possible legal consequences of proposed text or a contemplated action, would be privileged.[29] However, drafts (and communications about them) in which Premera 'was required as a business to prepare [the document] in response to the data breach' (e.g., press releases and breach notice letters) were not automatically privileged by virtue of '[t]he fact that Premera planned eventually to have an attorney review those documents or that attorneys may have provided initial guidance as to how Premera should draft [them].'[30] Because this includes documents the company 'would have prepared regardless of any concern about litigation, . . . [p]lacing them under the supervision of outside counsel and then labelling all communications relating to them as privileged does not properly establish an attorney–client privilege'; instead, '[t]he focus of the privilege must be the purpose for which a document was created'.[31]

Companies must also take care in the aftermath of an investigation to ensure that the privilege remains protected. In *Leibovic v. United Shore Financial Services, LLC,* the court found that United Shore had waived privilege for an investigation by disclosing 'the details' of the results in an interrogatory response.[32] United Shore's lawyers hired Navigant to assist them in an internal investigation. While the court did not specify what United Shore disclosed in the

25 ibid., at 1240 to 1241.

26 ibid., at 1242.

27 ibid., at 1241.

28 ibid., at 1242.

29 ibid., at 1244.

30 ibid., at 1241. While maintaining privilege over public relations vendors and efforts is beyond the scope of this chapter, it can be key in breach response work. For further guidance on maintaining privilege over public relations documents generally, see Jeffrey Schomig, 'Keeping PR Strategy Communications Privileged: Part 1', *Law360* (1 February 2019) and Jeffrey Schomig, 'Keeping PR Strategy Communications Privileged: Part 2', *Law360* (4 February 2019), www.wilmerhale.com/en/insights/publications/20190201-keeping-pr-strategy-communications-privileged-part-1 and www.wilmerhale.com/en/insights/publications/20190204-keeping-pr-strategy-communications-privileged-part-2.

31 *In re Premera,* 296 F Supp 3d at 1241 to 1242.

32 *Leibovic v. United Shore Fin. Servs*., LLC, No. 15-12639, 2017 WL 3704376 (ED Mich 28 August 2017), mandamus denied by *In re: United Shore Fin. Servs.*, LLC, No. 17-2290, 2018 WL 2283893 (6th Cir 3 January 2018).

interrogatory response, it found that the response 'went beyond providing factual information regarding the existence of the investigation and retention of Navigant[, . . . but] included details regarding Navigant's conclusions'.[33] The court placed significant emphasis on the fact that United Shore had disclosed the details of Navigant's conclusions during and in support of litigation. This is consistent with the overall principles that litigants cannot use privilege as 'a shield and a sword'.[34]

As exhibited by these cases, entities investigating a breach should take appropriate steps both in the engagement phase and during an investigation to maximise the likelihood that communications and forensic vendor work-product will be protected by privilege. Third-party forensic experts generally should be engaged by external counsel. The contract, and the SOW, should expressly make it clear whether the forensic work is being performed to assist counsel in providing legal advice in anticipation of potential litigation or regulatory enquiries, or both. During the course of the investigation, attorneys generally should be included in emails and, where practical, in correspondence between the company and the forensic investigators. All communications, working papers and deliverables should be labelled as privileged. Attorneys should be actively engaged in directing the investigator's work.

Coordinating internal IT and external forensic teams

The main concern companies often express about using third-party investigators is that the investigation will be slower and more cumbersome than an investigation conducted by in-house teams. IT and IT security personnel are often particularly concerned about vendors' lack of knowledge of the relevant systems and people, as well as delays in the early days of an investigation that may occur as vendors deploy their people and tools.

These concerns can be mitigated by engaging a forensic vendor prior to an incident occurring. Having this relationship in place, with contracts already negotiated and designated points of contact, allows forensic investigators to 'hit the ground running' when they receive notice of a breach. The more fully this relationship is developed before a breach (e.g., through discussions about the overall system architecture, advanced deployment of tools, developing a rapport), the quicker the external team can begin its incident response following a breach and the more streamlined the process will be as it progresses.

In addition to preparations in advance, forensic investigators have the most success in launching their investigation in an expeditious manner when they can work with the in-house team. By leveraging their knowledge of systems, networks and people, the vendor team can deploy its tools and obtain the artefacts and data it needs quickly.

Reporting considerations

Many companies assume, as standard, that they want the results of an investigation to be documented in a formal written report. However, this may not be necessary or otherwise desirable in all situations. Companies should consider the necessity for such a report prior to

33 ibid., at *3.

34 *In re: United Shore*, No. 17-2290 2018 WL 2283893, at *2 (quoting *United States v. Bilzerian*, 926 F 2d at 1295, 1292 (2d Cir 1991)).

deciding whether to commission a formal report, including considering the possibility that a report may not be shielded, in whole or in part, by privilege.

A company should consider whether external counsel should direct the report, and perform any reviews of it, before providing it to the company. External counsel should ensure the accuracy of the underlying descriptions of the incident as part of providing legal advice to the company. The goal should be to ensure that the report is straightforward and factual, without unnecessarily loaded terms or graphics. To the extent that the company has taken containment and remediation steps, these steps should be validated by the forensic investigator and included in the report. Once the report is finalised, its circulation should be limited. For example, the company should consider whether only certain parts of the report should be shared with the in-house IT team.

Parallel investigations by PCI forensic investigators

In the event of a suspected compromise of payment card information, one or more payment card brands may direct the breached entity to engage a PFI to conduct an investigation and report its findings to the card brands. PFIs must issue reports using card brand-approved templates.[35] In the reports, the PFI will describe whether and how PCI was compromised, confirm the date of containment, recommend further security enhancements, and identify specific areas of security non-compliance and whether that non-compliance caused or contributed to the breach.

This report will be provided to the card brands and will form the basis of any card brand fines. The card brands will also typically seek regular telephonic updates from the PFI. As such, PFI investigations are not protected by privilege. It is therefore important to navigate the relationship between the company and the PFI strategically and effectively. This requires:

- working throughout the investigation to establish goodwill between the company (and its counsel) and the PFI;
- having the company's privileged investigator collect the same evidence and follow similar forensic leads as the PFI so that the company can understand the technical facts underlying the PFI's findings; and
- managing and segregating the PFI's investigation (as well as communications with the PFI and the card brands) from the company's privileged investigation so as to avoid potentially compromising the privilege.

Ransomware considerations

Companies facing a ransomware or extortion event may need to take special incident response coordination steps, particularly if there is a potential business need to acquiesce to a payment demand. These types of attacks often prompt victim organisations to engage third-party experts to assist with interacting with a threat actor, evaluating threat actor demands, and

35 Payment Card Industry (PCI) Data Security Standard: 'PFI Preliminary Incident Response Report – Template for PFI Preliminary Incident Response Report', Version 2.2 (August 2017), https://www.pcisecuritystandards.org/documents/PFI_Preliminary_Incident_Response_Report_v2.2.pdf?agreement=true&time=1552267715716; Payment Card Industry (PCI) Data Security Standard: 'Final PFI Report – Template for Final PFI Report, Version 2.1 (August 2017), https://www.pcisecuritystandards.org/documents/Final_PFI_Report_v2.1.pdf?agreement=true&time=1552267715728.

potentially facilitating payment. Although the official position of federal law enforcement on ransomware attacks is to report the incident and refrain from paying a ransom, the Federal Bureau of Investigation (FBI) and Department of Justice (DOJ) have also asserted that the decision to pay a ransom is a business issue that companies must evaluate in light of the overall risks associated with an incident. DOJ guidance states that '[a]ny entity infected with ransomware should contact law enforcement immediately,' that 'there are serious risks to consider before paying the ransom,' and the government 'does not encourage paying a ransom to criminal actors'.[36]

Where a payment is contemplated, it is important to engage with counsel, to report the incident to law enforcement in advance, and to seek assistance from external counsel to evaluate regulatory risks. Ransomware and extortion payments present special regulatory concerns that must be carefully evaluated. On 1 October 2020, the US Department of the Treasury's Office of Foreign Assets Control (OFAC) issued an advisory addressing risks associated with facilitating ransomware payments: the Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments (the OFAC Ransomware Advisory). The advisory represents the first time that OFAC has issued guidance that specifically addresses ransomware payments. The advisory identifies regulatory risks associated with OFAC's strict liability regime:

> *OFAC may impose civil penalties for sanctions violations based on strict liability, meaning that a person subject to US jurisdiction may be held civilly liable even if it did not know or have reason to know it was engaging in a transaction that is prohibited under sanctions laws and regulations administered by OFAC.*

The OFAC guidance suggests that risk associated with payment may be mitigated by, among other things, cooperation with law enforcement. The guidance states that:

> *self-initiated, timely, and complete report of a ransomware attack to law enforcement to be a significant mitigating factor in determining an appropriate enforcement outcome if the situation is later determined to have a sanctions nexus.*

Coordinating with law enforcement

In the wake of a cyber incident, many companies share information with law enforcement, often publicly touting this coordination in public statements about the incident. In this section, we describe both the advantages and limitations of sharing with law enforcement. Next, we describe some of the logistical considerations in providing information to law enforcement. Finally, we describe some of the protections available to companies sharing information under the Cybersecurity Information Sharing Act (CISA) and how to maximise available protections when sharing with law enforcement.

36 See US Government, 'How to Protect Your Networks from Ransomware', at 5, www.justice.gov/criminal-ccips/file/872771/download ('Guidance'); see also FBI, 'Incidents of Ransomware on the Rise: Protect Yourself and Your Organization', 29 April 2016, www.fbi.gov/news/stories/incidents-of-ransomware-on-the-rise.

Advantages and limitations to sharing with law enforcement

Sharing information with law enforcement offers a number of advantages. Regulators typically look favourably on this form of information sharing, and coordination with law enforcement may be particularly important when responding to a ransomware event for reasons noted above.[37] In some circumstances, this can also arm law enforcement with information that is critical to bringing the perpetrator to justice. Cooperating with law enforcement is also typically viewed positively by customers and as a reputational matter. In certain limited circumstances, notifying law enforcement can also provide companies with an opportunity to delay notice to consumers if notification could impede a law enforcement investigation. In such circumstances, the company should obtain a written request from law enforcement.

That said, in deciding whether and how to share information with law enforcement, it is important to maintain realistic expectations. For example, except in exceedingly rare circumstances, law enforcement will not perform a forensic investigation for the breached company. It is also rare for law enforcement to provide the reporting company with information about a suspected perpetrator of the breach, or to immediately take legal action against a suspected perpetrator. While the DOJ is increasingly bringing charges against major cyber criminals and nation-state actors, these charges often come years after the fact, and frequently are the culmination of investigations into multiple incidents committed by the same or related actors. In these cases, law enforcement typically does its best to anonymise the victim companies.

Logistics of sharing information

Once a company has decided to engage with law enforcement, a number of practical considerations come into play. These include:

- Who. In the United States, cyber crimes are generally investigated by the Secret Service and the FBI. The Secret Service is generally responsible for investigating financial crimes and fraud (such as those involving theft of payment card data)[38] while the FBI's authorities are broader. Companies should develop relationships with relevant law enforcement officials in advance of a breach. Both agencies maintain regional task forces throughout the country.[39] In addition to reporting to law enforcement, companies can also upload cyber threat indicators to the US Department of Homeland Security (DHS) online portal.[40]

---

37 See, e.g., Mark Eichorn, 'If the FTC comes to call', FTC Business Blog (20 May 2015), www.ftc.gov/news-events/blogs/business-blog/2015/05/if-ftc-comes-call; see also Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments (OFAC Ransomware Advisory), https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf; and the Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments, FIN-2020-A006 (FinCEN Ransomware Advisory), https://www.fincen.gov/sites/default/files/advisory/2020-10-01/Advisory%20Ransomware%20FINAL%20508.pdf.

38 US Secret Service, 'The Investigative Mission', https://www.secretservice.gov/investigation/ (last visited 19 March 2019) ('Today the agency's investigative mission has evolved from enforcing counterfeiting laws to safeguarding the payment and financial systems of the United States from a wide range of financial and computer-based crimes.').

39 See Criminal Division, Computer Crime & Intellectual Property Section, Cybersecurity Unit, 'Best Practices for Victim Response and Reporting of Cyber Incidents', Version 2.0, Department of Justice [DOJ] (September 2018), www.justice.gov/criminal-ccips/file/1096971/download.

40 'DHS Cyber Threat Indicator and Defensive Measure Submission System',www.us-cert.gov/forms/share-indicators.

- When. Companies should contact law enforcement as soon as possible, if appropriate.
- What. Law enforcement is typically interested in hackers' tactics, techniques and procedures. Companies should share this information, to the extent that it is available, including 'indicators of compromise' (i.e., lists of suspicious IP addresses, domains or accounts; malware hashes, signatures and files; and attacker tools). Law enforcement may also seek copies of compromised systems or raw log data; companies should consult their legal counsel before sharing such data.
- How. Typically, data is shared either digitally or in hard copy. Sometimes, law enforcement may request a briefing, possibly with the forensic investigator. In those circumstances, companies should work with legal counsel to ensure appropriate steps are taken to preserve privilege. All communications with law enforcement should be tracked and logged. Written communications should be marked to invoke all available protections (discussed below).

Cybersecurity Information Sharing Act

In 2015, the United States enacted CISA, which provides authorisation and liability protection for cybersecurity information-sharing.[41] Specifically, CISA authorises private entities to share 'cyber threat indicators'[42] and 'defensive measures'[43] with federal entities, for 'a cybersecurity purpose,'[44] as long as the information is shared in a manner consistent with CISA, including a variety of provisions intended to protect personal information.[45]

Pursuant to CISA, the DHS and DOJ have published guidance documents to help companies understand CISA and how to share properly.[46] CISA also required the DHS to establish an online portal for the US Federal Government to receive cyber threat indicators from the private sector.[47] However, the process created by the DHS does not limit or prohibit sharing information associated with known or suspected criminal activity or the sharing of cyber threat indicators with federal entities in support of law enforcement investigations.[48]

41 The Cybersecurity Act of 2015 was enacted as Division N in the Fiscal Year 2016 omnibus spending bill. Title I of the Act, commonly referred to as the Cybersecurity Information Sharing Act (CISA), includes authorisation and liability protections for cybersecurity monitoring, information-sharing and use of defensive measures. CISA has been codified in the US Code at 6 USC Sections 1501 to 1510.

42 CISA defines a 'cyber threat indicator' broadly, to include, among other things, 'information that is necessary to describe or identify' malicious reconnaissance, a security vulnerability, a method of defeating a security control or exploitation of a security vulnerability, malicious cyber command and control, or the actual or potential harm caused by an incident. See 6 USC Section 1501(6)(A) to (H).

43 ibid., Section 1501(7)(A).

44 ibid., Section 1501(4).

45 ibid., Sections 1503(c) and (d), 1504, 1505(b).

46 See, e.g., Department of Homeland Security [DHS] and DOJ, 'Guidance to Assist Non-Federal Entities to Share Cyber Threat Indicators and Defensive Measures with Federal Entities under the Cybersecurity Information Sharing Act of 2015', 6 (15 Jun 2016), https://www.us-cert.gov/sites/default/files/ais_files/Non-Federal_Entity_Sharing_Guidance_%28Sec%20105%28a%29%29.pdf [hereinafter, DHS/DOJ Guidance]; DHS and DOJ, 'Cybersecurity Information Sharing Act – Frequently Asked Questions', https://www.us-cert.gov/sites/default/files/ais_files/CISA_FAQs.pdf [hereinafter, DHS/DOJ FAQ].

47 6 USC Section 1504(c).

48 ibid., Section 1504(c)(1)(e).

CISA does not include requirements to share with any particular agency. Rather, it authorises sharing with any federal entity. However, which mechanism is chosen for sharing might affect the availability of liability protections.[49]

Liability protections are most clearly available when a non-federal entity shares cyber threat indicators and defensive measures with the DHS.[50] CISA provides liability protection against suits for certain sharing of cyber threat indicators and defensive measures with the Federal Government if the information 'is shared in a manner that is consistent with section 105(c)(1)(B)'.[51] In turn, Section 105(c)(1)(B) provides that sharing through the DHS-established portal 'shall . . . be the process by which the Federal Government receives cyber threat indicators and defensive measures'.[52]

Agency guidance acknowledges, however, that 'Sections 105(c)(1)(B)(i) and (ii) of CISA describe two additional means of liability-protected sharing'.[53] These Sections provide two exceptions to the requirement that the DHS portal 'shall be the process' for sharing with the Federal Government. These include: '(i) . . . communications between a Federal entity and a non-Federal entity regarding a previously shared cyber threat indicator to describe the relevant cybersecurity threat or develop a defensive measure based on such cyber threat indicator; and (ii) communications by a regulated non-Federal entity with such entity's Federal regulatory authority regarding a cybersecurity threat.'[54] As agency guidance explains:

> *[Section 105(c)(1)(B)(i)] would apply when a non-federal entity first shares a cyber threat indicator with the DHS capability and process or a regulator as permitted by section 105(c)(1)(B)(ii) discussed below, and then engages in communications with a federal entity regarding that previously shared indicator. . . .*

49 DHS/DOJ Guidance (see footnote 44), at 10 ('[CISA] authorizes non-federal entities to share cyber threat indicators and defensive measures with federal entities . . . specifically through the Federal Government's capability and process for receiving cyber threat indicators and defensive measures under [CISA], which is operated by DHS . . . . *The manner in which information is shared affects the protections private entities receive for sharing* cyber threat indicators and defensive measures.' (emphasis added)).

50 ibid. ('[S]haring receives liability protections under 106(b)(2) when conducted with the Federal Government through the DHS capability and process, or as otherwise permitted under section 105(c)(1)(B).')

51 CISA Section 106(b)(2) (codified at 6 USC Section 1505(b)(2)).

52 ibid., at Section 105(c)(1)(B) (codified at 6 USC Section 1504(c)(1)(B)).

53 DHS/DOJ Guidance (see footnote 44), at 15. See also DHS/DOJ FAQ (see footnote 44), at 2 to 3.

54 CISA Section 105(c)(1)(B)(i) and (ii) (codified at 6 USC Section 1504(c)(1)(B)(i) and (ii)).

> *[S]ection 105(c)(1)(B)(ii) also permits communications between a regulated non-federal entity and its Federal regulatory authority regarding a cybersecurity threat.*[55]

Other than the three categories of sharing under CISA Section 105(c)(1)(B), sharing with the Federal Government is authorised but not protected from liability.[56] However, liability protection is only one of the protections under CISA and, arguably, it is limited in scope, particularly when it comes to sharing information with law enforcement.[57] CISA's numerous other protections, however, would be available regardless of the federal entity receiving the shared cyber threat indicators and defensive measures (as long as CISA's other requirements are met).[58] These include:

- No waiver of privilege. Sharing cyber threat indicators or defensive measures with the Federal Government under CISA 'shall not constitute a waiver of any applicable privilege or protection provided by law, including trade secret protection'.[59] This includes state or federal privileges and protections, notably including the attorney–client and work-product privileges.[60]
- Treated as proprietary. Shared information 'shall be considered the commercial, financial, and proprietary information of such non-Federal entity when so designated'.[61] This provision triggers a variety of protections under federal law for the handling of sensitive business information.

---

55 DHS/DOJ Guidance (see footnote 44), at 15. See also DHS/DOJ FAQ (see footnote 44), at 3 ('Section 105 contains two exceptions that authorize sharing cyber threat indicators or defensive measures with federal agencies other than through the DHS capability and process. Liability protection is available for private entities that share information directly with other federal agencies under those provisions. The first exception . . . provides for sharing . . . regarding a previously shared cyber threat indicator to describe the relevant cybersecurity threat or develop a defensive measure based on such cyber threat indicator. Sharing such information can therefore receive liability protection so long as the sharing is consistent with the other requirements in [CISA] . . . So, [while] CISA is not primarily designed to address sharing cyber threat information with law enforcement[, . . . it] does provide liability protection for sharing cyber threat indicators or defensive measures with law enforcement, if the indicator or defensive measure is shared with law enforcement as part of a communication regarding a cyber threat indicator that was previously shared by the private entity through the DHS capability and process').

56 DHS/DOJ Guidance (see footnote 44), at 10 ('In addition to sharing conducted as provided under section 105(c)(1)(B), section 104(c) also authorizes other sharing of cyber threat indicators and defensive measures with any federal entity, including sector-specific agencies; however, sharing that is not consistent with section 105(c)(1)(B) *will not receive liability protection under [CISA]*, even if a federal entity receiving the information shares it with DHS immediately upon receipt.' (emphasis added)).

57 See DHS/DOJ FAQ (see footnote 44), at 4 ('Sharing cyber threat information with law enforcement generally does not raise liability issues, particularly in the context of reporting an actual or attempted crime . . . In short, CISA supplements—but does not supplant—other measures that already protect private entities that report crimes, including restrictions on disclosing investigative material.').

58 DHS/DOJ Guidance (see footnote 44), at 10 to 11 ('Even though sharing conducted pursuant to section 104(c) but not consistent with section 105(c)(1)(B) does not receive liability protection (e.g., sharing with a federal entity that is not conducted through the DHS capability and process in section 105(c)), it still receives a variety of other protections that cover all sharing conducted pursuant to section 104(c).')

59 6 USC Section 1504(d)(1).

60 DHS/DOJ FAQ (see footnote 44), at 9.

61 6 USC Section 1504(d)(2).

- FOIA and CIIA protections. Information shared is protected from disclosure under the Freedom of Information Act and any state, tribal or local parallels.[62] Shared information will also be 'deemed voluntarily shared and exempt from disclosure' under the Critical Infrastructure Information Act.[63]
- Limitations on government use. Shared information may only be used for particular cybersecurity, law enforcement and defence purposes described in CISA.[64] Further, no government entity may use such information for regulatory action, including a regulatory enforcement action.[65]

62 ibid., Section 1504(d)(3)(B).

63 ibid., Section 1504(d)(3)(A).

64 ibid., Section 1504(d)(5)(A).

65 ibid., Section 1504(d)(5)(D)(i). However, this information may, consistent with regulatory authority specifically relating to the prevention or mitigation of cybersecurity threats to information systems, inform the development or implementation of regulations relating to such information systems. ibid., Section 1504(d)(5)(D)(ii)(I). According to the DHS/DOJ Guidance, 'CISA's legislative history states that congressional drafters viewed this as a narrow exception to ensure that government agencies with regulatory authority understand the current landscape of cyber threats and those facing the particular regulatory sector over which they have cognizance'. DHS/DOJ Guidance (see footnote 44), at 16.

4

Regulatory Compliance in the Context of a Cross-border Data Breach

Evan Norris, David M Stuart and Richard J Stark[1]

With the growing awareness of the vast amounts of personal data residing in the cloud, and the sophistication of those who wish to access it, comes an increasingly complex multinational regime of data protection laws with which global organisations must contend. While these laws share many common features, the sheer number of them – and the differences in definitions, standards and exceptions between them – presents a challenge when a data breach occurs. Perhaps most notably, the victim of the breach must adhere to regulatory deadlines in an environment of factual uncertainty that characterises the initial days following a breach. Where a significant number of individuals are affected, achieving regulatory compliance is an ever-increasing challenge for any organisation that does business across borders.

As discussed elsewhere in this Guide, one aspect of a breach investigation for an organisation is to assess early whether the breach raises notification obligations and, if so, in what jurisdictions. While a well-drawn incident response plan will have provided a head start on that assessment, one early aim of the investigation will be to complete the assessment by a careful review of the facts of the breach. In this chapter we provide an overview of the factors that bear on that assessment, as well as some considerations regarding the provision of notification itself. We then provide some observations about the broader data security compliance and enforcement landscape more generally, as we look to a future in which large-scale, cross-border breaches become increasingly commonplace and more and more data regulators and law enforcement authorities have the budgets and experience to address them.

1 Evan Norris, David M Stuart and Richard J Stark are partners at Cravath, Swaine & Moore LLP. The authors wish to thank Cravath associates Shanique C Campbell and Trevor H O'Bryan for their contributions to this chapter.

Determining whether and in what jurisdictions a data breach gives rise to notification obligations

Data breach notification laws across the globe reflect a mix of rules, standards and approaches. In the European Union, the General Data Protection Regulation (GDPR) imposes breach notification obligations that apply broadly to all data controllers and processors,[2] while France and other individual EU Member States maintain additional notification laws that apply more narrowly to specific industry sectors.[3] In the United States, each of the 50 states (as well as most districts and territories) has its own breach notification law, while a number of federal laws (and even some more state laws) regulating different industry sectors also contain breach notification rules for reporting incidents involving medical, financial and other types of data. In total, such rules have been adopted in approximately 130 countries, including jurisdictions throughout Asia, the Middle East, Africa, Latin America and other regions.[4]

These laws differ in myriad ways, including in the scope of their application, how they define a breach, the level of harm that triggers notification requirements, what exceptions may apply, who is notified, who does the notifying and what regulatory penalties may be imposed for noncompliance.[5] In the context of a cross-border data breach, the challenge this variability poses for organisations is particularly significant.

Identification of applicable laws

Data protection laws may apply based on different factors, such as the organisation's method of data collection, the industry in which the organisation operates and the residence of affected individuals.

In the United States, while there is no comprehensive data protection regime at the federal level, a handful of federal laws regulating various industries, including telecommunications, financial services and healthcare, include breach notification provisions that apply primarily based on the type of personal data a regulated entity may collect. For instance, the Gramm-Leach-Bliley Act imposes breach notification obligations on financial institutions, including federally chartered US banks and federal branches and agencies of foreign banks, with respect to non-public customer personal information.[6] Such laws also exist at the

2 'Processing' of data generally refers to the act of performing operations on personal data, including collection, storage and destruction, as well as analytics and alteration. A data 'controller' is an individual or organisation that determines the purpose and means of processing personal data, and a 'data processor' is an individual or organisation that processes data on behalf of the controller (e.g., payroll vendors and data warehouses). *See* GDPR, Article 4.

3 See, e.g., France Data Protection Act of 1978, Article 34 (data breach notification requirements specific to electronic communications services providers).

4 See David Banisar, 'National Comprehensive Data Protection/Privacy Laws and Bills 2020' (15 December 2020), https://ssrn.com/abstract=1951416.

5 The range of potential penalties differs widely between jurisdictions. In the EU, data protection authorities may impose administrative fines for breach notification violations equal to the higher of €10,000,000 or 2 per cent of any organisation's annual worldwide revenue. *See* GDPR, Articles 33, 34, 83(4). By contrast, in Canada, the Personal Information Protection and Electronic Documents Act (PIPEDA) caps the fine regulators can seek to impose on organisations that knowingly violate breach notification requirements to US$100,000 CAD. See PIPEDA, S.C. 2000, Chapter 5, Section 28.

6 15 U.S.C. §§ 6801(a), 6805(a).

state level. In New York State, for example, the Department of Financial Services enforces a cybersecurity regulation notification requirement that applies to financial service companies, including insurance companies and both domestic and non-US banks operating within the state, with respect to material business information and some personally identifying individual data.[7] In some instances, compliance with industry specific notification requirements in a federal statute will exempt an organisation from compliance with the requirements of a state's general breach notification law.[8] Outside the industry specific context, US states have consumer-oriented breach laws that typically apply broadly to organisations whenever a security incident involves data belonging to that state's residents. California's breach notification law, for instance, imposes obligations on any person or entity that conducts business in California and holds computerised personal information belonging to California residents.[9] In other words, depending on the type of data compromised in a breach, an organisation may have notification obligations under any number of US federal and state laws.

While many countries' breach laws are similar in scope to US laws, some apply regardless of industry sector and residence of affected individuals. The GDPR's data protection and breach regulations apply to data controllers and processors that maintain an establishment in the EU or conduct processing activities, wherever conducted, that are related to offering goods or services to data subjects in the EU or to monitoring those subjects' behaviour in the EU.[10] The post-Brexit data privacy laws in the UK – the Data Privacy Act of 2018 and the UK GDPR – are effectively identical in substance to the GDPR with respect to the obligations imposed on controllers and processors. And the data privacy laws of several other countries also mirror the GDPR, including, notably, Brazil's data protection regime, the LGPD, which went into effect in August 2020.[11]

Definition of 'personal information'

Many breach notification laws limit the definition of 'personal information' (or some analogous term) to an enumerated list of data characteristics that are considered sensitive. For example, many US state breach laws narrowly define personal information as an individual's first name (or first initial) and last name combined with any other data elements, such as a social security or driver's licence number.[12] California is among other states that apply a somewhat broader definition that covers 'any information that identifies, relates to, describes, or is capable of being associated with, a particular individual', including identifiers such as

7 See 23 CRR-NY 500.01(c), 500.02. New York also passed, in July 2019, the Stop Hacks and Improve Electronic Data Security (SHIELD) Act, which amends and extends data security and breach notification requirements for companies that collect information on New York residents. See N.Y. Gen. Bus. Law § 899-bb.

8 See, e.g., Va. Code Ann. § 18.2-186.6(G) (Virginia breach notification statute granting safe harbour for organisations already subject to the Gramm-Leach-Bliley Act).

9 Cal. Civ. Code §§ 1798.80(a),1798.82 (a)(1).

10 GDPR, Article 3. Under the GDPR, a 'data subject' is 'an identified or identifiable natural person,' and 'an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.' GDPR, Article 4.

11 Lei Geral de Proteção de Dados (LGPD), Law No. 13,709, Section 3.

12 See, e.g., Md. Code Ann., Com. Law § 14-3501(e)(1); Del. Code Ann. tit. 6 § 12B-101(7).

name, signature, address, employment, social security number, bank account number, and credit or debit card number.[13] And to take a US federal example, the Communications Act of 1934 protects 'customer proprietary network information', defined as information relating to the 'quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier'.[14]

By contrast, some breach notification laws adopt far more expansive definitions of personal information that cover any information relating to natural persons. For instance, the GDPR broadly defines 'personal data' as 'any information relating to an identified or identifiable natural person'.[15] Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) provides that 'personal information means information about an identifiable individual'.[16] Such general definitions could extend to almost any information relating to an individual, whether alone or combined with other data elements possessed by an organisation.

Definition of 'data breach'

Across jurisdictions, the definitional elements of a 'data breach' often include one or more of the use, disclosure, acquisition of, or access to data through illegal or unauthorised means.

Many US states define a data breach as the unauthorised or illegal acquisition of personal information.[17] In contrast, some jurisdictions consider unauthorised access, alone or in combination with another activity or a certain result, sufficient to constitute a breach. Under Singapore's data privacy statute, for example, a data breach broadly includes any 'unauthorised access, collection, use, disclosure, copying, modification or disposal of personal data', regardless of whether any harm or risk of harm was caused by the breach.[18] A few US states also define a breach as simply unauthorised access to personal information, whereas others require that the unauthorised access compromises the security, confidentiality or integrity of protected personal information.[19]

Some jurisdictions incorporate a risk standard into the definition of a data breach. For instance, Australia's mandatory Notifiable Data Breach Scheme defines an 'eligible data

13 See, e.g., Cal. Civ. Code § 1798.80(e). Alternatively, some states define personal information as 'any information concerning a natural person which, because of name, number, personal mark, or other identifier, can be used to identify such natural person'. See, e.g., N.Y. Gen. Bus. Law § 899-aa(1)(a).

14 47 U.S.C. § 222(h)(1).

15 GDPR, Article 4(1). Back in the United States, Virginia recently enacted a comprehensive data protection law (effective January 2023) that echoes the GDPR in broadly defining 'personal data' as information that is 'linked or reasonably linkable to an identified or identifiable natural person'. See Consumer Data Privacy Act § 59.1-571 et seq. Notably, Virginia's older breach notification law defines personal data more narrowly. See Va. Code Ann. § 18.2-186.6(A) (defining 'personal information' as 'the first name or first initial and last name in combination with and linked to any one or more . . . data elements that relate to a resident of the Commonwealth, when the data elements are neither encrypted nor redacted').

16 PIPEDA, S.C. 2000, Chapter 5, Section 2(1).

17 See, e.g., AS § 45.48.090(1); IN §§ 24-4.9-2-2(a).

18 Personal Data Protection (Amendment) Bill 2020, Section 26A.

19 Compare Fla. Stat. § 501.171(1)(a) (defining 'breach' as the 'unauthorised access of data in electronic form containing personal information') with Kan. Stat. Ann. § 50-7a01(h) (defining 'breach' as 'unauthorised access and acquisition of unencrypted or unredacted computerised data that compromises the security, confidentiality or integrity of personal information').

breach', in relevant part, as (1) any 'unauthorised access to, or unauthorised disclosure of, the information' or (2) 'information [that] is lost in circumstances where' unauthorised access or disclosure 'is likely to occur', both of which 'would be likely to result in serious harm to any of the individuals to whom the information relates'.[20]

As security incidents increase in sophistication, the definition of a data breach continues to evolve to include wide-ranging activities in addition to acquisition, access, use or disclosure. This evolution is noticeable in the GDPR's definition of a data breach as any 'accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed'.[21]

Exceptions and exemptions

Once an organisation determines that a breach of protected personal information has likely occurred, it must evaluate whether any exceptions or exemptions apply that could obviate the need to make a breach notification.

Encryption

Some breach notification laws carve out safe harbours for personal information or data that is encrypted (or substantially redacted) at the time of a breach. While the GDPR does not have an encryption exception, it treats 'state of the art' encryption as a data protection measure that reduces risk to individuals' rights and freedoms,[22] which could potentially excuse an organisation's duty to notify affected individuals.[23] Several US state breach laws, in contrast, explicitly distinguish between encrypted and unencrypted information when defining a data breach of personal information.[24] Some states completely exempt organisations from giving notice to affected individuals so long as the encryption was not compromised in the security incident.[25] In other states, encrypted data elements may be excluded from the legal definition of personal information or data, and the security incident that impacts encrypted data elements may be excluded from the legal definition of a data breach.

Good faith exemption

Notably, some breach notification laws exempt from the definition of a breach certain good faith access or acquisition of personal information by a company employee or agent. For

20 The Privacy Act 1988, § 26WE(2).

21 GDPR, Article 4(12). A few U.S. federal regulations adopt a comparatively broad definition, including the Veterans Affairs Information Security Act, which defines a data breach as 'the loss, theft, or other unauthorised access, other than those incidental to the scope of employment, to data containing sensitive personal information, in electronic or printed form, that results in the potential compromise of the confidentiality or integrity of the data.' 38 U.S.C. § 5727(4).

22 GDPR Article 32(1)(a).

23 See id.; GDPR, Article 33(1).

24 See, e.g., Cal. Civ. Code § 1798.82(a); Tex. Bus. & Com. Code Ann. § 521.053(a) (both requiring notification of a breach of encrypted personal information if the encryption key is also acquired).

25 See, e.g., D.C. Code § 28-3851(1)(B)(ii) ('The term 'breach of the security of the system' does not include . . . [a]cquisition of data that has been rendered secure, including through encryption or redaction of such data, so as to be unusable by an unauthorised third party unless any information obtained has the potential to compromise the effectiveness of the security protection preventing unauthorised access.').

instance, under the US Health Insurance Portability and Accountability Act (HIPAA), a data breach does not include 'any unintentional acquisition, access, or use of protected information' by employees of covered healthcare entities if 'made in good faith and within the scope of authority and does not result in further use or disclosure'.[26] Several US states, such as California and Virginia, also recognise a good faith exemption if an employee or agent acquires personal information for a legitimate business purpose and does not make further unauthorised disclosure of the personal information.[27] No similar exemption exists under the GDPR. Brazil also does not recognise a good faith exemption, but 'good faith of the offender' will be taken into consideration to determine appropriate administrative sanctions for data processors that violate the country's data protection law.[28]

Harm thresholds as notice triggers

Several jurisdictions have adopted data breach notification laws that utilise harm thresholds as notice triggers, whereby organisations need only give notice if harm occurred or there is a potential of harm or risk to the individuals whose personal information is breached. Notification laws in several US states enumerate the various types of harm that could trigger mandatory notification requirements, including misuse of personal information,[29] identity theft, fraud or other illegal use of personal information[30] and substantial economic loss or financial harm.[31]

More than half of the US states adhere to harm thresholds in their breach notification laws, but there is variance among the statutes with respect to the risk a breach must present to the resident consumers of those states (the typical group entitled to notice) to require notification. For example, Virginia's breach notification statute requires notification to the state Attorney General and any affected individual if there is a reasonable belief that the breach 'has caused, or will cause, identity theft or other fraud to any resident of the Commonwealth'.[32] Florida, on the other hand, does not require notice to individuals if, after appropriate investigation and consultation with federal, state and local law enforcement, the organisation determines that the breach 'will not likely result in identity theft or any other financial harm'.[33] Florida also does not require notification to its data regulator if fewer than 500 Florida residents are impacted by a breach.[34]

Harm thresholds are also used outside the United States. Under Canada's data privacy law, for example, notification to individuals and the regulator is required only where the breach creates 'a real risk of significant harm to an individual'.[35] Mexico's data privacy law requires that the breach 'significantly prejudice the property or nonpecuniary rights of the

26 45 C.F.R. § 164.402(1)(i), (iii).

27 See Cal. Civ. Code § 1798.82(g); Va. Code Ann. § 18.2-186.6(A).

28 Lei Geral de Proteção de Dados (LGPD), Law No. 13,709, Section 52, § 1(II).

29 See, e.g., Md. Code Ann., Com. Law § 14-3504(b)(2); N.J. Stat. Ann. § 56:8-163(a).

30 See, e.g., VA. Code Ann. § 18.2-186.6(A), (B); N.Y. Gen. Bus. Law § 899-aa(1)(c), (2)(a).

31 See, e.g., Ariz. Rev. Stat. § 18-552(J); Iowa Code Ann. § 715C.2(6).

32 Va. Code Ann. § 18.2-186.6(A), (B).

33 Fla. Stat. § 501.171(4)(c).

34 id. at § 501.171(3)(a).

35 PIPEDA, S.C. 2000, Chapter 5, Section 10.1(1).

data subjects' to require notification to individuals.[36] And the GDPR requires notification to the relevant supervisory authority if the breach presents a 'risk to the rights and freedoms of natural persons' and to individuals if the breach presents a 'high risk' to the same.[37] These differences in statutory definitions of the harm threshold may result in a determination, for instance, that a data breach occurred that was likely to result in a 'risk to the rights and freedoms' of EU citizens but did not pose a 'real risk of significant harm' to Canadian citizens, thus requiring notification under the GDPR but not under Canada's law.[38]

Some jurisdictions do not impose any harm thresholds either for defining a breach or setting forth the circumstances in which notification is required. For example, South Korea's data privacy law applies no harm threshold to the notification requirement.[39] Similarly, California's breach notification law imposes no harm threshold; rather, an organisation must notify affected California residents of any breach where 'unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorised person'.[40] Under these standards, actual or potential harm to individuals is not considered with respect to whether an organisation must notify individuals of a breach.

If the relevant threshold triggering a mandatory notice requirement is not met, then any notification to individuals or regulators by the impacted organisation would be voluntary. Regulators in some jurisdictions encourage such voluntary notification by organisations, even if the breach does not rise to the threshold that would require mandatory notification. Argentina, for example, has no mandatory breach reporting requirements but encourages organisations to have a plan to manage breach incidents and requires that they maintain a record of data breaches that may be given to the regulatory authority upon request.[41]

Considerations regarding the provision of notice

Once an organisation determines that notification is required or prudent, several considerations arise as to the provision of notice itself, most of which can be addressed in advance in a global breach response plan. Again, the variation between different notification regimes is significant and must be carefully considered to ensure an efficient and coordinated approach.

Who provides the notice

Under the multinational data privacy regime, only certain entities are required to provide notification in connection with a data breach. Some statutes, such as HIPAA, the US federal health law, require only that organisations operating within a specific industry sector provide notice of a breach. Other laws, however, require notification more broadly for all organisations that control or process individuals' personal data.

36 Federal Law on the Protection of Personal Data Held by Private Parties 2010, Chapter III, Article 64.

37 GDPR, Articles 33(1), 34(1).

38 Compare PIPEDA, S.C. 2000, Chapter 5, Section 10.1(1) and GDPR, Articles 33(1), 34(1).

39 Personal Information Protection Act, Article 34.

40 Cal. Civ. Code § 1798.82(a)(1), (b).

41 See Recommended Security Measures for the Processing and Conservation of Personal Data, AAIP Resolution No. 47/2018. Notably, Japan currently encourages voluntary notification in the event of a data breach, but a recent amendment to the Japanese Act of the Protection of Personal Information, which will take effect in 2022, will make such notification mandatory.

Several of the comprehensive data protection laws currently in effect require that all controllers of personal data notify individuals and regulators of a data breach. Although controllers of personal data are required to provide notice to individuals and regulators (or face penalties), the controller may not always be the entity that discovers a breach. The processors of data may be more likely to find evidence of a breach as they perform their work with the data, and for that reason a number of notification regimes require processors to notify the controller if they discover a breach. For example, the GDPR requires that the processor notify the controller 'without undue delay' after the processor becomes aware of a breach. Virginia's breach notification law also requires that those entities that maintain data that they do not own or license (i.e., processors) must report a data breach to the owner or licensee of the data (i.e., controllers) 'without unreasonable delay' after discovery of the breach.[42] These notification requirements for processors ensure that controllers will be able to timely meet their own notification obligations.[43]

Timing of notice

Many data privacy statutes require notification quickly after the organisation has discovered the breach and the scope of its impact. California's data breach notification statute, for example, requires that notification be made to individuals 'in the most expedient time possible and without unreasonable delay' following discovery or notice of the breach.[44] Notification may be reasonably delayed under California's statute to allow the organisation time to assess the scope of the breach or to prevent any interference with an ongoing criminal investigation. Several other states, including Virginia, New York and Massachusetts, require notice to data subjects without 'undue' or 'unreasonable' delay.[45] The same standard is seen in data privacy laws in other jurisdictions, such as the EU, which also requires notice to data subjects 'without undue delay'.[46]

The specific requirements vary in some statutes for notification to regulators as opposed to individuals. Some statutes may not require notification to a regulator at all unless a certain number of data subjects have been affected. California's statute, for instance, requires that there be at least 500 affected California residents before requiring that notification be made to the state attorney general. In other jurisdictions, the notice requirement for regulators is not tied to any number of affected individuals. For example, India's data protection law broadly requires organisations to 'report the cybersecurity incidents to [the regulator] within

42 Va. Code Ann. § 18.2-186.6(D).

43 This is an area where contractual considerations often arise. Controllers and processors of data maintain a symbiotic relationship, whereby controllers own and are responsible for data that may be in the possession of processors. This presents particular risks in the event of a data breach that occurs in connection with personal data a third party is processing on behalf of a controller. Controllers and processors frequently allocate these risks by entering into contracts that impose their own notification requirements and determine liability protection and exposure. Typically, controllers will seek to include specific time requirements for notification from the processor (such as within 48 hours of identifying a breach) and assignment of liability to the processor in the event of a data breach that is attributable to the processor's conduct. Processors, by contrast, typically will seek to limit their exposure in the event of a breach that may occur while the processor is in possession of the personal data.

44 Cal. Civ. Code § 1798.82(a).

45 Va. Code Ann. § 18.2-186.6(B); N.Y. Gen. Bus. Law § 899-AA(2); Mass. Gen. Laws, Chapter 93H, § 3.

46 GDPR, Article 34(1).

a reasonable time of occurrence' of the breach.[47] There is also variability in the time period to provide notice to regulators and data subjects. The GDPR, for example, specifies that notification must be made to the national supervisory authority (or lead supervisory authority in the case of cross-border breaches) 'not later than 72 hours after having become aware of' the data breach; if the supervisory authority is not notified within that window, the organisation must provide reasons for the delay.[48] This differs from notification to data subjects under the GDPR, which must be made 'without undue delay' but without reference to a specific time period.

Organisations impacted by a breach thus must assess differing notice timing requirements for regulators and data subjects both within a particular statute and across multiple jurisdictions.

Form and content of notice

Statutory requirements also vary with respect to the form and content of the data breach notice. The GDPR, for example, requires that the notice to the regulatory authority:

- describe the nature of the breach;
- provide the name and contact details of the company's data protection officer;
- describe the likely consequences of the breach; and
- describe the measures taken or proposed to be taken by the controller to address the breach.[49]

Other statutes are even more prescriptive with respect to the required form and content of the notice. California's breach notification statute, for instance, requires that the notice to individuals use a certain title ('Notice of Data Breach') and headings ('What Happened?'; 'What Information Was Involved?'; 'What We Are Doing'; 'What You Can Do'), that the title and headings be clearly and conspicuously displayed, and even that the text of the notice use no smaller than 10-point font.[50] The California statute also provides a model breach notification form that companies may use as a template for their notice, and the use of which ensures compliance with the statutory requirements.[51]

Public messaging

In addition to complying with regulatory requirements in the aftermath of a breach, organisations face the communications challenge of conveying an appropriate public message. Media outlets will quickly discover and report on any large-scale data breach – often triggered by a notification submitted to a data regulator or a public company's securities disclosure

47 Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules 2013, § 12(1)(a).

48 GDPR, Article 33(1).

49 id. Given the difficulty organisations frequently face in describing all of these elements within 72 hours of having become aware of the breach, the European Data Protection Supervisor's Guidelines permit phased reporting. European Data Protection Supervisor, Guidelines on Personal Data Breach Notification for the European Union Institutions and Bodies, Section 5.2 (Nov. 21, 2018).

50 Cal. Civ. Code §§ 1798.82(d)(1)(A-C).

51 id. at § 1798.82(d)(1)(D).

(see above). In turn, an organisation's management and directors frequently face pressure to release public statements to the media addressing the breach and any remedial steps taken. There are many facets of the communications strategy that are beyond the scope of this chapter, but from a regulatory standpoint what is critical is including in an organisation's incident response plan – and then following in the event of a breach – a tight internal coordination mechanism involving the legal and relevant global business functions to enable a measured, consistent approach to all public statements.

Data security compliance and enforcement observations

Separate and apart from the issue of notification, organisations that have experienced a data breach face a range of other potential regulatory challenges. For instance, all organisations must prepare to respond to regulatory inquiries with the potential to lead to an enforcement response, whether tied to an underlying security failure, the adequacy of the notification or some other issue. And public companies have the added challenge of evaluating whether the breach is material to their financial performance or operations and thus may be required to be disclosed to investors. As regulators across the globe gain in enforcement experience and begin to coordinate law enforcement activity with one another, organisations must increasingly be prepared to navigate the added complexities posed by these challenges when they arise in the context of multi-jurisdictional investigations of cross-border data breaches.

Data security

Many data protection laws contain provisions requiring organisations to maintain the security measures necessary to protect individuals' personal information from unauthorised access. For example, the GDPR requires that companies take 'appropriate technical and organisational measures' to ensure that data is securely stored and processed.[52] The California Consumer Privacy Act (CCPA) requires that organisations 'implement and maintain reasonable security procedures and practices' to protect California individuals' personal data.[53] And Mexico's data protection law requires that all data controllers and certain processors 'establish and maintain administrative, physical, and if applicable technical, security measures' to protect personal data.[54] These and other similar laws establish standards that data protection authorities and other enforcement agencies are increasingly using to hold organisations accountable if a data breach occurs that, in the view of regulators, should have been prevented or mitigated.

The GDPR permits regulators to pursue fines for data security violations equal to the higher of €20,000,000 or 4 per cent of an organisation's annual worldwide turnover.[55] In Brazil, the LGPD will permit regulators to pursue half that amount once the administrative sanction provision comes into force in August 2021.[56] California takes a different approach

52 GDPR, Article 5(1)(e).

53 CCPA § 1798.150(a)(1).

54 Federal Law on the Protection of Personal Data Held by Private Parties, Chapter III, Article 57. Mexico's law further identifies factors and actions that data controllers must take into consideration in determining security measures. Id. at Articles 59–61.

55 GDPR, Article 83(5).

56 See Ken Silva, 'LGPD sanctions postponed until August 2021', Global Data Review (12 June 2020), https://globaldatareview.com/coronavirus/lgpd-sanctions-postponed-until-august-2021.

and permits the state attorney general to seek civil penalties (calculated with respect to each affected consumer) of up to US$7,500 per intentional violation and US$2,500 per unintentional violation, with no maximum amount.[57] In the context of cross-border data breaches, the total amount of regulatory fines that could be imposed on an organisation by multiple enforcement authorities – and the potential for duplicative penalties given different approaches to conceptualising the fine amount and different definitions of data subjects and consumers – are both significant.

Public company disclosures

Public companies impacted by a breach face additional regulatory requirements. For instance, in the United States, the Securities and Exchange Commission (SEC) has issued interpretative guidance requiring public companies to disclose material cybersecurity incidents, including data breaches, in their public filings.[58] Even a non-material breach may give rise to a disclosure obligation where investors should be informed of potential risks the company faces. And in the European Union, the Market Abuse Regulation (MAR) requires EU-listed companies to disclose 'inside information', which potentially includes data breaches and other types of cybersecurity incidents, that directly affect their operations and the price of financial instruments.[59] Public companies thus must carefully determine both whether notification and disclosure of data breaches is required, as well as the potential impact one determination may have on the other. As the SEC's 2018 settlement with Yahoo makes clear, the issue of disclosure to investors can lead to significant enforcement consequences.[60]

The future of enforcement

Many data protection authorities around the world are still in the early phases of enforcing data protection laws and managing their budgetary constraints, and organisations will be monitoring enforcement trends closely. For instance, organisations will be watching for signs of the emerging enforcement priorities of Brazil's data protection authority once the LGPD's administrative sanctions go into effect in August 2021, and the impact of the California Privacy Rights Act, the successor to the CCPA that will divide enforcement between the California AG and a newly created data regulator when it goes into effect in January 2023, on the overall US enforcement landscape.

Organisations will also be closely watching for trends toward coordinated resolutions of enforcement actions among data protection authorities from different countries. We

57 CCPA § 1798.155(b).

58 Securities and Exchange Commission, Commission Statement and Guidance on Public Company Cybersecurity Disclosures, 83 Fed. Reg. 8166, 8168 (Feb. 26, 2018). This guidance followed earlier guidance issued by the SEC's Division of Corporation Finance in 2011. See Securities and Exchange Commission, CF Disclosure Guidance: Topic #2 (13 October 2011), www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

59 See MAR, Article 17(1); see also 'Untangling the Tangled Web of Cybersecurity Disclosure Requirements: A Practical Guide', Harvard Law School Forum on Corporate Governance (17 June 2018), https://corpgov.law.harvard.edu/2018/06/17/untangling-the-tangled-web-of-cybersecurity-disclosure-requirements-a-practical-guide/.

60 Press Release, 'Altaba, Formerly Known as Yahoo!, Charged With Failing to Disclose Massive Cybersecurity Breach; Agrees to Pay $35 Million', Securities and Exchange Commission (24 April 2018), www.sec.gov/news/press-release/2018-71.

have seen such coordination among US federal and state regulators, and within the EU, following cross-border data breaches. But while there have been examples of enforcement actions announced by multiple countries at different times in connection with cross-border data breaches (e.g., *Equifax*, *Yahoo* and *Starwood/Marriott*), it remains to be seen if and when regulators from different countries may begin to announce coordinated resolutions of the type we have come to see in corporate criminal investigations.[61] In the meantime, we anticipate debate about whether the merits of such an approach, such as encouraging cooperation among enforcement agencies and avoiding duplicative penalties for organisations, apply in the data breach context.

Conclusion

Today's complex regulatory environment presents great challenges for global organisations contending with a data breach of any magnitude. Compliance with the multitude of international breach notification laws requires an understanding of what facts may trigger statutorily mandated notice obligations and how and to whom that notice must be communicated. Even when breach notification obligations are satisfied, organisations still must be prepared to handle other regulatory challenges as well, including inquiries into security vulnerabilities that may have contributed to the breach. As more countries enact comprehensive data protection laws and cross-border data breach enforcement picks up, organisations that have breach response procedures that are carefully prepared and reflect a nuanced, global perspective will be best positioned to handle a major incident.

61 See, e.g., 'Airbus to pay $4 billion to settle bribery probes', Global Investigations Review (31 January 2020), https://globalinvestigationsreview.com/airbus-pay-4-billion-settle-bribery-probes ('Airbus has entered into the largest foreign corruption settlement of all time to resolve investigations by authorities in the US, UK and France. Courts in Paris, London and Washington, DC, each approved agreements on 31 January that total €3.6 billion ($3.9 billion) to resolve [the allegations]. The resolutions mark the end of a three-and-a-half-year joint investigation by the UK Serious Fraud Office (SFO) and France's National Financial Prosecutor's Office (PNF), as well as a parallel probe conducted by the US Department of Justice and State Department.').

5

Insurance

Richard DeNatale and Brian McDonald[1]

Insurance should be a central part of every company's breach preparedness strategy. We live in a world in which perfect security is not attainable. It has been shown time and time again that sophisticated hackers – given enough time and resources – can penetrate even the most advanced defensive systems. When breaches occur, they can result in significant costs for forensic investigations, network remediation, customer notifications, credit monitoring, legal fees, regulatory fines, etc. Most of these costs can be covered by insurance, such that an effective insurance programme can significantly reduce the financial consequences of any breach incident.

The aim of this chapter is to assist organisations and their advisers in developing an insurance programme to protect against cyber risk. Most of the chapter is devoted to cyber insurance policies, which are the most effective vehicle for covering cyber losses. We explain the major features of cyber policies, offer suggestions for the procurement process and discuss best practices for pursuing insurance claims following a cyberattack. We also review the cover available for cyber risk under other types of insurance policies and significant case law that addresses these issues.

The evolution of cyber insurance

The origins of insurance for cyber risk can be traced to the first years of the 21st century. With the explosion of the internet as a platform for commerce, businesses began looking for ways to insure the litigation risks associated with their online activities. The earliest cyber policies, labelled Tech E&O and Media E&O cover, emerged between 2000 and 2005 as a new form of professional liability insurance for companies in the technology and media sectors.

1 Richard DeNatale and Brian McDonald are partners at Jones Day who represent policyholders in cyber insurance and data breach coverage matters. They wish to thank their colleague Thilini Chandrasekera for her contributions to the second edition.

The demand for cyber insurance increased dramatically following the first wave of massive data breaches reported by US businesses between 2007 and 2009.[2] When a cyberattack resulted in theft of personal data, it was often followed by class action lawsuits by the affected consumers. Faced with these risks, corporate policyholders sought insurance that would cover a broad range of breach-related costs, including forensic expenses, notification costs, and legal fees for the defence of litigation and regulatory proceedings. Insurers responded in two ways. They began to sharply limit the cover available for cyber risk in commercial general liability (CGL), commercial property and other traditional types of insurance. At the same time, insurers accelerated the development and marketing of the modern form of cyber insurance that remains in use today.

During the past decade, there has been a rapid expansion of cyber insurance, marked by three recurring themes:

- ongoing evolution of policy forms to cover newly emerging threats, ranging from hacktivism and ransomware to attacks by nation states;
- heightened insurer involvement in breach response activities as a method of controlling costs; and
- lack of standard forms, as most insurers have developed their own policy forms using different language for key terms, conditions and exclusions.

As cyber insurance enters its third decade, we consider the lack of movement toward standard forms to be a major deficiency. Standard forms promote predictability of coverage, which benefits policyholders and insurers alike. Insurance policies are contracts that should be interpreted according to their express terms. But the multiplicity of forms, combined with the lack of governing case law, hinders the development of common understandings regarding the scope and meaning of cover. It has also contributed to an increase in claim denials as insurers sometimes adopt arbitrary interpretations of policy terms.

All these factors make it more difficult for companies to assess the adequacy of their own insurance programme. The remainder of this chapter offers guidance for policyholders and their counsel on how best to address these challenges.

2 These included breaches reported by TJ Maxx (2007), TD Ameritrade (2007) and Heartland (2009).

Major features of cyber policies

Core cover

Modern cyber policies combine third-party cover for the defence and settlement of claims with first-party cover for the policyholder's own breach-related losses.[3] Policies typically contain multiple insuring clauses that are intended to cover different categories of costs, but which in practice frequently overlap.[4] While the labels vary from insurer to insurer, most cyber policies contain the following insuring clauses.

Breach response costs

This insuring clause covers the policyholder's incident response costs, including (1) forensic consulting fees to investigate the breach; (2) legal fees paid to external counsel to coordinate the investigation and advise the company on its legal duties; (3) the cost of notifying individuals whose personal information has been compromised; and (4) the cost of providing those individuals with credit monitoring or identity theft protection services as a remedial measure.[5] While some cyber policies do not expressly reference legal fees in this insuring clause, it is commonly understood that such fees are covered as part of the cost of the forensic investigation.

An important difference among cyber policies relates to the type of information that will trigger cover under the data breach expense insuring clause. Many policies cover breach incidents involving a wide range of protected information, including personally identifiable information (PII), protected health information and confidential business information. But some cyber policies limit cover to breaches involving personal information. This is a significant shortcoming from the perspective of the policyholder, because an attack that targets confidential corporate data will result in many of the same response costs as an attack targeting PII.

Privacy liability

This insuring clause covers third-party claims resulting from a data breach or cyberattack. Covered costs include defence costs, damages and settlements. The types of claims that are covered vary from policy to policy, but generally include (1) claims by consumers for unauthorised disclosure of personal information, violation of data privacy laws, or violation of breach reporting requirements, and (2) claims by corporate customers for disclosure of confidential business information, transmission of malware or impairing access to computer networks.

The original focus of the privacy liability insuring clause was protection against claims for unauthorised disclosure of data, but as a result of recent legislative developments, companies currently face an increased risk of liability for data processing and handling practices. The European Union's General Data Protection Regulation (GDPR) and California's Consumer

3 As a general matter, first-party insurance covers loss or damage to a policyholder's own property, while third-party insurance covers lawsuits and third-party claims asserted against the policyholder.

4 The basic anatomy of an insurance policy can be described as follows: insuring clauses grant cover for the risks described in the clause, which can be stated generally ('all risk of loss or damage to property') or specifically ('property damage resulting directly from flooding'); exclusions seek to limit cover for certain risks that would otherwise be insured under the policy; definitions provide the meaning of key terms used in the insuring clauses and exclusions; conditions set forth other contractual obligations of the policyholder and the insurer; and endorsements are amendments to the basic policy form that modify the terms of cover.

5 Some cyber insurers offer cover for notification costs and credit monitoring costs in a separate insuring clause.

Privacy Act of 2018 impose new obligations on businesses relating to the collection, retention and transfer of consumer data, with violations potentially leading to civil damages and regulatory fines. Many cyber insurers have amended their policy forms to cover these types of data processing claims, and we expect others to follow suit.

Regulatory proceedings

The privacy liability insuring clause discussed above is triggered by a 'claim', which is typically defined to include complaints, arbitration notices, demand letters, or other written requests for monetary relief. In some policies, the definition of 'claim' is broad enough to include government regulatory proceedings. More frequently, cover for regulatory proceedings is offered in a separate insuring clause, which covers legal fees incurred to respond to government enquiries or investigations, amounts paid in settlement, and fines and penalties to the extent permitted by law. Some insurers make this cover optional and do not include it in their standard cyber form. In such cases, if the policyholder opts not to purchase regulatory cover, the insurer may resist efforts to seek indemnity for regulatory claims under other insuring clauses.

Network interruption

This insuring clause is modelled on the business interruption cover found in commercial property insurance policies. It insures against loss of revenue resulting from a network shutdown occasioned by a cyber incident. Such cover would be triggered, for example, when a company shuts down its network to contain a cyber intrusion or when hackers disable hardware or software applications needed to operate the network. Cover typically extends for 60 to 180 days after the shutdown occurs.

Network interruption insuring clauses also cover extra expenses incurred as a result of a cyber incident, though the scope of this cover varies widely. Some policies cover any extra expenses that would not have been incurred but for the network shutdown, while others limit cover to costs incurred to minimise lost income. In some policies, advance approval by the insurer is required. Most policies contain exclusions for costs associated with system upgrades.

Ancillary cover

Beyond these core insuring clauses, cyber insurers have developed additional optional cover to address particular risks. These ancillary clauses can be quite valuable for certain policyholders. The most important types are:

- data recovery – covers the cost of replacing or restoring data that is corrupted or destroyed in a cyberattack;
- cyber extortion – covers the costs of responding to a ransomware attack or other form of extortion;
- payment card industry (PCI) claims – covers fines and assessments imposed under the rules of the payment card brands for breaches involving credit or payment card data;
- fraudulent transfer and social engineering – covers amounts lost in fraudulent schemes to steal funds using forged emails and payment instructions; and
- technology products or services – covers third-party claims alleging defects in technology products (including software) or negligent acts, errors or omissions in the performance of technology services.

Consent provisions

The unpredictable costs of cyber claims have been a significant challenge for the insurance industry. Insurers typically price their products based on historical experience with similar claims. Because there is not yet sufficient data available for cyber policies, insurers attempt to control costs on individual claims by requiring policyholders to obtain approval for major expenditure.

Cyber policies typically require insurer consent before retaining counsel, hiring forensic consultants or other vendors; providing breach notices to affected individuals; offering credit monitoring services; or settling claims. These requirements go beyond what is found in other types of protection. Commercial property policies do not require a policyholder to obtain insurer approval before notifying stakeholders that facilities have been damaged, or before retaining contractors to carry out repairs.

The prevailing practice among most cyber insurers has been to show flexibility in applying these consent provisions. In crisis situations, it is not always possible to obtain insurer approval before retaining counsel or forensic consultants. Provided the policyholder promptly notifies the insurer of the retention and receives no objection, the consent requirement should be deemed satisfied.

From the policyholder's perspective, there should be no objection to reasonable consent requirements as long as they do not interfere with the breach response efforts.[6] By way of example, it would be unreasonable in most circumstances for an insurer to refuse to approve a policyholder's decision to notify individuals of a breach. To withhold such approval would interfere with the policyholder's duties to its customers and could expose the policyholder to legal liability.

Other terms and conditions

Like all insurance policies, cyber policies contain a host of other terms, conditions and definitions that qualify the cover in important ways. Insuring clauses often include defined terms to describe covered incidents and expenses. A standard formulation for third-party cover is that the insurer will pay for a 'loss' arising from a 'claim', so the definitions of those two terms are particularly important. From a policyholder's perspective, the definition of 'claim' should go beyond formal lawsuits and administrative proceedings to include written demand letters and informal regulatory enquiries. The term 'loss' should include defence costs, damages and settlements, as well as prejudgment and post-judgment interest, statutory damages and regulatory fines. Cyber policies generally will not cover non-monetary relief or the cost of complying with an injunction.

Policyholders should also pay close attention to financial terms relating to policy limits and retentions. Retentions in cyber policies tend to be high, particularly for larger companies and companies with a mixed record of data security. To compound the pain, some policies require payment of multiple retentions when a cyberattack triggers multiple insuring clauses. Thus, if a data breach results in a network shutdown, disclosure of PII and resulting lawsuits, the insurer may require payment of three retentions under the network interruption, data

6 Consent requirements regarding choice of counsel are discussed in the section titled 'Choice of counsel' (see page 72).

breach expense and privacy liability clauses. Policyholders should avoid, whenever possible, policies that require the satisfaction of multiple retentions.

Cyber policy exclusions

There has been a proliferation of exclusions in cyber policies, with some containing as many as 60 or 70 exclusions. Certain insurers appear to view exclusions as a way of managing risk at the micro level, making fine distinctions between fact scenarios and drafting language intended to cover some exposures but not others. This approach leads to overly complex policies that increase the risk of insurance disputes. It is in the interest of both insurers and policyholders for exclusions to be stated in simple and straightforward terms, to foster a common understanding of the risks excluded from cover.

Below, we discuss three exclusions commonly found in cyber policies that can be problematic in the event of a cyberattack.

War exclusion

The war exclusion has been a standard feature of CGL and commercial property policies for more than 100 years.[7] Over time, language has been added to broaden its scope beyond the simple paradigm of war.[8] Nonetheless, courts have consistently held that the war exclusion is limited to warfare in the classic sense of the word, namely, armed conflict between sovereign nations or their functional equivalents. *Pan American World Airways, Inc v. Aetna Casualty & Surety Co*[9] (holding that a war exclusion does not apply to violent terrorist hijacking). Random acts of violence by individuals or groups will not trigger the exclusion.[10] No reported decision has ever applied the war exclusion to a cyberattack.

Some cyber policies address this issue by expressly stating that the war exclusion does not apply to cyberattacks. Such language adds helpful clarity, but is not necessary. Even without such language, the war exclusion cannot fairly be read to apply to hostile activities carried out in cyberspace.

Contractual liability exclusion

The contractual liability exclusion bars coverage for the liability of third parties that the policyholder assumes via contractual indemnification provisions. The insurance industry tends to disfavour indemnification provisions, though they are a standard feature in business-to-business contracts. Most contracts involving the transfer, processing or storage of confidential data will contain indemnity provisions that allocate costs between the two parties in the event of unauthorised disclosure. Companies that take on indemnification obligations should delete or modify the contractual liability exclusion to ensure that their obligations are covered.

7 Stempel on Insurance Contracts, Section 24.04 (2008).

8 A typical war exclusion in a cyber policy bars cover for losses resulting from 'war, invasion, acts of foreign enemies, terrorism, hijacking, hostilities or warlike operations (whether war is declared or not), military or usurped power, civil commotion assuming the proportions of or amounting to an uprising, strike, lockout, riot, civil war, rebellion, revolution or insurrection'.

9 505 F.2d 989 (2d Cir 1974).

10 *Holiday Inns Inc. v. Aetna Ins. Co.*, 571 F. Supp. 1460, 1497 (S.D.N.Y. 1983).

Exclusion for negligent security practices

Many cyber insurers try to manage risk by reviewing their policyholders' network security practices during the underwriting process. This review can include detailed application questions and interviews with IT staff. Some cyber policies go a step further and exclude losses caused by an inadvertent failure to follow the security practices described in the application. Other policies contain exclusions for failure to implement software patches; failure to maintain current antivirus software; failure to adequately design or configure computer systems; or other errors in network security. Such exclusions run counter to one of the basic purposes of insurance – protecting policyholders from losses caused by their own negligence. Policyholders should seek to strike these exclusions from their policies whenever possible.

Procuring the right insurance

Any effort to enhance breach preparedness through insurance must begin at the time the policies are purchased. That is when policyholders, as buyers in a competitive market, have the opportunity to obtain new cover, purchase higher limits and negotiate changes in policy wording.

Yet the procurement process can be challenging for a number of reasons. Cyber policies are both relatively new and highly complex. Policyholders with no prior experience in cyber claims may not understand how key provisions will be applied. In addition, because there are no standard policy forms, it is difficult to compare the cover offered by different insurers. Finally, the nature of cyber risk is constantly changing, which requires the risk management group to remain alert to the new threats and vulnerabilities that emerge every year.

To successfully navigate these issues, we recommend that policyholders periodically conduct a detailed review of their cyber insurance programme in a collaborative process involving corporate risk management, legal and IT groups, as well as insurance brokers and specialist counsel who have experience in handling data breach claims. Together, this integrated team should work through the following framework of issues.

First, the team should develop a solid understanding of the company's current insurance programme, both to assess the adequacy of cover and to identify specific policy provisions that need improvement. The discussion in the previous section can serve as a reference point for this analysis. Specialist counsel can explain how policy terms have been interpreted in prior breach incidents, while insurance brokers can help to compare existing policies with those offered by other insurers.

Second, the team must understand the legal and regulatory environment – including the company's obligations with respect to data, the potential liabilities for violations, and the type of regulatory proceedings to which the company may be subject. The regulatory landscape can change over time, as seen by the recent enactment of the EU's GDPR and California's Consumer Privacy Act, so companies must stay abreast of developments that create new exposures.

Third, the team should have access to a risk assessment that identifies the most important cyber threats facing the business. This assessment is necessary to determine which ancillary cyber cover should be purchased. In addition, most companies face their own unique risks owing to the nature of their business operations. These risks might include a disabling attack on a critical supplier, investigations by a specific government agency, or exposure to a particular

type of claim. Where such specialised risks are not adequately covered under existing policy forms, the policyholder should try to negotiate policy endorsements to address them.

Each set of issues discussed above will change over time. An insurance programme that offered ample protection four years ago may no longer be adequate in light of new business activities or threat vectors. Consequently, this review process should take place at frequent intervals. If done correctly, it will generate a concrete list of policy enhancements to be implemented over time to build a more robust insurance programme.

Significant case law developments

Below we review the significant case law addressing insurance for cyber claims. Most of the relevant cases involve traditional types of policies, such as commercial crime and CGL. These traditional policies continue to provide cover for cyber risk, though insurers have added exclusions in recent years that sharply curtail the extent of this cover.

Commercial general liability policies

Attempts to seek coverage for cyber risks under CGL policies have focused on insuring clauses that cover property damage and personal and advertising injury.

Property damage

CGL policies provide defence and indemnity cover for claims alleging 'property damage', which is defined as: 'physical injury to tangible property, including all resulting loss of use of that property . . . [or] loss of use of tangible property that is not physically injured'.

The Insurance Services Office (ISO) amended this definition in 2001 to expressly state that tangible property does not include electronic data.[11] Under the revised definition, coverage is generally not available under CGL policies for claims alleging loss or corruption of data without additional injury.[12]

The situation may be different when a cyberattack results in corruption of data that, in turn, disables computer hardware on which the data was stored. The disabled hardware may qualify as 'loss of use of tangible property that is not physically injured' and therefore fall within the definition of property damage. For example, in *Eyeblaster, Inc. v. Federal Insurance Co.*,[13] an internet advertising business sought coverage for a customer's lawsuit alleging that his computer was infected with a spyware program. The court held that there was no coverage for the customer's claims alleging loss of data, because the policy defined tangible property to

11 The Insurance Services Office (a subsidiary of Verisk Analytics) is responsible for drafting standard forms for US insurance policies.

12 For CGL policies issued prior to this revision, courts were split on whether data constituted tangible property. Compare *Retail Sys., Inc. v. CNA Ins. Cos*, 469 N.W.2d 735, 738 (1991) (finding that computer tape and data were tangible property under the insurance policy) with *America Online v. St Paul Mercury Ins. Co.*, 347 F.3d 89, 96 (2003) (rejecting cover because tangible property does not include damage to data or software). See also *Ward Gen. Ins. Servs., Inc. v. Emp'rs Fire Ins. Co.*, 114 Cal. App. 4th 548, 556, 557 (2003), as modified on denial of rehearing (2004) (holding that the loss of a database did not qualify as 'direct physical loss of or damage to' property under the terms of a commercial property policy).

13 613 F.3d 797 (8th Cir 2010).

exclude data. However, the court found the claim was insured based on loss of use, because the customer was unable to use the computer that housed the damaged data.

A subsequent court decision applied *Eyeblaster* to reject loss of use coverage for a payment card data breach. In *Target Corp. v. ACE American Insurance Co.*,[14] policyholder Target sought coverage for its settlement liability to multiple banks following a data breach resulting in the theft of credit and debit card data. The breach necessitated the cancellation of the compromised payment cards and reissuance of new cards. The court held that loss of use did not apply because the record lacked any allegation or evidence of the value of the use of the payment cards to either customers or payment card companies. As such, the court held, the policyholder could not establish the required connection between the damages incurred to settle the claims and the value of the use of the cards.

Personal and advertising injury

Policyholders have also sought coverage under the personal and advertising injury insuring clause (personal injury clause) for data breach claims alleging disclosure of confidential personal information. The personal injury clause covers (among other things) claims alleging 'publication, in any manner, of material that violates a person's right of privacy'. Policyholders have argued that disclosure of private information in a data breach constitutes this type of covered publication. Some courts have accepted that argument, particularly where the policyholder itself inadvertently disclosed the information. For example, in *Travelers Indemnity Co of America v. Portal Healthcare Solutions LLC*,[15] a policyholder sought coverage for the inadvertent release of confidential patient records online. The court found the claim was insured based on the policyholder's negligent disclosure of information in violation of patients' privacy rights.

Other courts have rejected similar arguments. In *Innovak International, Inc. v. Hanover Insurance Co.,*[16] the policyholder sought coverage for privacy claims alleging the release of plaintiffs' private information in a data breach. The *Innovak* court ruled against the policyholder on the grounds that the hackers, not the policyholder, were the publisher of the information. The court held that cover under the personal injury clause was limited to claims alleging acts of publication by the policyholder itself.[17] This result seems questionable in light of the relevant policy language, which covered claims alleging publication 'in any manner' arising out of the policyholder's business and for which the policyholder was legally responsible.

It is important to note that in 2015, ISO introduced a new data breach exclusion for standard form CGL policies. The exclusion states that the personal injury clause does not apply to claims 'arising out of any access to or disclosure of any person's or organization's confidential or personal information'.[18] Under the broad language of this exclusion,

14 No. 19-cv-2916 (WMW/DTS), 2021 WL 424468 (D. Minn. Feb. 8, 2021).

15 35 F.Supp.3d 765 (E.D. Va 2014), aff'd 644 Fed. App'x 245 (4th Cir. 2016).

16 280 F.Supp.3d 1340 (M.D. Fla 2017).

17 The same court that decided the Innovak case reached a similar conclusion in *St. Paul Fire & Marine Insurance Co. v. Rosen Millennium, Inc.*, 377 F. Supp. 3d 1176 (M.D. Fla. 2018) (insurer had no duty to defend claim arising from data breach affecting credit card information).

18 See ISO Form CG 2 07 05 15.

insurance is no longer available under CGL policies for most data privacy claims arising from a breach incident.

Crime policies

Commercial crime policies typically cover the loss of money, securities or other business property as a result of fraud, employee dishonesty, theft and other third-party acts. Some crime policies include cover for computer fraud and fraudulent electronic transfers. Such policies may serve as a source of insurance for cyber-related claims. For example, courts have found coverage under commercial crime policies where hackers used forged emails to induce a policyholder's employee to wire funds outside the organisation.[19]

Courts have rejected coverage, however, when the particular circumstances of a loss fall outside the crime policy's insuring clause. In *Aqua Star Corp. v. Travelers Casualty & Surety Co.*,[20] hackers gained access to an email account used by one of Aqua Star's vendors. The hackers then sent forged emails to an Aqua Star employee, which purported to come from the vendor and directed the employee to change the vendor's bank account information for receiving wire transfers. The Aqua Star employee made this change, and subsequent wire transfers were made to an account controlled by hackers. The policyholder submitted a claim under the computer fraud section of its crime policy, but the court rejected the claim based on a policy exclusion for 'loss or damages resulting directly or indirectly from the input of electronic data by a natural person having the authority to enter the insured's computer system'.[21] The court noted that the Aqua Star employees who changed the vendor bank account information and sent the wire transfers had authority to use the company's computer system. According to the court, it did not matter that the employees had been deceived into taking those actions.

The *Aqua Star* case illustrates a common problem with commercial crime policies, which typically contain insuring clauses that cover specific fact scenarios. If the factual circumstances of a loss does not match the terms of the insuring clause, coverage may be unavailable. See I*nComm Holdings, Inc. v. Great Am. Ins. Co*.[22] (finding no coverage for losses arising out of fraudulent debit card redemptions); *Mississippi Silicon Holdings, L.L.C. v. Axis Ins. Co*.[23] (rejecting coverage for fraudulently induced invoice payments); *Sanderina, LLC v. Great Am. Ins. Co*.[24] (finding no coverage for fraudulent wire transfer); *Childrens Place, Inc. v. Great Am. Ins. Co*.[25] (rejecting coverage where the insured failed to follow required procedures for verifying wire transfer instructions).

19 See *Medidata Sols Inc. v. Fed. Ins. Co*., 729 Fed. App'x 117 (2d Cir 2018) (finding that use of the policyholder's email system to send a forged email purportedly from a corporate officer fell within the cover grant for 'entry of data into' or 'change to data elements' of a computer system); see also *Am. Tooling Ctr. Inc. v. Travelers Casualty & Surety Co. of America*, No. 17-2014, 2018 WL 3404708 (6th Cir 2018) (finding cover where fraudulent email induced an employee to wire funds outside the organisation).

20 719 Fed. App'x. 701 (9th Cir. 2018).

21 ibid., at 703.

22 No. 15-cv-2671-WSD, 2017 WL 1021749, at *11 (N.D. Ga. Mar. 16, 2017) (aff'd, 731 Fed. App'x 929 (11th Cir. 2018)).

23 No. 20-60215, 2021 WL 406238, at *2 (5th Cir. Feb. 4, 2021).

24 No. 18-cv-00772-JAD-DJA, 2019 WL 4307854, at *3 (D. Nev. Sept. 11, 2019).

25 No. 18-11963 (ES) (JAD), 2019 WL 1857118 (D.N.J. Apr. 25, 2019).

One additional issue courts have grappled with is the interpretation of crime policies that require 'direct' causation between the use of a computer and the loss. For example, in *G&G Oil Co. of Indiana, Inc. v. Continental Western Insurance Co.*,[26] the insurer argued that the insured's decision to pay a Bitcoin ransom to hackers in return for restored access to the insured's computer systems was an intervening cause of the loss. The Indiana Supreme Court disagreed and found that the loss resulted 'directly from the use of a computer' because the Bitcoin transfer was 'nearly the immediate result – without significant deviation – from the use of a computer'. Similarly, in *Cincinnati Insurance Co. v. Norfolk Truck Center, Inc.*,[27] the court interpreted 'directly' in a crime policy to mean 'something that is done in a "straightforward" or "proximate" manner and "without deviation" or "without intervening agency" from its cause'. Under this definition, the court found the insured's wire transfer in response to a fraudulent vendor invoice to be a covered loss.

Directors' and officers' liability

Directors' and officers' liability (D&O) policies are issued to companies to cover claims for wrongful acts against directors and officers – and often claims against the company as well. Because the term 'wrongful act' tends to be broadly defined, a D&O policy could potentially provide cover for claims arising out of cyber incidents. For example, a company or its executives could be accused of negligent supervision of operations that leads to the disclosure of PII or confidential information of corporate customers. Similarly, corporate executives might be accused of failing to provide timely notice of a breach incident. While there are no published court decisions addressing these issues, it is reasonable to believe that a D&O policy would cover such claims in the absence of an applicable policy exclusion.

Cyber policies

Cyber policies are relatively new and case law interpreting them is sparse. The few published cases that exist involve disputes about specific instances of fact rather than broad legal principles. Two of the more notable cases are discussed below.

In *P.F. Chang's China Bistro, Inc v. Federal Insurance Co.*,[28] the policyholder was a restaurant owner who suffered a data breach resulting in disclosure of customer credit card information. The owner sought indemnity under its cyber policy for PCI assessments imposed by the payment card brands. The policyholder had not purchased cover for PCI claims, so it asserted claims under insuring clauses for privacy notification, privacy liability and network interruption. The court, interpreting these insuring clauses broadly, determined that the PCI assessments might qualify as (1) costs to notify affected individuals under the privacy notification clause or (2) extra expense under the network interruption clause. The court nonetheless denied coverage for the assessments based on the contractual liability exclusion, which barred cover for 'liability assumed by any Insured under any contract or agreement'. The court found that the policyholder's liability for the assessments arose solely from its contractual agreements to indemnify the credit card servicing company.

26 No. 20S-PL-617, 2021 WL 1034982, at *16 (Ind. Mar. 18, 2021).

27 430 F. Supp. 3d 116, 130 (E.D. Va. 2019).

28 No. CV-15-01322-PHX-SMM, 2016 WL 3055111 (D. Ariz. May 31, 2016).

Travelers Property Casualty Co. of America v. Federal Recovery Services [29] arose from a dispute between the owner of fitness centres (Global Fitness) and its credit card processor (Federal Recovery Acceptance (FRA)). Global Fitness sued FRA for allegedly disrupting a planned merger by refusing to return customer credit card data until all outstanding invoices were paid. FRA's cyber policy included technology services cover, which insured FRA for claims alleging 'any error, omission or negligent act'. The court denied coverage on the grounds that the claims were based on intentional conduct rather than negligence. According to the court, the complaint alleged FRA had knowingly refused to return the customer data until its payment demands were met, and therefore did not give rise to potential liability for negligent acts.

One lesson that can be drawn from these cases is that both disputes could have been avoided if the policyholders had identified the relevant risks and purchased appropriate insurance. With respect to the *P.F. Chang* case, for example, restaurant owners face the risk of PCI assessments if customer credit card data is stolen, and should purchase cyber policies that include PCI cover.

This lesson underscores the importance of pursuing a coordinated procurement strategy (as outlined in the section 'Procuring the right insurance'). It will never be possible to predict every claim or loss a company may face in the future. But the goal of any insurance programme should be to identify the risks most likely to affect the business and then procure adequate cover to address them.

Pursuing insurance after a cyberattack

For companies that fall victim to a cyberattack, insurance policies become an important asset that can be used to fund response and remediation efforts. As with any asset, the value of a company's insurance policies can be enhanced through careful management or squandered through neglect. Companies that wait too long to focus on insurance or mishandle the claims process will reduce their ultimate recovery. Below we discuss best practices for the effective pursuit of insurance claims following a breach event.

Incident response coordination

From the outset, the pursuit of insurance cover should be closely integrated with the company's overall breach response efforts. A risk management representative should be included in the incident response team, with other key constituencies – IT, legal, finance, accounting, communications, etc. The risk management team must be kept informed regarding developments in the investigation, retention of vendors and major expenses. And management must be made aware of issues that could affect the availability of insurance. Insurance policies come with their own special requirements, which may not be well understood outside the risk management department. Sometimes these requirements run counter to other priorities for the incident response team. For example, it may be necessary to delay key decisions on the retention of vendors to allow time for communication with the insurers. Management's desire to maintain confidentiality regarding the breach investigation may conflict with the company's duty to provide information to its insurers. In most cases, there are ways to

29 156 F.Supp.3d 1330 (D Utah 2016).

reconcile these tensions, but if insurance issues are left out of the dialogue, there is a risk that decisions will be made that impair the insurance recovery.

Immediate steps

Pursuing coverage for breach-related losses requires early engagement with insurers to comply with consent requirements and respond to information requests. Policyholders therefore need to develop, as soon as possible, an insurance strategy based on a solid understanding of the coverage issues. Companies should aim to accomplish the following steps within the first two weeks after discovery of a cyber incident:

- give notice to insurers under all policies that may potentially apply – even those under which coverage may be uncertain. Under the law of many jurisdictions, policyholders cannot recover for costs incurred before the date of notice;
- put mechanisms in place to track all breach-related costs and to document all related expenditure;
- reach out to the primary insurer to establish a line of communication and discuss any required consents. Communications on consent issues should be confirmed in writing. In the early stages of a breach, it is reasonable to expect insurers to respond to consent requests within 48 hours at most. If the insurer does not respond, it may waive its right to object to the policyholder's decision; and
- prepare a strategic legal plan that summarises the available insurance, explains which costs will be covered and identifies the steps that must be taken to maximise recovery. This plan will inform communications with the insurers and assist the incident response team in making decisions that could affect the insurance recovery.

In many cases, the policyholder will retain external counsel to assist with the tasks outlined above. One of the benefits of retaining insurance lawyers is that their discussions with the company are protected from disclosure by attorney–client privilege. Note that most insurers will either retain insurance counsel on cyber claims or assign the claim to experienced managers with law degrees. This can put the policyholder at a disadvantage, particularly if it does not have prior experience with cyber claims.

Managing insurer communications

Shortly after giving notice, the policyholder should expect to receive requests from the insurers for information. These requests are often technical and detailed. The policyholder has a duty to respond to reasonable requests pursuant to the cooperation clause that is part of every insurance policy. However, it is proper – and often necessary – to manage these requests. There is no need to provide immediate responses if the work would interfere with breach response efforts or if forensic evidence is not yet available. The policyholder is generally not required to provide insurers with privileged attorney–client communications or attorney work-product. At the same time, withholding information unnecessarily is likely to be counterproductive in the long run. The policyholder has an interest in maintaining positive working relationships with its insurers, and disputes about routine information requests will make the insurance claim more difficult to resolve.

As the insurance claim progresses, the policyholder should provide regular updates to insurers about the forensic investigation, regulatory proceedings, third-party claims and

major expenditure. Communications will initially focus on the primary insurer, to consult on consent issues, settlement opportunities and breach notification. If costs are likely to exceed the primary policy limits, the policyholder should maintain communications with excess insurers as well. Failure to do so increases the likelihood that the excess insurers will second-guess decisions made by the underlying layers.

Invoices should be submitted for reimbursement promptly and regularly. Many cyber policies require that a formal proof of loss be submitted within 90 or 120 days of discovery of the incident, though these deadlines can be extended by mutual agreement. If the policyholder is required to file the proof of loss before final cost figures are available, it can reserve the right to make supplemental submissions in the future.

Areas of potential dispute

While there has been very little litigation to date regarding cyber insurance policies, disputes frequently occur during the claim process. Based on the growing number of claim denials in the past two to three years, we expect litigation to become more frequent in the future. Below we review some of the most common areas of dispute that are likely to spawn litigation in the years ahead.

Policy application

As noted in the subsection discussing 'Cyber policy exclusions', cyber policy applications typically include detailed questions about the policyholder's network security measures. The responses may become the source of disputes about coverage. It is becoming increasingly common for insurers to raise defences based on the policy application, particularly when a cyber incident occurs as a result of a failure to follow the security procedures described in the application responses. When a policyholder makes a material misrepresentation or omission in the application, the insurer may be entitled to reject the claim.[30] It would be improper, however, to reject a claim based on an immaterial error or minor inaccuracy.

Choice of counsel

Many cyber insurers seek to limit a policyholder's right to select counsel as a way to control costs. The limitations come in several forms. Some policies simply give the insurer the right to appoint counsel. Others provide that counsel should be chosen by mutual agreement between the policyholder and the insurer, but should they fail to agree, the insurer makes the final decision. A third approach is to require the policyholder to retain counsel from a panel of law firms selected by the insurer.

From the perspective of the policyholder, any restrictions on its right to be represented by skilled and loyal counsel is problematic. In the United States, most states give the policyholder the right to select counsel when the insurer is providing a defence under a reservation of rights.[31] Courts have reasoned that the prospect of a future coverage dispute creates

30 See *Admiral Ins. Co. v. Sup. Ct. (A Perfect Match, Inc.)*, 18 Cal. App. 5th 383, 389 (4th Dist 2017); *Varshavskaya v. Metro. Life Ins. Co.*, 890 N.Y.S. 2d 643, 643, 2009 N.Y. Slip Op. 09215 (2d Dep't 2009).

31 A reservation of rights allows an insurer to cover the policyholder's legal fees for the defence and investigation of a claim, while reserving the insurer's right to deny cover for any ultimate judgment, settlement or

a conflict of interest that prevents the insurer from controlling the choice of counsel.[32] The principles apply with equal force to the selection of counsel under a cyber policy. If the insurer has raised defences in a reservation of rights letter, or has not yet stated its position, the policyholder should have the right to select counsel. Insurance policy provisions that seek to negate or limit this right should be deemed unenforceable. Where possible, a policyholder should seek to add language to the policy at the time of purchase to preserve the right to select counsel. Alternatively, the policyholder should request an endorsement that approves its preferred counsel to handle breach investigations and cyber claims.

Settlement of claims

A frequent area of dispute involves the settlement of third-party claims. Most insurance policies contain provisions that require insurer consent for settlements. Policyholders may jeopardise coverage if they enter into a binding settlement agreement without first seeking insurer consent. This typically requires a candid discussion, often involving defence counsel, regarding the merits of the claim and the likely exposure. Insurers have a duty to accept a settlement if the proposed payment is reasonable in light of the risk of liability and the likely range of damages.[33] If an insurer breaches this duty, the policyholder has the option of proceeding with the settlement and then pursuing claims against the insurer to recover the cost. Before doing so, the policyholder should carefully document the insurer's failure to approve a reasonable settlement offer.

State-sponsored attacks

When cyberattacks involve state actors, insurers are sometimes tempted to assert defences based on the war exclusion, or the related civil authority exclusion. Attempts to invoke these exclusions in the context of a cyberattack should be seen as opportunistic. As discussed in the section 'Cyber policy exclusions', the war exclusion is limited to acts of military force and no published court decision has ever applied it to a cyber incident.

The civil authority exclusion bars cover for losses 'arising out of or attributable to any action of a public or government authority, including the seizure, confiscation or destruction of the Insured's computer system or data'. This exclusion is meant to apply to lawful orders by governments, acting pursuant to legal process and within the scope of their authority.[34] It does not apply to cyberattacks launched under the cloak of secrecy by clandestine agents of foreign governments.

---

indemnity payment.

32 Under New York law, '[w]here an insurer defends under a reservation of rights, the insured is entitled to retain its own counsel'. *Federated Dep't Stores, Inc. v. Twin City Fire Ins.* Co., 807 N.Y.S. 2d 62, 66 n.1, 2006 N.Y. Slip Op. 00105 (1st Dep't 2006). Under California law, the policyholder has a right to independent counsel if the actions of defence counsel can affect the outcome of a disputed cover issue. *See* California Civil Code, Section 2860; *San Diego Navy Fed. Credit Union v. Cumis Ins. Soc'y, Inc.*, 162 Cal. App. 3d 358, 375 (1984).

33 *Luria Bros. & Co., Inc. v. Alliance Assur. Co.*, 780 F.2d 1082, 1091 (2d Cir 1986) (New York law); *Kransco v. American Empire Surplus Lines Ins. Co.*, 23 Cal. 4th 390, 401 (2000) (California law).

34 See *Kao v. Markel Ins. Co.*, 708 F. Supp. 2d 472, 478 (E.D. Pa 2010) (civil authority exclusion applies 'where damage results from an act done within the scope of and in execution of a lawful order'); *Dunlap v. Illinois Founders Ins. Co.,* 250 Ill. App. 3d 563, 568 (1993) (exclusion does not apply to actions outside the scope of the official's authority).

Conclusion

As the cyber insurance market matures, claim disputes such as those described above will occur with greater frequency. Some will lead to litigation. In most cases, the outcome of such disputes will be determined by the language of the insurance policy. When the language favours the policyholder, it will have significant leverage to negotiate a successful resolution of the dispute. Such an outcome becomes much more difficult to achieve when the language is unclear or favours the insurer. All this points, once again, to the importance of the procurement process in laying the foundation for a successful insurance recovery when, inevitably, cyber incidents occur.

6

Complying with Regulatory Requirements and SEC Guidance: A Practitioner's Perspective for Working with Boards of Directors and Auditors

Michael E Liftik and Kristin S Starr[1]

Introduction

During the past several years, regulators have increasingly focused attention on public companies' cybersecurity disclosure policies, and on their responses to and reporting of cyber incidents. The result of this intensified focus is that boards of public companies and financial institutions subject to the jurisdiction of the US Securities and Exchange Commission (SEC or Commission) must carefully weigh how to best present their exposure to cyberthreats and how to react in the wake of cyber incidents. This chapter seeks to provide and review guidance regarding how companies and their directors and officers, with their counsel, can navigate the evolving cybersecurity landscape. The topics include: (1) when to contact the board and auditors, and the recommended frequency and nature of such updates; (2) the type of information auditors typically request during post-breach forensic reviews of financial controls required by the Sarbanes-Oxley Act of 2002 (SOX); (3) an overview of SEC guidance regarding boards, disclosures and insider trading; and (4) considerations regarding the content and timing of any SEC disclosure updates.

Brief history of SEC guidance on cybersecurity for public companies

The SEC began a dedicated look at cybersecurity issues and information security for public companies in 2011. In October that year, the staff of the SEC's Division of Corporation Finance issued guidance (the 2011 Disclosure Guidance) aimed at public issuers to 'provide an overview of specific disclosure obligations that may require a discussion of cybersecurity risks and cyber incidents'.[2] The 2011 Disclosure Guidance made it clear that companies and

1 Michael E Liftik is a partner at Quinn Emanuel Urquhart & Sullivan, LLP. Kristin S Starr is a former associate. The information in this chapter is accurate as at May 2019.

2 Div. of Corp. Fin. SEC, CF Disclosure Guidance: Topic No. 2 – Cybersecurity (13 Oct 2011), available at https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

their boards were required to disclose material information regarding cybersecurity risks and incidents.[3] Yet the Guidance, while an important early acknowledgement of the potential impact of cybersecurity issues on public companies, merely emphasised that the familiar materiality standard applies to cybersecurity-related issues. Specifically, the 2011 Disclosure Guidance mandated that registrants disclose existing cybersecurity risks and cyber incidents in relevant SEC filings if those incidents and risks 'are among the most significant factors that make an investment in the company speculative or risky'.[4] In making this determination, registrants were told to consider factors such as the severity and frequency of any prior cyber incidents, 'the probability of cyber incidents occurring and the quantitative and qualitative magnitude of those risks', and 'the adequacy of preventative actions taken to reduce cybersecurity risks in the context of the industry in which they operate and risks to that security, including threatened attacks of which they are aware'.[5]

In 2013, there were calls for the SEC to issue further guidance to make cybersecurity disclosures mandatory;[6] the Commission declined to do so. Instead, it began issuing company-specific guidance about what cybersecurity disclosures the company should make.[7] Additionally, in April 2013, the SEC adopted Regulation S-ID, which requires the development and implementation of identity theft programs by certain regulated financial institutions.[8]

In March 2014, the SEC held a Roundtable on Cybersecurity. In her opening remarks, Mary Jo White, then chair of the SEC, called cybersecurity 'a global threat' to 'all of our critical infrastructures, our financial markets, banks, intellectual property, and, as recent events have emphasized, the private data of the American consumer'.[9] She explained that the SEC had 'formal jurisdiction over cybersecurity', which it was using to 'directly focus[] on the integrity of our market systems, customer data protection, and disclosure of material information'.[10]

Most recently (as at the time of writing), the Commission released updated public company disclosure guidance, in February 2018, 'emphasiz[ing] that "cybersecurity presents ongoing risks and threats to our capital markets and to companies operating in all industries, including public companies regulated by the Commission"' (the 2018 Guidance).[11]

---

3 ibid.

4 ibid.

5 ibid.

6 Letter from John D Rockefeller IV, Chairman, Comm. on Commerce, Sci. & Transp. to Mary Jo White, Chair, SEC (9 Apr 2013), available at http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=49ac989b-bd16-4bbd-8d64-8c15ba0e4e51.

7 Letter from Mary Jo White, Chair, SEC, to John D Rockefeller IV, Chairman, Comm. on Commerce, Sci. & Transp. (1 May 2013), available at http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=7b54b6d0-e9a1-44e9-8545-ea3f90a40edf.

8 See 'Identity Theft Red Flags Rules', Release No. 34-69359 (10 Apr 2013), available at www.sec.gov/rules/final/2013/34-69359.pdf.

9 Mary Jo White, Chair, SEC, Opening Statement at SEC Roundtable on Cybersecurity (26 Mar 2014), https://www.sec.gov/news/public-statement/statement-3-26-14-mjw.

10 ibid.

11 'Commission Statement and Guidance on Public Company Cybersecurity Disclosures', at 2 (21 Feb 2018), available at https://www.sec.gov/rules/interp/2018/33-10459.pdf [2018 Guidance]; see also World Economic Forum Insight Report, 'The Global Risks Report 2018', at 6 (17 Jan 2018), available at http://www3.weforum.

Notably, the 2018 Guidance was issued by the Commission itself, rather than staff, which not only enhances the prescriptive value of the statement, but also serves as a marker that the Commission itself is focused on and has made cybersecurity disclosures a priority. The Commission's statement, which is discussed more fully below, provided companies with much-needed supplementary and detailed guidance as to the SEC's treatment of material cyber events.

In April 2018, the public finally saw the SEC's guidance and interpretations about these issues play out in the Commission's enforcement action against Yahoo! based on Yahoo!'s 2016 disclosures regarding 2013 and 2014 data breaches.[12] The Commission's Order detailed facts about what the SEC found deficient about Yahoo!'s disclosures. First, it found that Yahoo! materially misled investors by only disclosing potential future data breach risks, 'without disclosing that a massive data breach had in fact already occurred'.[13] Second, the SEC found fault with Yahoo!'s management discussion and analysis of financial conditions and results of operations (MD&A) as 'it omitted known trends or uncertainties with regard to liquidity or net revenue presented by the 2014 data breach'.[14] By failing to disclose these possible financial effects on revenue from a cybersecurity incident, Yahoo!'s MD&A made 'affirmative representations denying the existence of any significant data breaches in a . . . stock purchase agreement', dealing with Verizon's then-pending purchase of Yahoo!. Showing the material consequences of these events, Verizon renegotiated the purchase after learning of the data breaches, reducing the price by US$350 million. The SEC imposed a US$35 million civil penalty and issued a cease-and-desist order based on anti-fraud violations of the Securities Act and the financial reporting requirements of the Exchange Act.

While the *Yahoo*! case was the SEC's first enforcement action based on inadequate cybersecurity disclosures, the Commission added to the dialogue later in 2018 with its 'Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934 Regarding Certain Cyber-Related Frauds Perpetrated Against Public Companies and Related Internal Accounting Controls Requirements' relating to breakdowns in several companies' internal financial controls, which had allowed each company to fall victim to business email compromises.[15] The Commission identified nine issuers, who lost between US$1 million and US$30 million as a result of various forms of hacking and phishing attacks. The attacks caused the companies to make inappropriate payments to foreign bank accounts controlled

org/docs/WEF_GRR18_Report.pdf [World Economic Forum Report] (identifying cyberattacks as one of the top five global risks in terms of likelihood).

12 Order Instituting Cease-and-Desist Proceedings Pursuant to Section 8A of the Securities Act of 1933 and Section 21C of the Securities Exchange Act of 1934, Making Findings, and Imposing a Cease-and-Desist Order, *In the Matter of Altaba Inc., fld/b/a Yahoo! Inc.* (SEC, 24 Apr 2018).

13 ibid.

14 ibid.

15 SEC, 'Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934 Regarding Certain Cyber-Related Frauds Perpetrated Against Public Companies and Related Internal Accounting Controls Requirements', 2 (16 Oct 2018) [SEC Cybersecurity 21(a) Report], available at https://www.sec.gov/litigation/investreport/34-84429.pdf. The Cybersecurity 21(a) Report utilises a Commission mechanism that allows the Division of Enforcement to report on an investigation when it determines that an enforcement is not appropriate. See Securities Exchange Act Section 21(a); 15 USC Section 78u(a).

by the perpetrators.[16] The Commission concluded that the hacks exposed vulnerabilities in the companies' internal financial controls by allowing these payments to be made even though the companies had certain levels of authorisation and verification, which were followed. The report's bottom line message states:

> *internal accounting controls may need to be reassessed in light of emerging risks, including risks arising from cyber-related frauds. Public issuers subject to the [internal control provisions of the federal securities laws] must calibrate their internal accounting controls to the current risk environment and assess and adjust policies and procedures accordingly.*[17]

Financial regulations and SEC guidance

Board involvement, required disclosures and insider trading

It is evident that the SEC has adopted an increasingly vocal approach in response to the growing threats facing public companies and regulated entities in the cybersecurity field – from issuing guidance, making speeches and hosting roundtables to investigating, reporting on and charging violations stemming from cyber events. However, while cyberattacks are growing increasingly frequent, complex and widespread, there is still a dearth of laws and regulations aimed at ensuring public companies prioritise cybersecurity. The 2018 Guidance aimed to provide the most detailed view of the SEC's opinion on cybersecurity matters. But this guidance is layered on top of an existing framework of disclosure and control regimes mandated by federal securities laws. While they are not specific to cybersecurity, it is increasingly clear that the SEC expects companies to treat these requirements as if they were, and views existing internal control and disclosure regulations as sufficient tools to compel companies to address their cybersecurity obligations.

Internal control for financial reporting obligations

The SEC's most powerful financial accounting provisions, adopted more than 40 years ago, may prove to be some of the best tools for combating cyber risks and events. Provisions in the Exchange Act require certain issuers to devise and maintain a system of internal accounting controls sufficient to provide reasonable assurances that transactions are executed with, or that access to company assets is permitted only with, management's general or specific authorisation. Specifically, Exchange Act Section 13(b)(2)(B) requires certain issuers to 'devise and maintain a system of internal accounting controls sufficient to provide reasonable assurances that (i) transactions are executed in accordance with management's general or specific authorization', and that '(iii) access to assets is permitted only in accordance with management's general or specific authorization'.[18] Exchange Act Rules 13a-15 and 15d-15 require companies to maintain disclosure controls and procedures, and management must evaluate their effectiveness[19] ('A fundamental aspect of management's stewardship responsibility is to

16 See SEC Cybersecurity 21(a) Report (footnote 15), at 3 and 4.

17 ibid., at 6.

18 15 USC Section 78m(b)(2)(B), paras. (i) and (iii).

19 17 CFR 240.13a-15; 17 CFR 240.15d-15.

provide shareholders with reasonable assurances that the business is adequately controlled.')[20] These regulations are merely signposts – ultimately issuers themselves are in the best position to develop internal accounting controls that account for their particular operational needs and risks in complying with Section 13(b)(2)(B).[21] Additionally, Exchange Act Rules 13a-14 and 15d-14:[22]

> *require a company's principal executive officer and principal financial officer to make certifications regarding the design and effectiveness of disclosure controls and procedures, and Item 307 of Regulation S-K and Item 15(a) of Exchange Act Form 20-F require companies to disclose conclusions on the effectiveness of disclosure controls and procedures.*[23]

Thus, '[w]hile the cyber-related threats posed to issuers' assets are relatively new, the expectation that issuers will have sufficient internal accounting controls and that those controls will be reviewed and updated as circumstances warrant is not'.[24]

The 2018 Guidance

In this context, the 2018 Guidance stitches together the threads from prior guidance and the Exchange Act's internal and disclosure control regimes to directly apply those regulations to cybersecurity risks and events.

Maintaining comprehensive disclosure and internal financial controls

The issuance of the 2018 Guidance established that, for public companies, key elements of enterprise-wide risk management includes managing cybersecurity risk policies and procedures and the adherence of those policies to federal securities laws.[25] The 2018 Guidance encourages companies 'to adopt comprehensive policies and procedures related to cybersecurity and to assess their compliance regularly, including the sufficiency of their disclosure controls and procedures as they relate to cybersecurity disclosure', and to:

---

20 S. Rep. No. 95-114, at 8 (1977) (1977 Senate Report); see also 'Promotion of the Reliability of Financial Information and Prevention of the Concealment of Questionable or Illegal Corporate Payments and Practices', Exchange Act Release No. 15570, at 6 (15 Feb 1979) (adopting release) ('An equally important objective of the new law . . . is the goal of corporate accountability.').

21 See 1977 Senate Report, at 8 ('management must exercise judgment in determining the steps to be taken, and the cost incurred, in giving assurance that the objectives expressed, will be achieved.'); The Council of Economic Advisers, 'The Cost of Malicious Cyber Activity to the U.S. Economy', at 45 (Feb 2018), available at https://www.whitehouse.gov/wp-content/uploads/2018/02/The-Cost-of -Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf ('Private firms are ultimately in the best position to figure out the most appropriate sector- and firm-specific cybersecurity practices.'); 2018 Guidance (footnote 11), at 4 and 5 ('In addition, the Commission believes that the development of effective disclosure controls and procedures is best achieved when a company's directors, officers, and other persons responsible for developing and overseeing such controls and procedures are informed about the cybersecurity risks and incidents that the company has faced or is likely to face.').

22 17 CFR 240.13a-14; 17 CFR 240.15d-14.

23 2018 Guidance (footnote 11), at 20.

24 See SEC Cybersecurity 21(a) Report (footnote 15).

25 2018 Guidance (footnote 11), at 18.

> *assess whether they have sufficient disclosure controls and procedures in place to ensure that relevant information about cybersecurity risks and incidents is processed and reported to the appropriate personnel, including up the corporate ladder, to enable senior management to make disclosure decisions and certifications and to facilitate policies and procedures designed to prohibit directors, officers, and other corporate insiders from trading on the basis of material non-public information about cybersecurity risks and incidents.*[26]

As a result, the 2018 Guidance stated plainly for the first time that the requirement of assessing the effectiveness of internal and disclosure controls must also include cybersecurity internal controls:

> *These certifications and disclosures should take into account the adequacy of controls and procedures for identifying cybersecurity risks and incidents and for assessing and analyzing their impact. In addition, to the extent cybersecurity risks or incidents pose a risk to a company's ability to record, process, summarize, and report information that is required to be disclosed in filings, management should consider whether there are deficiencies in disclosure controls and procedures that would render them ineffective.*[27]

The 2018 Guidance explained that even in designing and evaluating disclosure controls and procedures pursuant to Exchange Act requirements, companies should consider how their controls and procedures mandate the detailing and processing of information relevant to cybersecurity risks and incidents that must be disclosed in filings.[28]

Therefore, good corporate governance dictates that companies should strongly consider conducting forensic assessments of internal and external cyberthreats and of a company's cybersecurity systems. This process, which should be iterative and routine, gives management the confidence it needs to make the necessary assessments and certifications required under the federal securities laws, and to satisfy the 2018 Guidance.

Satisfying disclosure obligations

The standard for disclosure of cybersecurity risks and incidents remains 'materiality' under the 2018 Guidance. Thus, companies are directed to consider the materiality of such threats and events when preparing requisite disclosures in registration statements under the Securities Act or the Exchange Act, and the periodic and current reports under the Exchange Act.[29] It is perhaps not surprising that the regulations governing the content of both Securities Act and Exchange Act registration statements and periodic reports and proxy statements required by the Exchange Act – generally found in Regulation S-K[30] and Regulation S-X[31] – do not directly refer to cybersecurity risks or incidents.[32] However, the 2018 Guidance clarifies that

26 ibid., at 18 and 19.
27 ibid., at 20 (emphasis added).
28 ibid., at 19 and 20.
29 ibid., at 7.
30 17 CFR part 229.
31 17 CFR part 210.
32 2018 Guidance (footnote 11), at 7 and 8.

these requirements should be read to require disclosure of material cybersecurity-related issues. Companies also have a general requirement under Exchange Act Rule 12b-20 to disclose any other material information that is needed to ensure that the required statements are not misleading.[33] Today, cybersecurity risks must clearly be included within the scope of compliance with this rule as well.

In determining its disclosure obligations then, a company must carefully assess the potential materiality of any identified cyber risk and the importance of any information that is compromised by an incident. This assessment should consider the nature and the extent of the risk or incident, and the degree of harm to a company's 'reputation, financial performance, and customer vendor relationships, as well as the possibility of litigation or regulatory investigations or actions'.[34] The SEC has recognised that such determinations can take time, and notes that it does not expect 'detailed disclosures that could comprise [a company's] cybersecurity efforts' by disclosing 'specific, technical information about their cybersecurity systems, the related networks and devices, or potential system vulnerabilities in such detail as would make such systems, networks, and devices more susceptible to a cybersecurity incident'.[35] Instead, the Commission 'expects companies to disclose cybersecurity risks and incidents that are material to investors, including the concomitant financial, legal, or reputational consequences' and to do so in a timely manner.[36]

Updating the board and auditors: when, what and who

If a company identifies a serious cyber risk, the company must work to determine how best to disclose the risk to its investors and board members and how to prevent the risk from materialising. If a company identifies not just a risk but an incident, the calculations change and the pressure intensifies as the company must properly contact all stakeholders while in the midst of a crisis. 'Given the frequency, magnitude and cost of cybersecurity incidents, the Commission believes that it is critical that public companies take all required actions to inform investors about material cybersecurity risks and incidents in a timely fashion, including those companies that are subject to material cybersecurity risks but may not yet have been the target of a cyber-attack.'[37] Sufficient advance planning, including well developed incident response plans, table-top exercises and crisis communications flow charts, is critical for companies to mitigate disclosure risks in the face of cyber events.

Management also needs to take substantive responsibility to ensure its board is adequately informed about how the company is dealing with cybersecurity risks and incidents. The federal securities laws require a company to disclose the extent of its board of directors' role in overseeing risk, such as how the board administers its oversight function and the effect this has on the board's leadership structure.[38] Thus, disclosure of material cybersecurity risks and

33 Rule 408 of the Securities Act [17 CFR 230.408]; Rule 12b-20 of the Exchange Act [17 CFR 240.12b-20]; and Rule 14a-9 of the Exchange Act [17 CFR 240.14a-9].

34 2018 Guidance (footnote 11), at 10 and 11.

35 ibid., at 11.

36 ibid., at 11 and 12.

37 ibid., at 4.

38 See, e.g. Item 407(h) of Regulation S-K and Item 7 of Schedule 14A (17 CFR 229.407(h); 17 CFR 240.14a-101 – Schedule 14A).

incidents should include a discussion about the board's role in managing and overseeing such risks and incidents.[39]

Notifying the board

Once a risk or incident is identified, it is vital to maintain transparency with the board of directors as the threat or event evolves so that the board can best exercise its external and internal oversight function. Not only does board notification ensure proper public messaging, but it is necessary for the board to fulfil its legal duties to the company and ensure the company's adherence to SEC reporting requirements.

Disclosures to the board should occur soon after what is deemed to be a material (or potentially material) risk or incident, in view of the directors' duties to the company, which include the duty to obey the law, to fulfil the Caremark [40] duties of loyalty and care, and to assure, in good faith, that the company has a satisfactory information and reporting system. From the latter, it is within the purview of directorial duties to make sure the company has developed and implemented appropriate cyber risk management policies and vigorous security systems.

Working with auditors

The Commission will expect a company, as a best practice, to maintain a close and open relationship with its auditors. This expectation directly ties into Section 404(b) of the Sarbanes–Oxley Act of 2002, which requires a public company's auditor to report on management's assessment of its internal controls, and attest to the accuracy of the company management's assertion that internal controls are in place, operational and effective in the same report as the one detailing management's assessment.[41] To help auditors with this task, companies should understand how auditors will assess the fidelity of corporate systems that contain data relevant to financial reporting and internal control requirements. As part of their testing and reviews, auditors often request information about the relevant information technology systems that could potentially affect a company's reporting of financial results. To facilitate these reviews, companies should consider developing, reviewing and maintaining a list of those systems that record, interact with or could affect a company's financial books and records or internal controls over financial reporting. Perhaps equally as important is maintaining a list of the credentials for each critical financial reporting related system. Ensuring that the auditors have a working understanding of the information technology environment of a company's key financial controls systems may foster the cooperative relationship between management and the external auditors.

In the context of a breach response, auditors will be highly focused on whether the breach extended to the information technology systems associated with financial reporting. Thus, while understandably much of the company's focus at such a time will be on the systems that were known to have been compromised, halting and remediating the breach, and performing a root cause analysis, an auditor's task is different. The auditor will be focused on ensuring

39 2018 Guidance (footnote 11), at 18.

40 *In re Caremark Int'l Inc. Derivative Litig.*, 698 A.2d 959 (Del. Ch. 1996).

41 Sarbanes–Oxley Act of 2002, Section 404(b).

that the company's financial reporting controls have not been compromised. This exercise may require establishing the negative – that these systems were not affected by the breach, which can present a unique forensic challenge. Here, both the auditor and management should be able to leverage earlier work done to understand the relevant systems and environment, particularly if there was a breach of such a system, so that the auditors can readily understand the information it contained and how the breach may have affected not only that system but the overall financial control environment. Ultimately, companies should expect auditors to seek to prove that certain sensitive information was not affected by the breach before they certify the internal financial systems according to SOX requirements.

Large audit firms also employ cybersecurity experts and may draw from that expertise in making such an assessment as it relates to cybersecurity risk controls; likewise, companies should consider whether they have sufficient expertise within their own ranks to meet this requirement. At a minimum, it is in a company's best interest to maintain a close and informed relationship with its auditors.

Importantly, it remains an open question as to whether it is necessary for public companies to employ an individual with cybersecurity expertise on the board. For example, the Commission has questioned whether boards of directors 'have been doing enough to oversee risk management within their companies' particularly in the area of 'ensuring the adequacy of a company's cybersecurity measures' – 'a critical part of a board of director's risk oversight responsibilities'.[42] Thus, boards must ask themselves, just as they have members with accounting expertise to serve on the audit committee who bring appropriate oversight to the company's chief financial officer and finance function, whether they have sufficient cybersecurity expertise to oversee the chief technology and information security officer and his or her functions within the company. To address this concern, companies may consider creating a separate independent risk committee on the board (already required for large financial institutions by the Dodd–Frank Act) and moving the risk oversight function from the purview of the board audit committee to this risk oversight committee.[43] Additionally, companies should ensure they have the appropriate personnel to engage in effective cyber risk management and assessment. This may involve engaging auditors or experts, or implementing full-time board-level personnel focused on cybersecurity issues to help prevent and mitigate the effects of cyberattacks.

Providing updates to the SEC: what to say and when

Although, as noted above, the SEC recognises that it takes time to determine the severity and consequences of a cyber incident, the 2018 Guidance is notable for its emphasis on the need to disclose incidents promptly, even before the company understands the full scope of an attack. The Commission stated 'we recognize that a company may require time to discern the implications of a cybersecurity incident . . . [and] that it may be necessary to cooperate

42 Luis A Aguilar, SEC, 'Boards of Directors, Corporate Governance and Cyber-Risks: Sharpening the Focus' (10 Jun 2014), available at http://www.sec.gov/News/Speech/Detail/Speech/1370542057946.

43 For the government corollary of this principle, see Executive Office of the President, Office of Management and Budget, OMB Circular No. A-123, 'Management's Responsibility for Enterprise Risk Management and Internal Control' (15 Jul 2016), available at https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2016/m-16-17.pdf.

with law enforcement'.[44] And yet, the Commission has also stated – no doubt in response to accepted orthodoxy – that 'an ongoing internal or external investigation—which can often be lengthy—would not on its own provide a basis for avoiding disclosures of a material cybersecurity event'.[45] Notably, companies and their counsel should expect that the SEC, whether raised in the context of the Division of Corporation Finance review process or a Division of Enforcement inquiry, will investigate the determination of materiality and the company's knowledge at the time of the incident. This will involve questions from SEC staff relating to what senior management and the board knew, when they knew it, and how materiality was assessed in light of all the relevant facts and circumstances, including but not limited to prior cyber incidents and breaches. Finally, an initial disclosure is not enough – companies should focus on whether their disclosures need to be updated over time as the financial consequences of the incident are quantified and other consequences emerge, and whether the prior disclosures must be corrected.[46]

Conclusion

As the cybersecurity threat landscape evolves, so too must companies' approach to disclosure. It is clear that management and boards will be expected to maintain high standards by regulators and investors. Gone are the days of professing shock and disappointment when cyber events occur – companies today will be judged on the quality and timeliness of their response, their efforts at defence and, perhaps most critically for the SEC, whether the disclosures accurately disclosed the material risks and material events.

44 2018 Guidance (footnote 11), at 12.

45 ibid.

46 ibid.

7

Cyber and Data Privacy Due Diligence

Megan Gordon, Daniel Silver, Benjamin Berringer and Brian Yin[1]

Introduction

On 25 July 2016, Verizon Communications announced that it would pay US$4.83 billion in cash to purchase Yahoo! Inc.[2] Seven months later, that price was cut by US$350 million and Yahoo! agreed to pay 50 per cent of any costs relating to government investigations and private litigation relating to historic data breaches.[3] The reason for the change? Verizon identified two massive undisclosed data breaches during its due diligence, which dramatically changed the value of the transaction.

The Yahoo! transaction highlights an increasingly important aspect of due diligence in today's data- and technology-driven society: cyber and data privacy due diligence. These topics, which were once peripheral to a transaction, have become critical. This chapter discusses some of the key issues that practitioners should consider when analysing a company's cybersecurity and data privacy practices, including pre-diligence steps, commonly requested diligence items and potential red flags that may signal the need for additional scrutiny.

Overview of cyber due diligence

A critical aspect of any transaction is due diligence. During this process, a purchaser or investor (the Buyer) will typically conduct an in-depth review of the corporation to be acquired (the Target) to accurately value the transaction. This due diligence will also form the basis of the representations and warranties that the Target will include in the transaction documents.

---

1 Megan Gordon and Daniel Silver are partners and Benjamin Berringer and Brian Yin are associates at Clifford Chance US LLP.

2 Verizon, 'Verizon to acquire Yahoo's operating business' (25 Jul 2016), https://www.prnewswire.com/news-releases/verizon-to-acquire-yahoos-operating-business-300303133.html.

3 Verizon, 'Verizon and Yahoo amend terms of definitive agreement' (21 Feb 2017), https://www.prnewswire.com/news-releases/verizon-and-yahoo-amend-terms-of-definitive-agreement-300410420.html. The revised agreement's cost-sharing provision excluded investigations by the Securities and Exchange Commission.

Preparing for diligence: diligence requests

Due diligence, including cyber and privacy due diligence, is not a one-size-fits-all exercise – the Buyer needs to have a basic understanding of the Target's business to focus on key issues. For example, if a Target only does business with other corporations, due diligence focusing on the protection of personally identifiable information (PII) and credit card information is less important than due diligence focusing on the protection of trade secrets. Conversely, data privacy issues are more important for a consumer-facing Target that collects significant PII. As a result, Buyers should consider the nature of the Target and its data to properly scope and focus due diligence. The following are some of the issues to consider:

- Industry. In the United States, unlike in Europe, cybersecurity and data privacy are not subject to a single overarching regulatory and statutory framework. Instead, the requirements will vary depending on the specific industry. Therefore, for certain industries, such as healthcare and financial services, it is important that diligence questions focus on the requirements that are unique to those industries.
- Customer profile. Having a well-developed understanding of a Target's customer base prior to conducting due diligence is also important. By identifying the Target's typical customers (e.g., individuals, other corporations, the government), the Buyer can focus diligence requests on the typical data privacy and cybersecurity issues that arise in companies with the identified customer profile. In particular, companies that provide data processing services to other entities will likely have contractual obligations related to data protection and privacy.
- Location. As discussed in more detail in Chapter 12, a Target located in the European Union or that does business with EU customers is likely to be covered by the General Data Protection Regulation (GDPR) and therefore should be subjected to more scrutiny given the large penalties that are authorised under the GDPR.[4] Companies can also be indirectly affected by the GDPR if they receive data from companies in the EU, due to the GDPR's cross-border transfer restrictions. Similarly, in the United States, the states in which the company does business can have significant impact on what privacy obligations the company has, such as whether the company is subject to the California Consumer Privacy Act (CCPA).[5]
- Data collection practices. Understanding the data that a Target typically collects and how it is collected will allow a Buyer to better understand the Target's data privacy and cybersecurity risks. Care should be taken in analysing any Target that collects a significant amount of PII or receives credit card information.
- Previous cybersecurity incidents. A review of historic cybersecurity incidents can help a Buyer understand whether a Target has system vulnerabilities or inadequate policies and procedures, which may indicate that there are unidentified risks related to the Target. Certain documents (such as policies and procedures) may warrant more scrutiny for a

4 A company that is found to have violated the General Data Protection Regulation is subject to penalties of €20 million or 4 per cent of the company's global annual revenue, whichever is greater. See Article 84, Regulation (EU) 2016/679 (the General Data Protection Regulation [GDPR]).

5 The CCPA became effective in 2020 and applies to companies that do business in California and meet certain thresholds (annual global revenue over US$25 million, process information of 50,000 or more California residents, or derive over 50 per cent of their annual revenue from selling personal information).

Target that has a history of cybersecurity breaches and other incidents, and in some cases the Buyer may want to engage in careful technical diligence of the Buyer's system.

These initial observations will serve two purposes. First, it will allow the Buyer to tailor its due diligence requests to the specific Target by identifying issues that are likely to be most important to the review. Second, it will allow the Buyer to identify at an early stage the biggest risks to the transaction and ensure that those risks are specifically analysed during the due diligence review. The following are some of the key risks that can be identified in the process:

- Financial industry. Cybersecurity in the financial sector has been an increasing area of focus for US and state regulators. Therefore, cyber diligence should be a specific area of focus for these entities. This diligence should consider whether, for example, the financial institution complies with the New York Department of Financial Services (NY DFS) cybersecurity regulations[6] and the Gramm-Leach-Bliley Act (GLBA)[7] and implementing regulations such as the Security and Exchange Commission's (SEC) Regulation S-P[8] and the Interagency Guidelines Establishing Information Security Standards,[9] as applicable.
- Healthcare industry. Targets in the healthcare industry may be subject to laws that specify data protection requirements for that sector, such as the Health Insurance Portability and Accountability Act (HIPAA)[10] and the Health Information Technology for Economic and Clinical Health Act (the HITECH Act).[11]
- Government contractors. Government contractors are subject to a variety of cybersecurity requirements, the most prominent of which is the National Institute of Standards and Technology's (NIST) Special Publication No. 800-171 (Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations).[12] Federal govern-

6 Among other requirements, the New York Department of Financial Services (NY DFS) cybersecurity regulations require that regulated entities carry out a risk assessment in accordance with written policies and procedures, which must include: (1) criteria for evaluation and categorisation of threats; (2) criteria for assessment of confidentiality, integrity security and availability of the DFS-licensed entity's information systems and non-public information; and (3) requirements describing risk mitigation or acceptance. Regulated entities must also maintain systems that are designed to reconstruct material financial transactions and keep audit trails designed to detect and respond to a cybersecurity event that has a reasonable likelihood of materially harming any material part of the normal operation of the entity. See NY Comp. Codes Rules & Regs Title 23, Section 500.

7 15 U.S.C. Section 2801, et seq.

8 Regulation S-P requires covered entities to have policies and procedures to address the protection of customer information and records. Regulation S-P, 17 CFR Section 248.30.

9 The Interagency Guidelines Establishing Information Security Standards establish standards for administrative, technical, and physical safeguards to ensure the security, confidentiality, integrity and proper disposal of customer information. 12 CFR Part 30, app. B (OCC); 12 CFR Part 208, app. D-2 and Part 225, app. F (Board); 12 CFR Part 364, app. B (FDIC); and 12 CFR Part 570, app. B (OTS).

10 The Health Insurance Portability and Accountability Act [HIPAA] Security Rule and the HIPAA Privacy Rule require the adoption and maintenance of reasonable and appropriate administrative, technical and physical safeguards for protecting personal health data. See HIPAA Security Rule, 45 CFR Section 160, 164; HIPAA Privacy Rule, 45 CFR Sections 160, 164.

11 The Health Information Technology for Economic and Clinical Health Act [HITECH] Act strengthens the civil and criminal enforcement of HIPAA rules that protect health information transmitted electronically. See HITECH Act, 42 USC Section 300jj et seq., Section 17901 et seq.

12 See NIST, Special Publication No. 800-171, Rev. 2 'Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations' (28 January 2021), https://csrc.nist.gov/publications/detail/sp/800-171/

ment contractors may be required to implement all (Department of Defense contractors and subcontractors) or some (all other federal agency contractors and subcontractors) of the requirements in this standard.

- Companies that conduct transactions with credit cards. Any company that collects and processes credit card information is likely required to comply with the Payment Card Industry Data Security Systems (PCI DSS).[13]
- Companies with EU customers. The GDPR, which took effect in May 2018, is a sweeping EU data privacy law with broad extraterritorial effect that aims to protect the personal data of EU residents.[14] Companies with EU customers may be in scope of the law or affected by some of its provisions if they process personal data of EU individuals or receive data from EU entities subject to the GDPR.

Using this information, the Buyer can determine a materiality threshold for its diligence process. This materiality threshold is likely to take into account financial, litigation and reputational risk and reflect the Buyer's appetite for risk and the importance of the Target's data and IT assets to the value of the transaction overall. For example, diligence on a Target that collects significant PII is likely to have a lower materiality threshold for data breaches – which could cause significant litigation and reputational risks – than diligence on a Target that has little PII. Whatever the materiality threshold, it is important that the Buyer communicates this threshold to the diligence team as well as the Target. Furthermore, a Buyer should periodically re-evaluate the project's materiality threshold in light of changes in the value of the deal or information uncovered during the diligence process.

Once the Buyer has assembled this information, the next step in the process is to make information requests. These requests are aimed at allowing the Buyer to fully understand the Target's cybersecurity and data privacy policies. The goal is to ensure that at the end of the diligence process the Buyer has:

- analysed any pre-existing data breaches or other actual or threatened data security- or privacy-related enforcement or litigation;
- understood the PII that the company collects;
- identified sensitive data and data assets;
- evaluated the seller's cybersecurity and compliance infrastructure;
- analysed the adequacy of the Target's cybersecurity and privacy policies and procedures, including penetration testing, vulnerability assessments and corrective follow-up; and
- identified cyber- and privacy-relevant terms of vendor and customer contracts, especially with respect to any indemnification provisions relating to cyber or privacy incidents.

rev-2/final.

13 The Payment Card Industry Data Security Systems [PCI DSS] applies to all companies that store, process or share cardholder data and consists of technical and operational practices required for systems that store and use this data. See Payment Card Industry Security Standards Council, Data Security Standard: Requirements and Security Assessment Procedures, Version 3.2.1 (May 2018), https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf (note: users may first need to accept Ts & Cs of website).

14 Regulation (EU) 2016/679.

As has been discussed, these requests should consider information that the Buyer already has about the Target. For example, if the Target is a financial institution, these requests will need to address the specific documents that the Target is required to have under the NY DFS regulations and the GLBA Safeguards Rule and Interagency Guidelines.[15] Similarly, diligence on a government contractor should request documents establishing compliance with NIST and other government-mandated standards. Meanwhile, requests to Targets that process credit card transactions may focus on PCI DSS requirements.[16]

In addition to these targeted requests, the Buyer should also ask for information about any historic data breaches, data-related customer or regulatory complaints, enforcement matters or litigation; the Target's cybersecurity and privacy policies and practices; copies of any existing documents describing the Target's compliance with applicable laws; documents describing any third-party testing of the Target's cybersecurity and data privacy practices; and any other existing documents describing the Target's cyber policies and practices. The Buyer should also consider whether the Target currently has cybersecurity insurance. As diligence is conducted, observations and findings should be cross-referenced, where possible, against both the Target's documents and industry standards. Any discrepancy will be noteworthy, not necessarily as a red flag, but as a subject that requires further diligence to ensure that the deviation does not affect the Target's valuation or raise concerns about potential future liabilities.

Finally, to complement the Buyer's targeted diligence requests, a Buyer can obtain some baseline information about a Target by reviewing its website and other background information that is publicly available. This could not only uncover relevant documents such as online privacy policies or major data breaches or enforcement actions, but also provide clues to inform the diligence process. For example, a Buyer should take care to consider the CCPA if the Target has offices in California. Similarly, a commercial site that appears to offer localisation for the EU (e.g., prices in EU currencies, language preferences) may provide clues that the GDPR will apply.

Conducting the diligence: policies and procedures

Cyber and data privacy policies and procedures are critical documents to review during due diligence. Depending on the Target, there may be a variety of policies and procedures relating to these topics, including policies regarding security controls, data access and confidentiality, data retention, cyber incident response, disaster recovery, rights of data subjects, data disclosure and sharing, acceptable use of company-issue devices and the use of social media.

These policies and procedures come in a wide variety of forms. Some Targets may have separate policies that are internal-facing and external-facing; for example, a company may have a privacy policy that is published on its website as well as a more detailed internal privacy policy in the company handbook. There may also be different policies and procedures for data of different data subjects; for example, a company may have separate retention policies for existing customer data, prospective customer data and employee data. Similarly, a Target company comprised of multiple divisions or units carrying on separate businesses may have

15 e.g., the NY DFS cybersecurity regulations requires covered entities to have: written policies approved by the board of directors that describe the cybersecurity programme in place to protect consumers' private data; records of risk assessments; audit trails; and various notices and certifications submitted to the superintendent.

16 The PCI DSS consists of 12 broad requirements that make up six groups entitled 'control objectives'.

different policies and procedures that need to be analysed separately. These variations are immaterial, so long as the Target has policies and procedures in place that, as a minimum, are reasonable and comply with the Target's contractual and legal obligations.

The Buyer should have a checklist of the policies and procedures that they expect to see prior to beginning this review. This checklist will be informed by the Buyer's pre-diligence analysis regarding the Target's industry, the types of data that are likely to be held and the Target's customer profile. Using that checklist, the Buyer should aim to make, as a minimum, the following determinations about those policies and procedures.

Do the policies and procedures exist?

Lack of policies is typically a red flag that may warrant re-evaluating the Target's purchase price and may require disclosure in any purchase agreement.

Are the policies and procedures adequate?

This evaluation should consider not only relevant laws and regulations but also industry best practices, contractual obligations and public representations (e.g., whether internal policies and procedures align with public-facing privacy notices or past statements on the Target company's data practices). Attention should be given to Targets that are in one of the US industries, such as healthcare, that are subject to higher data protection standards. The evaluation should further consider whether the policies and procedures are based on a comprehensive risk assessment of the company or appear to be off-the-shelf policies that do not address the Target's risk profile.

As part of this process, the diligence team should also review historical policies and procedures to determine whether there is any legacy risk of complaints or violations.[17] In that regard, how often the Target's policies and procedures are reviewed and updated can serve as an indicator of the attention the Target pays to data protection. Generally, policies and procedures should be reviewed annually to ensure they remain adequate for the company in light of any changes to its legal or contractual obligations as well as any new risks or vulnerabilities identified (e.g., as a result of a new business initiative). Some policies may also have internally mandated review cycles. Outdated policies and procedures, in particular policies and procedures that pre-date significant legislative developments, may be a red flag that warrants investigation and remediation.

How does the Target collect and store PII?

Increasingly, one of the biggest risks that corporations face is a data breach that exposes customer PII. Therefore, diligence needs to ensure that the Target is only collecting PII with customer consent (where required), that the Target is taking steps to delete unnecessary historical PII and that the Target is using appropriate safeguards to store the PII. In this regard, it is important to note that Targets subject to the GDPR or US state laws such as the CCPA must have certain policies and procedures in place to fulfil requirements under these laws.

17 There are no general laws in the United States that require such records to be maintained. However, failure to maintain these records may be a red flag, depending on the standards and best practices of the Target company.

What steps does the Target take to protect special categories of sensitive data?

Specifically, the Buyer should ensure that the Target has taken reasonable steps to protect any special categories of sensitive data (such as healthcare or financial data) that it holds from unauthorised internal or external access. As part of this process, the Buyer should also evaluate how the seller has identified special categories of sensitive data and whether this identification is over- or underinclusive.

As part of its review of policies and procedures, the Buyer should also request related documents, such as cyber-focused risk assessments, testing records and training logs. These records can serve a variety of purposes; for example, risk assessments may help to identify areas of concern and vulnerability, or help to identify and mitigate legacy risks. Similarly, penetration testing and employee training records, audits and other evaluations can identify any specific historic problems at the Target and provide insight into the attention (or lack thereof) the company has historically paid to cybersecurity and data privacy issues.

Once the Buyer has completed its review of the Target's policies and procedures and related documents, it will need to consider whether and how any red flags that have been identified can be mitigated. One of the most common data privacy and cybersecurity representations that is included in a purchase agreement is that the seller or Target has adequate policies and procedures relating to its processing of personal data and that these policies comply with applicable laws and regulations, as well as any other obligations the company may have from service agreements, industry standards, or public-facing disclosures and communications. A less common representation may go further and state that the seller has made all current and past versions of its policies and procedures available to the Buyer. To the extent that due diligence findings do not support these representations, the Buyer should ensure that these issues are included on any disclosure schedule.

Cyber diligence: historical exposure to cybersecurity and data privacy incidents

Understanding historical cyber and data privacy events is also a major area of focus in due diligence.

First, the Buyer needs to understand whether there are any pre-existing risks from an earlier breach or whether there are undisclosed breaches.

Second, the Buyer needs to recognise that companies are increasingly vulnerable to consumer complaints about how their data is handled. For example, the GDPR gives all data subjects in the European Union the right to file a complaint with an empowered regulatory authority or to bring a private suit against companies who do not honour their rights.[18] The United States has lagged in this regard, but it is catching up quickly with state laws such as the CCPA[19] and increasing popular support for a federal law.[20]

18 Article 77, GDPR.

19 The CCPA became effective and enforceable in 2020 and provides California consumers with certain privacy rights. However, there is no private right of action, so only the state regulator can bring enforcement actions. In early 2021, Virginia passed its own law, the Consumer Data Protection Act, which will become effective in 2023. Other states are considering similar legislation.

20 As at March 2021, there is not yet any federal privacy law, but there is significant support for such legislation and several draft bills under consideration by the US Congress, including at least one version with a private right of action.

In this environment, Buyers need to understand the risks of past or future data breaches to adequately value the potential liability that they are acquiring from the Target, as well as the steps that the Buyer can take to mitigate that liability. This diligence typically includes evaluating any complaints against the company (including notices of violations and investigations) by individuals and regulatory authorities. The diligence team should also review any incident logs that are available, because the frequency of cybersecurity incidents (whether successful or not) can provide insight into whether the company and its data systems are common targets. Diligence should also include public records searches to identify whether the Target has been subject to any relevant allegations regarding cybersecurity. In addition, this review should be informed by the processes and procedures through which the Target detects, monitors and responds to cybersecurity incidents.

The Buyer should also consider complaints and notices of violations relating to other data privacy issues, such as the failure to respect a data subject's access rights or non-compliance with restrictions on data sharing. The existence of such complaints may identify an undisclosed liability, while the frequency of violations and complaints can inform the Buyer about the customers (and other data subjects) it is acquiring with the Target. Finally, the Target's response to such incidents can be a useful data point for understanding the Target's culture of compliance with cybersecurity and data privacy requirements.

Once the diligence review is complete on this area, the Buyer can protect itself from undisclosed liabilities by adding robust representations and warranties to the purchase agreement. A representation that the Target is not aware of any cybersecurity or data privacy incident (whether successful or not) will provide comfort to the Buyer that it understands the risks before the purchase is finalised. It is important to understand, however, that this representation does not protect against undetected breaches or unknown complaints. In addition, in some circumstances sellers may insist that these representations are limited by a specific look-back period, such as three or five years. This is one reason why thorough diligence on a company's policies and procedures is so important – a company with a culture of robust cybersecurity policies and effective monitoring is less likely to have undiscovered issues.

Conducting diligence: contractual obligations and liabilities

Another area the Buyer should consider is whether the Target has contractual cybersecurity or privacy obligations. There are two types of contractual relationships that may touch on cybersecurity and data privacy – contracts with service providers and contracts with customers – both of which can create obligations and liabilities that extend beyond those imposed by laws and regulations.

In the United States (and most other jurisdictions), a company can be held liable for data privacy and cybersecurity-related incidents caused by third-party service providers. As a result, the Buyer needs to conduct cyber diligence on these entities. At the outset of the diligence process, the Buyer should request a list of all the Target's service providers and vendors, and any agreements that are above a preset materiality threshold. The focus of this review should be on service providers that have access to the Target's data, such as IT support, outsourced human resources, software developers, data servers and storage providers, and security providers. The review should include not only the service agreement and primary contracts, but also any terms of service, privacy notices and similarly related and relevant documents.

For service providers, the diligence process should aim to identify what obligations and liabilities are created by these relationships and how the Target mitigates these vulnerabilities. Questions that should be considered include the following:

- Are there adequate provisions in the agreements to provide comfort to the Target that its data is sufficiently protected?
- Are there any reciprocal requirements imposed on the Target company?
- Are there indemnification or allocations of liability provisions?
- What types of data are being shared or processed? Are there specific obligations that arise from those types of data (e.g., HIPAA requirements for health data)?
- Are any jurisdictions involved outside that of the Target? If so, do the agreements and procedures adequately satisfy laws and regulations of both jurisdictions? Are there any cross-border transfer issues?
- Do third-party vendors and service providers have their own vendors and service providers?
- Are the contracts consistent with any applicable Target vendor management policies?
- Are there provisions that address requirements from applicable laws?[21]

The Buyer should also evaluate how the Target selects and monitors these third-party service providers.

The review of customer contracts will focus on any obligations and liabilities in those contracts to which the Target has agreed. The Buyer should evaluate any service agreements, terms of service, privacy notices, and other relevant documents that define the customer relationship. The Buyer should also determine whether the Target has made any representations relating to cybersecurity and data privacy when establishing the relationship underlying the transaction and whether those representations appear consistent with the Target's practices, based on the remainder of the review.

As part of the Buyer's review, it should also consider the Target company's cyber insurance policies, if such cover exists. Insurance against data breaches and unintentional privacy violations is becoming increasingly common, both as part of a company's umbrella cover as well as specifically and separately for companies in industries where data is an area of focus. The policies may provide some comfort by mitigating any identified risks or, conversely, identify areas of greater risk. In conducting this analysis, the Buyer must also confirm that a change of control will not affect the cover.

If a Target company has numerous contractual obligations, the Buyer may consider inserting representations and warranties into the purchase agreement to provide additional comfort that there will not be undue liability because of these obligations. There are two types of representations and warranties that Buyers can add. The first is a representation stating that the seller has provided the Buyer with all agreements with vendors and third parties during the diligence process. The second goes further to state that the seller has complied with its privacy and data security contractual obligations. Both representations are less common than some of the representations and warranties described previously, but it may be relevant to include them if some of these issues are uncovered during due diligence and cannot be addressed in other ways.

21 For example, the CCPA requires covered entities to have specific contractual provisions in place with service providers to address the law's requirements.

Conducting diligence: other common areas of focus

Depending on the characteristics of the Target and the context of the transaction, there are a variety of other areas that cyber diligence may include, such as compliance with public representations and industry standards, and the security of the company's IT infrastructure.

In addition to complying with laws and regulations relating to data privacy and cybersecurity, a company may also have obligations that stem from its public representations or from industry standards and best practices. In the United States, for example, (as discussed further in Chapter 11) the primary federal watchdog for data privacy and cybersecurity issues is the FTC, which derives its authority from the FTC Act, which in turn prohibits unfair and deceptive commercial practices. While the FTC has broadly interpreted the FTC Act to require companies to provide 'reasonable' protections for sensitive consumer data, its primary enforcement focus is on ensuring that companies comply with prior statements, such as posted privacy policies or advertisements that tout a company's security measures. A Target that is diligent about cybersecurity and data privacy issues will keep track of such statements and advertisements (or lack thereof) and document its compliance with the Act to protect against an FTC complaint or enforcement action. The Buyer should therefore request such records to consider whether they raise any red flags. The Buyer may also request representations and warranties that provide assurances that the company has materially complied with all such statements and advertisements, particularly if its records regarding compliance are not comprehensive.

On a more general level, the Buyer should also request any records or documents that the Target has that can provide insight into its IT infrastructure and technology inventory, such as network diagrams. These records will help the Buyer to analyse its data mapping and identify security vulnerabilities. The Buyer may also want to consider whether the Target company's security measures align with the needs and complexity of a Target company's IT infrastructure and technology. Once diligence is complete, a Buyer may request representations and warranties to provide assurance that the Target company has adequate (i.e., commercially reasonable) security measures in place.

Addressing red flags

As the diligence process nears its close, the Buyer should consider the red flags that have been identified and determine whether and how they can be mitigated.

Some issues can be addressed by the Target prior to conclusion of the transaction. For these issues, pre-closing conditions or covenants can be used to ensure that the Target addresses these issues. Generally, this will only work for discrete concerns that can be resolved quickly or concerns that may become more complicated once the transaction is concluded. For example, a pending data access request needs to be addressed quickly, as waiting until the transaction closes will only increase the risk of liability. The Buyer can confirm that the Target has addressed these pre-closing conditions and covenants prior to closing either through additional diligence or the use of representations and warranties confirming that the conditions and covenants have been met.

Other issues may be addressed through representations and warranties in the purchase agreement, which can be integrated into existing sections of a purchase agreement (e.g., compliance with laws) or can form their own separate section. Typically, sellers argue that such representations and warranties should be based on a materiality threshold or on the

knowledge of the company or certain officers of the company (or both). The seller's materiality threshold will typically be higher than the one used by the Buyer, but it will be determined by considering many of the same factors as a Buyer will consider in setting its own materiality threshold for its diligence process.

There are more general representations and warranties that a Buyer may consider using to mitigate risks. One common representation that a Buyer may request from a seller has to do with the transaction itself – that, to the best of the seller's knowledge, there will be no adverse effects from the transaction, such as a violation of any applicable laws, internal or external policies and procedures, prior statements or other obligations. An obvious example of this would be a provision in a third-party contract that gives a counterparty the right to terminate the relationship in the event of a change in control.

Purchase price adjustments are another mechanism that a Buyer can use to allocate cyber risk. Specifically, if the Target is unwilling to agree to either pre-closing conditions or representations and warranties, the Buyer may instead be able to negotiate an adjustment in price to account for the costs of remediation or the expected cost of uncovered liabilities and obligations.

Another method a Buyer can use to mitigate the cyber risks identified during its due diligence review is to purchase representations and warranties insurance (R&W insurance). R&W insurance can be purchased by either the Buyer or the Target, but Buyer-side policies are generally more common since Targets generally prefer to limit their continued liability. R&W insurance for Buyers also tends to provide broader cover and longer indemnification periods. A Buyer may offer to purchase R&W insurance in return for the Target's agreement to specific representations and warranties. A Buyer should consider how the cost of such insurance will change the value of the transaction. In addition, R&W insurers will often rely on the Buyer's due diligence when considering whether and how to provide R&W insurance, including cyber insurance. Thus, if a Buyer's cyber diligence uncovers potential liabilities or does not contain adequate bases for its conclusions, an underwriter may insist on exclusions, such as for historic cybersecurity incidents.

Once the Buyer has done all it can during the transaction negotiation to account for the red flags it has identified during its cyber diligence, it should consider how these will inform its plans to integrate the Target. An extended discussion of post-acquisition issues is beyond the scope of this chapter, but common issues that arise include:

- considering how best to incorporate the Target's database and IT assets into the Buyer's existing IT infrastructure;
- retrofitting the Buyer's cybersecurity policies and procedures to account for any unique cybersecurity obligations or vulnerabilities that the Target company has;
- transferring and converting key data into a format that is compatible with the Buyer's systems;
- remediating any identified red flags that were not addressed prior to closing; and
- implementing monitoring protocols to ensure the Target continues to comply with its data privacy and cybersecurity obligations.

In addition, the Buyer should ensure that it takes into account the newly acquired company when it considers the practicality and lawfulness of its future plans (e.g., ensuring that expansion plans adequately account for any effects on the Target's operations).

Conclusion

The average cost of a data breach in 2020 was almost US$4 million, and the likelihood of such a cyber incident is greater than ever before as companies deal with new risks from remote working, ransomware and increasingly sophisticated threat actors. The massive data breaches that have affected some of the biggest companies in the world show that every company is vulnerable to a data breach, regardless of the strength of its policies and procedures and how robust its IT security infrastructure is. As little as five years ago, these risks were not fully understood, and cyber due diligence may have been an afterthought in the due diligence process. Today it is a necessity. This chapter has addressed some of the key issues that a Buyer should consider in the diligence process as well as some of the key red flags, but a full description of cyber due diligence could easily fill a book. Therefore, to adequately conduct this diligence, it is critical that the Buyer use a professional team that understands cybersecurity risks and the specific material issues that Targets in a specific industry are likely to face.

8

Cyber Investigations in the Healthcare Sector

David C Rybicki, Gina L Bertolini and John H Lawrence[1]

Introduction

In February 2014, an advanced persistent threat (APT) actor based in China used a phishing scam to hack the computer of an employee at Anthem, Inc, one of the largest health insurance providers in the United States. Over the next year, the APT actor obtained access to at least 90 systems within the company's IT infrastructure, compromising the data of approximately 78.8 million patients nationwide. The ramifications of the breach – the largest of 2015 and still the largest healthcare sector data breach in US history – were costly, extensive and prolonged: a US$115 million class-action settlement with individuals whose protected health information (PHI) was compromised; a US$16 million settlement and corrective action plan imposed by the US Department of Health and Human Services (HHS) Office for Civil Rights (OCR), the federal agency tasked with enforcing the Health Insurance Portability and Accountability Act (HIPAA); and a US$39.5 million global settlement of data breach, identity theft and consumer protection claims with 44 state attorneys general. The *Anthem* breach starkly illustrates the layered liability exposure that a cybersecurity event can create for participants in the healthcare industry.

Healthcare is one of the most heavily regulated sectors of the US economy and the data-protection regulations that apply to healthcare entities at the state and federal levels are extensive. This chapter begins by exploring this complex regulatory framework and analyses key cybersecurity standards required by HIPAA, the primary federal statute governing the protection of PHI, and related authorities. The chapter then examines major cybersecurity threat vectors for the healthcare industry and concludes with a discussion of best practices to manage the risk of cyber intrusions.

1 David C Rybicki, Gina L Bertolini and John H Lawrence are partners at K&L Gates LLP.

Key cybersecurity standards for healthcare entities

The primary statutory and regulatory framework governing individually identifiable health information of US healthcare providers is the Health Insurance Portability and Accountability Act of 1996, the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009, and their implementing regulations found at 45 CFR Parts 160 and 164 (collectively, HIPAA).[2] The regulations implementing HIPAA are divided into three sections: (1) Security Standards for the Protection of Electronic Protected Health Information (the Security Rule); (2) Standards for Privacy of Individually Identifiable Health Information (the Privacy Rule); and (3) the Breach Notification Rule. While the focus of this chapter is electronic health information (EHI), it is important to note that HIPAA applies to all PHI, whether in paper or electronic format.

HIPAA applies to 'covered entities' – health plans, healthcare clearing houses, and healthcare providers that transmit health information in electronic form in connection with certain financial or administrative transactions outlined in the regulations.[3] In 2009, as part of the HITECH Act, HIPAA's Privacy and Security Rules were extended to include direct liability for certain entities that contract with healthcare providers, which HIPAA defines as 'business associates', expanding OCR's enforcement jurisdiction and bolstering protections for providers that previously were only contractual in nature.[4] Business associates are persons or entities, other than members of a covered entity's workforce, that perform certain functions or activities involving the use or disclosure of PHI for or on behalf of a covered entity. Such activities include, for example, revenue cycle management, legal representation and other professional consulting, health information technology services, utilisation management, and health benefits or health plan administration. The definitions of business associate and covered entity are not mutually exclusive: a covered entity can also be a business associate of another covered entity, and it is important for covered entities to recognise arrangements in which they are acting as a business associate.

For violations of HIPAA, OCR may impose civil monetary penalties from US$100 to more than US$50,000 per violation, not to exceed US$1,500,000 for identical violations in a calendar year. Factors determining the amount per violation include whether the covered

2 As a general rule, HIPAA preempts state laws pertaining to the privacy and security of health information, except where state laws provide greater privacy protections than those contained in the HIPAA Privacy Rules. In addition, many state laws mandate security incident or breach notification provisions in addition to those outlined in HIPAA's Privacy and Security Rules. Accordingly, because HIPAA may not be the only regulatory framework that healthcare sector entities must observe in relation to data privacy and security, they should be mindful of other state and federal laws that apply to certain sensitive data, such as substance use disorders, genetic information, mental health, and other sensitive diagnoses.

3 45 CFR § 160.103.

4 The HITECH Act was enacted as Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (ARRA), Pub. L. 111-5, 42 U.S.C. § 17934. HITECH applies to certain of HIPAA's privacy and security provisions and creates liability for business associates under HIPAA's Privacy and Security Rules. Prior to this statute and HHS's 2013 HIPAA Final Rule, 78 Fed. Reg. 5566 (25 January 2013), *et seq.*, business associate liability was limited to contractual remedies available under a mandatory Business Associate Agreement (BAA) with a covered entity. Although the 2013 Final Rule identified specific provisions of HIPAA that apply to business associates, BAAs are still mandatory under HIPAA. The HITECH Act also established breach notification obligations through implementation of the Breach Notification Rule and expanded penalties for violations of the Privacy and Security Rules.

entity or business associate did not know and, by exercising reasonable diligence, would not have known that it violated HIPAA; whether the violation was due to reasonable cause or wilful neglect; and whether the entity corrected the violation within 30 days of when it knew, or by exercising reasonable diligence, would have known that the violation occurred.[5] Potential fines and settlements with OCR can be costly, and OCR's website is replete with examples of recent enforcement actions and multi-million-dollar settlements involving breaches related to failure to apply appropriate administrative, physical and technical safeguards in accordance with the Security Rule.[6] HIPAA does not grant a private right of action to individuals affected by a violation, but the HITECH Act gave state attorneys general the authority to bring civil actions on behalf of state residents impacted by a HIPAA violation.

HIPAA's Security Rule

The adoption of technologies that enhance the mobility and efficiency of the healthcare workforce and give patients enhanced access to their medical records, such as electronic health records, electronic claims management and web-based applications, have increased security risks for covered entities, business associates and the patients they serve. HIPAA's Security Rule establishes the framework for health information security, outlining the security standards to be followed by covered entities and their business associates to safeguard EHI, protect against reasonably anticipated security threats and minimise the risk of security incidents and other impermissible uses or disclosures of EHI.[7] Because the Security Rule aims to allow the adoption of new technologies that will improve the quality and efficiency of patient care, it does not dictate all security measures that covered entities and business associates are required to implement. Instead, the Security Rule requires that entities use any security measures that 'reasonably and appropriately implement the standards and implementation specifications'.[8] In determining such measures, covered entities and business associates must consider:

- the entity's size, complexity and capabilities;
- the entity's technical infrastructure, hardware and software security capabilities;
- the costs of security measures; and
- the probability and criticality of potential risks to the entity's EHI.[9]

Both the Privacy and Security Rules outline 'standards', which are high-level requirements, and 'implementation specifications', which are specific measures designed to ensure adherence to a standard. In contrast to the Privacy Rule, however, and in recognition of the Security Rule's flexibility, implementation specifications under the Security Rule are either 'required' or 'addressable'. 'Addressable' implementation specifications are not optional; rather, they permit the covered entity or business associate to determine whether the specification is a reasonable and appropriate safeguard in its environment, taking into consideration how that

5 45 CFR § 160.401, et seq.

6 See, e.g., HHS.gov, Health Insurer Pays $5.1 Million to Settle Data Breach Affecting Over 9.3 Million People, 15 January 2021, https://www.hhs.gov/about/news/2021/01/15/health-insurer-pays-5-1-million-settle-data-breach.html.

7 45 CFR § 164.306(a).

8 id. § 164.306(b)(1).

9 id. § 164.306(b)(2).

particular specification contributes to protecting EHI. If the specification is not reasonable and appropriate, the entity must document the reasons why and implement an equivalent alternative measure, if reasonable and appropriate.[10]

The Security Rule outlines standards and implementation specifications in four broad categories: administrative safeguards, physical safeguards, technical safeguards and organisational requirements. Broadly speaking, administrative safeguards refer to eight standards that require an entity covered by HIPAA to manage the implementation and maintenance of security measures that protect EHI.[11] Key implementation specifications include a risk analysis, designation of a security official, implementation of security measures to reduce EHI vulnerabilities, adoption of a workforce sanctions policy and a regular review of system activity.[12] Entities covered by HIPAA also must implement policies and procedures that authorise access to EHI consistent with the Privacy Rule, address security incidents (including the identification and response to known or suspected security incidents) and outline emergency and disaster responses, and must implement a security awareness and training programme for workforce members.[13]

Physical safeguards refer to policies and procedures that physically limit access to an entity's EHI and include facility access, workstation and device and media controls.[14] Technical safeguards refer to the technology that protects and controls access to EHI, including: access, audit and integrity controls; person or entity authentication; and transmission security.[15] Organisational requirements require business associates to comply with applicable Security Rule requirements (including reporting breaches and implementing policies and procedures), enter into Business Associate Agreements (BAAs), and ensure that any subcontractors that create, receive, maintain or transmit EHI also comply with applicable requirements and enter into appropriate written agreements.[16]

The Privacy Rule

The Privacy Rule establishes standards governing when covered entities may use or disclose PHI. Except as required or permitted under the Privacy Rule, covered entities may not use or disclose PHI unless authorised to do so in writing by the individual who is the subject of the PHI (or the individual's personal representative). 'Authorisation' is a term of art under the Privacy Rule: it refers to an individual's written permission to use or disclose PHI in a manner not otherwise required or permitted by the Privacy Rule, such as for marketing purposes. An authorisation must contain certain core elements, including a description of the records to be disclosed and a statement notifying the individual that the information disclosed may be subject to re-disclosure by the recipient and no longer will be protected under the Privacy Rule.[17]

10 id. § 164.306(d)(3).
11 id. § 164.308.
12 id. § 164.308(a)(1)(ii), (a)(2), (b)(8).
13 id. § 164.308(a)(4), (a)(5)(ii), (a)(6), (a)(7)(i).
14 id. § 164.310(a)(2), (b)(2), (d)(1)–(d)(2).
15 id. § 164.312.
16 id. § 164.314.
17 id. § 164.508(c)(2)(iii).

There are two situations under which the Privacy Rule requires the disclosure of PHI:

- to the individual who is the subject of the PHI (or the individual's personal representative) upon the individual's request for access or an accounting of disclosures; and
- to HHS as part of a compliance investigation or enforcement action.[18]

While the Privacy Rule can be restrictive, in practice, there are many situations where it permits the use or disclosure of PHI. Most notably, the Privacy Rule allows for the use or disclosure of PHI for treatment, payment, and healthcare operations purposes.[19] For example, an individual's primary care physician may consult with a specialist about the treatment of a patient without obtaining the individual's permission to disclose his or her information to the specialist. Similarly, a physician may contact the individual's insurance carrier regarding the status of a claim to facilitate payment for services the physician has rendered to the individual. Additionally, a covered entity may use or disclose PHI to a business associate for operations purposes, such as utilisation review, quality assessment and improvement, auditing, business planning and development, and for legal or accounting services.[20] Covered entities are not required to obtain an individual's authorisation for disclosure to a business associate of PHI necessary for the business associate to perform a service for the covered entity; however, covered entities and business associates are required to execute BAAs containing certain required provisions and assuring that the business associate will comply with Privacy and Security Rule requirements.[21]

Breach Notification Rule

The Breach Notification Rule requires covered entities and business associates to provide notification following a breach of unencrypted PHI.[22] A breach is defined as the acquisition, access, use, or disclosure of PHI in a manner not permitted by the Privacy Rule that compromises the security or privacy of the PHI, as determined by a risk assessment.[23] If a breach has occurred, the entity will notify the affected individuals and, depending on the size of the breach, will notify OCR either at or near the time of discovery of the breach, or when the covered entity makes its annual report to OCR.[24] The covered entity or business associate also may be required to notify the media and post a notice on the entity's website.[25] For many entities, the desire to avoid negative coverage and the ensuing erosion of public and patient trust that can occur from a data breach are key motivators to building a strong HIPAA compliance programme.

The term 'breach' excludes:

18 id. § 164.502(a)(2).

19 id. § 164.502(a)(1). The term 'healthcare operations' refers to certain administrative, financial, legal, and quality improvement activities necessary to support the covered entity's treatment and payment functions. Id. § 164.501.

20 id. § 164.501.

21 id. § 164.502(e)(2); see id. § 164.508(b)(3).

22 id. § 164.404.

23 id. § 164.402.

24 id. §§ 164.404, 164.408.

25 id. §§ 164.406.

- any unintentional acquisition, access or use of PHI by a workforce member or person acting under the authority of a covered entity or a business associate, if made in good faith and within the scope of authority and if it does not result in further impermissible use or disclosure;
- any inadvertent disclosure by a person authorised to access PHI at a covered entity or a business associate to another person authorised to access PHI at the same covered entity or business associate when the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under the Privacy Rule; and
- a disclosure of PHI where a covered entity or business associate has a good-faith belief that an unauthorised person to whom the disclosure was made would not reasonably have been able to retain such information.[26]

Any acquisition, access, use, or disclosure of PHI that does not qualify as an exception is presumed to be a breach, unless the covered entity or business can demonstrate that there is a low probability that the privacy or security of the PHI has been compromised by utilising a risk assessment based on at least the following factors:

- the nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
- the unauthorised person who used the PHI or to whom the disclosure was made;
- whether the PHI was actually acquired or viewed; and
- the extent to which the risk to the PHI has been mitigated.[27]

Other key considerations include: whether any sensitive financial information (e.g., account identifiers or Social Security Numbers) or sensitive medical diagnoses or conditions were disclosed; the relationship between the individual and the person who acquired or viewed the PHI; whether the unauthorised person had an independent obligation to maintain the confidentiality of the PHI; and whether the information was destroyed or returned.

Primary cybersecurity threat vectors for healthcare entities

A security incident, as defined by the Security Rule, is an attempted or successful access, use, disclosure, modification or destruction of information, or an interference with system operations in an information system. Entities covered by HIPAA are required to identify and respond to suspected or known security incidents; mitigate the harmful effects of security incidents; and document security incidents and their outcomes.

While the healthcare sector has long been a target of cybersecurity threat actors, the number of security incidents has increased substantially since 2020, driven largely by the effects of the covid-19 pandemic, which has exacerbated a pre-existing lack of adequate cybersecurity measures throughout the industry.[28] Many small and mid-size healthcare entities

26 id. § 164.402(1).

27 id. § 164.402(2).

28 Bitglass, Healthcare Breach Report 2021: Hacking and IT Incidents on the Rise, 2021, available at https://pages.bitglass.com/rs/418-ZAL-815/images/CDFY21Q1HealthcareBreachReport2021.pdf?aliId=eyJpIjoiOE54NGRRTkhCZDY3aUxGMiIsInQiOiJ0RTZ1QVZXbnFPUGRhZXhVbmhyMmVnPT0ifQ%253D%253D.

simply do not have the resources to keep up with the security requirements necessitated by the valuable information they create or maintain. Additionally, the abundance of PHI available via digital platforms and its relatively high value on the dark web make healthcare providers attractive targets for malicious actors.

The top 10 healthcare data breaches reported to OCR over the past five years have affected approximately 80 million individuals.[29] With respect to breaches reported to OCR over a two-year period from 2019 to 2020, a substantial majority (71.87 per cent) were due to hacking or IT-related incidents affecting an average of approximately 80,500 individuals per incident.[30] Unauthorised access or disclosure accounted for approximately 19 per cent of breaches, and the remaining 10 per cent were attributed to improper disposal, misplacement and theft of PHI.[31] Healthcare providers have been affected the most, accounting for approximately 79.18 per cent of breach incidents, while other targeted entities include business associates (11.11 per cent), health plans (9.42 per cent) and healthcare clearinghouses (0.28 per cent).[32]

Ransomware

Ransomware attacks are perhaps the most formidable emerging cybersecurity threat for the healthcare industry, causing nearly half of all malware-related breaches targeting this sector.[33] Ransomware attacks on healthcare entities in the United States alone cost approximately US$21 billion in 2020,[34] a year that saw targeted ransomware attacks on the healthcare sector and a high number of related data breaches in part due to the easing of certain telehealth regulations by HHS in response to the covid-19 pandemic.[35] In October 2020, the US Cybersecurity and Infrastructure Security Agency (CISA), Federal Bureau of Investigation (FBI), and HHS issued a joint advisory on ransomware warning of 'an increased and imminent cybercrime threat to US hospitals and healthcare providers.'[36] While healthcare entities are often aware of the typical consequences of a ransomware attack such as reputational harm, administrative burden and financial costs, it is important to recognise that losses associated with a large-scale breach may be severe and lasting in terms of loss of data, implementation of additional security measures and other corrective actions, and erosion of patient and provider confidence. Moreover, a recent study found that data breach remediation efforts, particularly

29 See US Dep't of Health & Human Servs. Office of Civ. Rights Breach Portal, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf [hereinafter, OCR Breach Portal].

30 See OCR Breach Portal.

31 See id.

32 See id.

33 Tenable, The Tenable Research 2020 Threat Landscape Retrospective, 14 January 2021, www.tenable.com/blog/tldr-the-tenable-research-2020-threat-landscape-retrospective.

34 Comparitech, Ransomware Attacks on US Healthcare Organizations Cost $20.8bn in 2020, 10 March 2021, www.comparitech.com/blog/information-security/ransomware-attacks-hospitals-data/.

35 See SecurityScorecard & Darkowl, Listening to Patient Data Security: Healthcare Industry and Telehealth Cybersecurity Risks at 7-17 (2020), available at https://securityscorecard.com/resources/healthcare-industry-telehealth-cybersecurity-risks-report.

36 Cybersecurity & Infrastructure Security Agency et al., Alert (AA20-302A): Ransomware Activity Targeting the Healthcare and Public Health Sector, 28 October 2020, https://us-cert.cisa.gov/ncas/alerts/aa20-302a.

those related to ransomware attacks, can be associated with decreased patient care outcomes and negatively impacted timeliness of care.[37]

In addition to the direct threat of infiltration to a healthcare system, covered entities should be aware of the risk of ransomware attacks on their business associates and how breaches at the vendor level can affect the covered entity's operations. For example, cloud computing provider Blackbaud, Inc, became aware of a large-scale ransomware attack in May 2020 that had been ongoing for approximately three months. According to information obtained from the cloud provider's public statements and required government notifications, a cybercriminal exfiltrated a subset of data from a self-hosted environment affecting millions of individuals across dozens of healthcare entities nationwide.[38] Blackbaud indicated in a press release that it remedied the ongoing issue by paying the hacker's demanded ransom, conditioned on receipt of a certificate of destruction. While this is a common approach taken by ransomware victims, both the FBI and OCR have recommended against paying ransoms,[39] and there is now increased risk associated with payment in light of recent guidance issued by the US Department of Treasury's Office of Foreign Assets Control (OFAC) stating that entities can run afoul of US sanctions laws if they make ransomware payments to certain cybercriminals who are sanctioned or otherwise have a sanctions nexus.[40] The 2017 WannaCry attack, for example, the first to widely target vulnerabilities commonly found in medical devices, is believed to have been sponsored by the North Korean government.[41]

Business email compromise and phishing

While ransomware attacks have increased in frequency and scale since the onset of the covid-19 pandemic, phishing attempts and targeted email compromise campaigns are likely the most common cybersecurity attacks on the healthcare industry.[42] Healthcare entities should ensure employees are routinely trained to be aware of the threat of phishing and typical techniques used in third-party emails that attempt to obtain sensitive information, like employee account compromise, high-level executive fraud or impersonation, and bogus invoice schemes.

For example, spear phishing attempts in the healthcare sector often take timely topics and use targeted messaging to infiltrate an unsuspecting recipient's system. Beginning in 2020, business email compromise schemes frequently utilised information about covid-19,

37 Sung J Choi, et al., Data breach remediation efforts and their implications for hospital quality, Health Services Research, Sept. 10, 2019.

38 Blackbaud Newsroom, Learn more about the Ransomware attack we recently stopped, 16 July 2020, www.blackbaud.com/newsroom/article/2020/07/16/learn-more-about-the-ransomware-attack-we-recently-stopped.

39 Federal Bureau of Investigation, Ransomware, www.fbi.gov/scams-and-safety/common-scams-and-crimes/ransomware; Cyber Extortion, US Dep't of Health and Human Services, Office for Civil Rights, January 2018, www.hhs.gov/sites/default/files/cybersecurity-newsletter-january-2018.pdf.

40 US Dep't of Treasury, Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments, October 2020, https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf.

41 AHA Center for Health Innovation, Ransomware Attacks on Hospitals Have Changed, 15 May 2020, www.aha.org/center/cybersecurity-and-risk-advisory-services/ransomware-attacks-hospitals-have-changed.

42 HHS Cybersecurity Program, Business Email Compromise in the Health Sector, 9 July 2020, www.hhs.gov/sites/default/files/business-email-compromise-in-the-health-sector.pdf [hereinafter Business Email Compromise in the Health Sector].

particularly within the healthcare industry. HHS has recently issued notifications regarding emails from hackers posing as the Centers for Disease Control and Prevention and claiming to provide information on covid-19 safety measures or a link to an 'incident management system', or posing as company employees providing a link to a new 'disease management policy'.[43] At the height of the covid-19 pandemic, hackers impersonated suppliers to persuade in-house purchasing department employees to initiate wire transfers for personal protective equipment (PPE).[44] Agent Tesla, a remote access trojan capable of providing attackers with full computer or network access via accessing credentials, sensitive information, key strokes, screen activity and form-grabbing, launched a number of covid-19-related phishing campaigns specifically targeting the healthcare sector, including those with malware-containing attachments such as 'COVID 19 NEW ORDER FACE MASKS' or 'COVID-19 Supplier Notice'.[45]

Insider threats

Insider threats play a disproportionately large role in the healthcare space, and OCR recently observed that 69 per cent of data breaches involving health sector entities had some nexus to an insider acting intentionally or inadvertently.[46] OCR recommends that the best way to guard against insider threats is to detect and prevent leakage of data through certain security protocols and processes. In terms of security processes, organisations should be aware of where data is stored, who is permitted to access specific types of data within the organisation, and how such authorised users are permitted to interact with the data.[47] OCR recommends that organisations implement safeguards, detection software and audits to promptly identify unauthorised access, and to be especially mindful of these processes in high-risk situations, such as when an employee is involuntarily terminated.[48]

Advanced persistent threats

Long-term cybersecurity attacks, often originating from hostile, state-sponsored foreign actors, are known as advanced persistent threats (APT). OCR has observed that the most concerning aspect of APTs is the ability of the threat actor to remain undetected by constantly modifying tactics that allow the APT to persist within an entity's IT system.[49] APTs are routinely engaged in cybersecurity attacks on healthcare entities in the United States and abroad and frequently involve zero-day exploits.[50] OCR recommends implementing certain safeguards, such as encryption and access controls to mitigate the harm caused by APTs. The HHS Cybersecurity Program has recommended additional tactics that organisations

43 Coronavirus Theme E-mail Phishing, Health Sector Cybersecurity Coordination Center (HC3), 3 February 2020, www.hhs.gov/sites/default/files/coronavirus-themed-email-phishing.pdf.

44 See Business Email Compromise in the Health Sector.

45 Health Sector Cybersecurity Coordination Center (HC3), Remote Access Trojan 'Agent Tesla' Targets Organizations with COVID-themed Phishing Attacks, 16 June 2020, www.hhs.gov/sites/default/files/remote-access-trojan-agent-tesla-targets-organizations-covid-themed-phishing-attacks.pdf.

46 See HHS.gov, Summer 2019 OCR Cybersecurity Newsletter, 29 August 2019, www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity-newsletter-summer-2019/index.html.

47 See id.

48 See id.

49 See id.

50 See id.

may implement to mitigate the potential harm caused by APTs: security monitoring, understanding APT tactics, increased identification of APTs, updating networks and VPNs, and maintaining up-to-date IT resources to prevent vulnerabilities.[51]

Internet of Medical Things

Internet of Medical Things (IoMT) devices are able to collect, analyse, and transmit healthcare data, saving the healthcare industry billions of dollars annually due their ability to facilitate remote patient monitoring.[52] The increase in IoMT is due, in part, to the increased number of connected medical devices, with approximately 120 million connected IoMT devices in the United States alone, all of which are potentially vulnerable to cyberattack.[53] Like the risk posed by insider threats, the IoMT is subject to human error, resulting in inadvertent breaches of valuable information. To reduce the human factor, experts recommend the removal of hard-coded passwords to mitigate the risks of cyberattacks and subsequent breaches, in particular, those tied to a privileged account with universal access and permissions.[54]

Best practices for managing cyber intrusions

The threat of cyber intrusions in healthcare is varied, complex, and has the potential to trigger substantial liability on the part of providers under the myriad of laws and regulations that may be implicated by a breach. Medical records and other PHI are highly valued bundles of information that command high prices on the dark web, thereby further encouraging cybercriminals to target healthcare providers. As such, being prepared for – and effectively responding to and managing – a security incident or breach of EHI is essential, particularly in light of the demanding regulatory requirements that apply to cybersecurity in the healthcare industry.

Risk assessments and security audits

The threshold step in preventing and mitigating security incidents and PHI-related breaches requires conducting a risk analysis that identifies and implements safeguards that carry out Security Rule standards and implementation specifications.[55] The risk analysis should be 'an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate'.[56] According to HHS, a risk analysis is 'foundational' to an entity's compliance with the Security Rule and the protection of EHI.[57] Providers and

51 See id.

52 See TechTarget IoT Agenda, IoMT: A pulse on the internet of medical things, 8 August 2020, https://internetofthingsagenda.techtarget.com/blog/IoT-Agenda/IoMT-A-pulse-on-the-internet-of-medical-things.

53 See HealthTech, What Makes IoMT Devices So Difficult to Secure? 25 February 2020, https://healthtechmagazine.net/article/2020/02/what-makes-iomt-devices-so-difficult-secure-perfcon.

54 See id.

55 HHS.gov, Guidance on Risk Analysis, 22 July 2019, www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html [hereinafter, HHS Guidance on Risk Analysis].

56 45 CFR § 164.308(a)(1)(ii)(A).

57 HHS Guidance on Risk Analysis.

their business associates should conduct an initial risk analysis and thereafter periodically repeat risk analyses as technology, amount or type of EHI, or other circumstances change, and when threats are detected.

OCR issues annual guidance on the Security Rule and has consistently explained that the risk analysis is not a 'one size fits all' undertaking and does not guarantee compliance with the Security Rule. Instead, OCR maintains that each risk analysis must be tailored to the 'characteristics of the organization and its environment'.[58] Accordingly, covered entities and business associates should regularly review their size and complexity, the volume of their EHI and how such EHI is used, and their technical capabilities and available resources. Because these factors can change rapidly, particularly as technology develops and healthcare delivery models evolve, entities subject to HIPAA's Security Rule should assure that IT resources are current and commensurate with the amount and content of their EHI and the ways in which they use EHI.[59]

OCR suggests that the following non-exhaustive list of questions can help guide an organisation's risk analysis:

- Has the organisation identified all the EHI that it creates, receives, maintains, or transmits?
- What are the external sources of EHI? For example, do vendors or consultants create, receive, maintain, or transmit EHI?
- What are the human, natural, and environmental threats to information systems that contain EHI?[60]

OCR guidance also delineates specific areas that regulated entities should consider as a part of a comprehensive HIPAA-compliant risk analysis:

- Assess current security measures. Organizations should assess and document the security measures an entity uses to safeguard EHI, whether security measures required by the Security Rule are in place, and if current security measures are configured and used properly.[61]
- Determine the likelihood of threat occurrence. The Security Rule requires organisations to take into account the probability of potential risks to EHI. The results of this assessment, combined with the initial list of threats, will influence the determination of which threats the Security Rule requires protection against because they are 'reasonably anticipated'.[62]
- Determine the potential impact of threat occurrence. The Security Rule requires consideration of the 'criticality', or impact, of potential risks to confidentiality, integrity and availability of EHI.[63]
- Determine the level of risk. Organisations should assign risk levels for all threat and vulnerability combinations identified during the risk analysis.[64]

58 id.
59 id.
60 id.
61 See 45 CFR §§ 164.306(b)(1), 164.308(a)(1)(ii)(A), and 164.316(b)(1).
62 id. § 164.306(b)(2)(iv).
63 id.
64 See id. §§ 164.306(a)(2), 164.308(a)(1)(ii)(A), & 164.316(b)(1).

Ultimately, covered entities and business associates should carefully consider the threat environment in which they operate and tailor the frequency of the risk assessment accordingly. For example, a provider that is a hospital system operating in multiple locations and providing services to a large number of patients – and any business associates of such provider – should strongly consider an annual or more frequent risk assessment to ensure that their systems and processes are secure. Regardless of an entity's size and sophistication, however, a risk assessment may also be needed if the entity introduces new technologies to its operations; acquires other entities or facilities; or becomes aware of a specific type of breach experienced by a similarly situated entity.

While the Security Rule does not require a specific format for documenting an entity's risk analysis, it does require the risk analysis be documented, and providers should take care to do so.[65]

Security incident and breach response

To respond effectively to a security incident and a potential breach of EHI, covered entities and business associates should have clear security incident procedures and response and reporting processes in place before the incident occurs. The security incident response plan should outline steps to take when a security incident occurs or is suspected. An entity's workforce should be adequately trained regarding how to identify a security incident, including understanding early indications of a ransomware attack and common business email compromise and phishing schemes, and how and to whom to report a security incident or a breach of EHI. Entities should have a data back-up plan that creates and maintains retrievable exact copies of EHI;[66] a disaster recovery plan that includes procedures to restore loss of data; and an emergency mode operation plan that includes procedures to enable continuation of critical business processes and protection of the security of EHI while operating during an emergency. Entities should periodically test and revise contingency and emergency response plans, assess the criticality of specific applications and data in support of other contingency plan components, and should periodically re-evaluate policies and procedures to confirm that they continue to meet Privacy and Security Rule requirements.

When covered entities or business associates become aware of a potential security incident, it is critical to respond in an organised, focused and prompt manner. The entity should have a designated team of response experts – whether inside or outside the entity – that is tasked with receiving reports of security incidents, responding promptly and investigating such reports. This response team should be able to identify, contain and ultimately eliminate the source of the incident and restore the entity's IT systems to a secure state. The response team should, among other things, identify:

- the genesis of the suspected incident;
- the type and nature of the incident;
- the duration of the incident and whether it is ongoing;

65 See id. § 164.316(b)(1).

66 OCR recommends that entities periodically conduct test restorations to verify the integrity of back-up data and, because some ransomware variants remove or otherwise disrupt online back-ups, consider maintaining offline backups. *See* FACT SHEET: Ransomware and HIPAA, available at www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf.

- the extent of the incident, including affected data types and systems;
- whether a breach of EHI occurred and, if so, the identities of affected individuals (which may include workforce members and patients);[67] and
- the necessary steps to stop the incident (if ongoing) and re-secure the affected information systems.

In the event of a ransomware attack, the response team also should advise the entity, along with legal counsel, on whether and how the compromised data may be retrieved.

As soon as the incident or breach is discovered, the entity should consult legal counsel to determine whether the incident must be reported, to whom, to what extent, and within what time frame. Even if an investigation is ongoing, immediate consideration of these matters is essential, as the Breach Notification Rule requires notice to affected individuals 'without unreasonable delay', and in no event more than 60 days from the date of discovery. Moreover, given the host of state laws that may be applicable in addition to HIPAA, determining whether the incident is reportable and to which agencies, and whether individual and media notices are required, is a critical but complex analysis. Legal counsel, therefore, must become intimately familiar with the incident and its impacts to effectively assess the entity's reporting obligations and to help develop an appropriate timeline for reporting.

Heightened vigilance and responsiveness in a post-covid world

The covid-19 pandemic has heightened the need for covered entities and business associates to comprehensively conduct risk assessments and promptly respond to suspected breaches. As the United States raced to develop and deploy effective covid-19 vaccines and tens of millions of Americans received treatment and vaccinations in 2020 and 2021, healthcare providers were inundated with PHI. Hackers and other cybercriminals were aware of this, making healthcare providers increased targets for breaches.

Of particular concern surrounding the covid-19 pandemic and cybersecurity is the fact that the pandemic was not and is not an isolated public health crisis, but one that will last for years. As such, hackers and cybercriminals may have been more inclined during the pandemic to breach providers' systems and to lie in wait to collect the myriad of PHI that continues to be collected throughout the pandemic. Such a breach tactic is not without precedent in healthcare. For example, in January 2021, HHS announced a US$5.1 million settlement with Excellus Health Plan (Excellus), a health services corporation that provides health insurance coverage to citizens of New York State.[68] In September 2015, Excellus reported that a breach lasting from December 2013 to May 2015 resulted in the impermissible disclosure

67 The presence of ransomware (or any malware) is a security incident under HIPAA that may result in an impermissible disclosure of EHI in violation of the Privacy Rule and, depending on the facts and circumstances, may constitute a breach, as defined by the Privacy Rule.

68 HHS.gov, Health Insurer Pays $5.1 Million to Settle Data Breach Affecting Over 9.3 Million People, 15 January 2021, www.hhs.gov/about/news/2021/01/15/health-insurer-pays-5-1-million-settle-data-breach.html.

of 9.3 million individuals' PHI.[69] According to OCR, the hackers roamed undetected in Excellus's systems for over a year harvesting PHI.[70]

The *Excellus* settlement serves to underscore the increased need for vigilance in the covid-19 and post-covid-19 world. In particular, due to the heightened potential for long-term attacks during the pandemic like the one demonstrated in the *Excellus* matter, entities should consider engaging in routine risk assessments to identify potential security vulnerabilities and breaches as early as possible.

69 id.
70 id.

9

Ransomware Attacks and Responses

Ryan Fayhee and Tyler Grove[1]

Ransomware attacks have become a daily occurrence across a wide spectrum of businesses, healthcare facilities and educational institutions. This trend has only been exacerbated by the covid-19 pandemic, as many businesses have transitioned to fully remote work.[2] Victims of ransomware attacks risk the loss of essential data, operational delays and significant reputational damage. Often, victims are forced to respond to ransom demands within a limited time frame. Many are reasonably tempted to simply pay the requested sum when that monetary price is balanced against devastating enterprise risk.

However, there is also considerable risk to making such payments if the attackers are subject to sanctions or are a terrorist organisation, exposing in particular insurers and response vendors acting as third-party payors, cyber-risk vendors and other private responders in the absence of some reasonable diligence in the midst of an attack. The two primary US government agencies responsible for enforcing these rules – the Office of Foreign Assets Control (OFAC) and Financial Crimes Enforcement Network (FinCEN), both housed within the US Department of the Treasury – recently released advisories that signal an intention to strictly apply these laws, even against victims of cybercrime.[3] It is therefore critical that victims of ransomware attacks understand the risks involved and best practices in responding before taking any action and carefully plan in advance for an attack.

---

1 Ryan Fayhee is a partner and Tyler Grove is an associate at Hughes Hubbard & Reed.

2 See, e.g., '*COVID-19 pandemic sparks 72% ransomware growth, mobile vulnerabilities grow 50%*', Sec. Mag. (Jul. 22, 2020), https://www.securitymagazine.com/articles/92886-covid-19-pandemic-sparks-72-ransomware-growth-mobile-vulnerabilities-grow-50.

3 See *Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments*, U.S. Dep't of the Treasury (Oct. 1, 2020), https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf ('OFAC Advisory'); Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments, FIN-2020-A006, U.S. Dep't of the Treasury (Oct. 1, 2020), https://www.fincen.gov/sites/default/files/advisory/2020-10-01/Advisory%20Ransomware%20FINAL%20508.pdf ('FinCEN Advisory').

This chapter first provides an overview of the common forms of known ransomware and developing trends. It then summarises some of the key legal risks if ransom is to be paid, particularly those arising under sanctions, terrorist financing, and anti-money laundering laws.[4] Finally, it recommends best practices to consider in response to an attack.

Ransomware attacks and trends

Ransomware is malicious software that blocks access to a computer system or data as a means to extort monetary payments from victims in exchange for restoring access. Ransomware often works by encrypting the targeted files, and attackers may additionally threaten to sell or make public sensitive or embarrassing data if the payments are not made.

While ransomware attacks can affect businesses of any size and sophistication, increasingly ransomware attackers are targeting larger enterprises and extorting more significant payouts, often referred to as 'big game hunting.'[5] These attacks may also involve a correspondingly higher investment by the attacker in studying the target to identify potential vulnerabilities and developing advanced infiltration strategies.[6]

On the other hand, some attackers may seek to extort the same targets repeatedly.[7] Rather than seeking one larger payout, these attackers may demand comparatively low ransoms that incentivise the victim to pay without making substantial improvements to their cybersecurity or to otherwise address the vulnerability. These attackers hope that, in the aggregate, multiple 'nuisance' ransoms would exceed the amount that could be obtained through a single attack.

As commercial enterprises become savvier about preventing and detecting ransomware, ransomware developers have adapted and have, in fact, built an economy around their malign activities. Some ransomware attackers target sensitive or embarrassing information on their victims' networks. In addition to encrypting the data on the victim's networks, these attackers may make a copy of the data and demand two payments: one to encrypt the data on the victim's system, and one to prevent the attacker from selling or releasing the data.[8] The attackers may also simply sell the data, without regard to whether the ransom is ultimately paid by the victim.

One developing typology is the franchising of ransomware, known as ransomware-as-a-service (RaaS), and other forms of resource-sharing among attackers. RaaS allows malicious

4 There is no federal statute that comprehensively governs payments made in response to ransomware attacks. There may be additional legal risks and reporting requirements depending on, among other things, the jurisdictions affected and the organisation of the targeted business.

5 See *High-Impact Ransomware Attacks Threaten U.S. Businesses and Organizations*, Alert No. I-100219-PSA, FBI (Oct. 2, 2019), https://www.ic3.gov/Media/Y2019/PSA191002.

6 See, e.g., Lyle Adriano, *Ransomware 'big game hunting' has insurers on the ropes*, Insurance Business Mag. (Oct. 28, 2019), https://www.insurancebusinessmag.com/us/news/cyber/ransomware-big-game-hunting-has-insurers-on-the-ropes-189771.aspx.

7 See, e.g., Alexander Culafi, *Repeat ransomware attacks: Why organizations fall victim*, TechTarget (Jun. 16, 2020), https://searchsecurity.techtarget.com/news/252484720/Repeat-ransomware-attacks-Why-organizations-fall-victim#:~:text=Repeat%20ransomware%20attacks%20have%20become,hit%20with%20ransomware%20multiple%20times.

8 See, e.g., Alex Scroxton, *Double extortion ransomware will be a big theme in 2021*, Computer Weekly (Dec. 2, 2020), https://www.computerweekly.com/news/252493002/Double-extortion-ransomware-will-be-a-big-theme-in-2021.

actors to essentially license out their malware to less technically sophisticated criminal partners, either through a fixed fee or on a profit-sharing basis.[9]

Another emerging technique is the use of 'fileless' ransomware. In fileless ransomware, malicious code is inserted directly into a programs script or is written into its memory, so that there is no standalone malware file on the machine.[10] Fileless ransomware is, accordingly, significantly more challenging to detect.

Legal risks

Despite the increasing prevalence of ransomware attacks and the growing number of victims, responding to a ransom demand is fraught with many pitfalls. Businesses and their counsel should understand the basic legal frameworks that underlie these risks before deciding on how to respond to a ransom demand. Some of the most common legal risks if ransom is paid include those from transacting with a party subject to sanctions, making a payment to a terrorist organisation, as well as failing to make required Suspicious Activity Reports (SARs). Each risk is discussed in turn below.

Sanctions risks

There are a number of authorities that allow OFAC to sanction known cybercriminal organisations, such as those engaging in systemic ransomware attacks. In particular, on 1 April 2015, President Obama issued Executive Order 13694,[11] which was subsequently amended on 28 December 2016 by Executive Order 13757.[12] Those orders authorise OFAC to add individuals and entities to the Specially Designated Nationals (SDN) list who are determined to engage in certain malicious cyber activities. These activities include, inter alia, 'causing a significant disruption to the availability of a computer or network of computers' or 'causing a significant misappropriation of funds or economic resources, trade secrets, personal identifiers or financial information for commercial or competitive advantage or private financial gain.'

OFAC has designated a number of established cybercrime organisations and associated individuals under these authorities, which, as detailed in the OFAC Advisory, include the following:

- Evgeniy Mikhailovich Bogachev, the developer of Cryptolocker, which has infected an estimated 234,000 computers since 2013;
- Ali Khorashadizadeh and Mohammad Ghorbaniyan, two Iranian nationals who helped exchange digital currency (Bitcoin) ransom payments into Iranian rials on behalf of Iranian malicious cyber actors involved with the SamSam ransomware scheme that targeted over 200 known victims in 2015; and
- Evil Corp, a Russian cybercrime organisation, and its leader, Maksim Yakubets, for developing and using the program Didrex to steal more than US$100 million since 2015.[13]

9 See, e.g., *Ransomware as a Service (RaaS) Explained*, CrowdStrike (Jan. 28, 2021), https://www.crowdstrike.com/cybersecurity-101/ransomware/ransomware-as-a-service-raas/.

10 See, e.g., *How Fileless Ransomware Works,* CrowdStrike, https://www.crowdstrike.com/resources/infographics/how-fileless-ransomware-works/.

11 See Executive Order 13694 (Apr. 1, 2015), https://home.treasury.gov/system/files/126/cyber_eo.pdf.

12 See Executive Order 13757 (Dec. 28, 2016), https://home.treasury.gov/system/files/126/cyber2_eo.pdf.

13 See OFAC Advisory at 2.

Additionally, a number of US sanctions programmes apply to governments of countries viewed by the US government as adversaries, and extend to entities and organisations owned or controlled by those governments. For example, Executive Order 13772 blocks all property and interest in property of the government of North Korea, which is defined to include the government's 'agencies, instrumentalities, and controlled entities'.[14] Cybercrime groups under the control of the government of North Korea are therefore subject to sanctions, even if they are not explicitly identified on a US sanctions list, and on 13 September 2019, OFAC affirmed that three well-known North Korean hacking groups – Lazarus Group, Bluenoroff and Andariel, who used the ransomware program WannaCry 2.0 to infect approximately 300,000 computers in May 2017 – were, in fact, controlled by the government of North Korea.[15]

US persons – including US nationals, permanent residents, individuals physically present in the United States, and entities organised under US law – are prohibited from engaging in virtually all transactions involving these or other SDNs, or entities owned 50 per cent or more by an SDN, whether directly or indirectly. This prohibition extends to actions and activities that would 'facilitate' a transaction by a non-US person that would be prohibited if done by a US person. The concept of 'facilitation' is broad, and may include, for example, approving or directing payments by non-US persons, changing policies or procedures to remove US persons from the transaction, and even strategising about potential transactions with prohibited parties.

In addition, US persons are broadly prohibited from engaging in transactions with or involving citizens and permanent residents of comprehensively embargoed territories who are ordinarily resident in those territories, which include the Crimea region of Ukraine, Cuba, Iran, North Korea and Syria. This restriction applies regardless of whether the national of the embargoed territory is an SDN or otherwise identified on a sanctions list.

Non-US persons should also take heed of these prohibitions. If a US person or US dollars are involved in a transaction, non-US persons could face scrutiny for 'causing' the US person to violate sanctions. This risk also arises when converting US dollars (which generally are processed by a US correspondent bank) or using a US-based bank account or cryptocurrency exchange to make a ransom payment to a sanctioned party. Even if a US person or US dollars are not involved, Executive Order 13694 authorises OFAC to designate as subject to sanctions (i.e., include on the SDN list) any person determined 'to have materially assisted' or 'provided financial, material, or technological support for' persons sanctions under the order, and it is possible that ransom payments to sanctioned groups could be viewed as 'material assistance' by OFAC.

Significantly, civil violations of US sanctions are assessed under a strict liability standard, meaning that intent is not considered and even inadvertent transactions may, and often do, constitute violations. This renders payments to ransomware attackers extremely risky because often very little is known about the attacker that could allow the victim to gauge whether the attacker is an SDN or a national of a comprehensively embargoed country. If, after a payment, it is later discovered that the attacker was, in fact, subject to sanctions, the payor

14 See Executive Order 13772 (Mar. 15, 2016), https://home.treasury.gov/system/files/126/nk_eo_20160316.pdf.

15 See Press Release, Treasury Sanctions North Korean State-Sponsored Malicious Cyber Groups, U.S. Dep't of the Treas. (Sept. 13, 2019), https://home.treasury.gov/news/press-releases/sm774; *see also* OFAC Advisory at 2.

could be liable if OFAC discovers the transaction and brings an enforcement action. Civil violations may result in a monetary penalty of up to US$311,562 (as periodically adjusted for inflation) or twice the value of the transaction, whichever is higher.

If a person or entity violates sanctions 'wilfully,' or even 'wilfully blind', it could be subject to criminal liability. The standard for 'wilful' intent is set forth in *Bryan v. United States*, 524 US 184 (1998). Under *Bryan*, an act is wilful if done with the knowledge that it is illegal. The government, however, is not required to show the defendant was aware of the specific law, rule, or regulation that its conduct may have violated. Criminal violations may result in fines of up to US$1 million and forfeiture of any property involved in the violations, as well as up to 20 years in prison for individuals convicted of criminal sanctions violations.

Terrorist financing

Section 2339B of Title 18 of the United States Code provides:

> *Whoever knowingly provides material support or resources to a foreign terrorist organization, or attempts or conspires to do so, shall be fined under this title or imprisoned not more than 20 years, or both, and, if the death of any person results, shall be imprisoned for any term of years or for life.*

Notably, to face liability under this section, the violator 'must have knowledge that the organisation is a designated terrorist organization . . . , that the organization has engaged or engages in terrorist activity . . . , or that the organization has engaged or engages in terrorism.' Significantly, Section 2339B has broad extraterritorial application.

In scenarios where the ransomware attacker is known to be a foreign terrorist organisation, payment of the ransom could therefore constitute a violation of §2339B. It is worth noting that, in policy guidance regarding US citizens taken as hostages abroad, the US Department of Justice (DOJ) emphasised that it 'has never used the material support statute to prosecute a hostage's family or friends for paying a ransom for the safe return of their loved one'.[16] However, it is not clear if DOJ would extend this policy to payments of commercial ransoms where human life was not at risk. Considering the emphasis in the OFAC Advisory and FinCEN Advisory on compliance with sanctions and anti-money laundering requirements even for victims of ransomware attacks, §2339B should also be viewed as a potential risk when considering payments in response to ransomware attacks

Anti-money laundering reporting obligations

Certain businesses that qualify as a 'financial institution'[17] under the Bank Secrecy Act (BSA) – including 'money services businesses' that include certain currency exchanges and money transmitters – are required to file SARs. A financial institution is required to file a SAR if it:

- knows, suspects or has reason to suspect a transaction conducted or attempted by, at, or through the financial institution involves or aggregates to US$5,000 (or, with one

16 See Press Release, No. 15-790, *Department of Justice Statement on U.S. Citizens Taken Hostage Abroad*, U.S. Dep't of Jus. (Jun. 24, 2015), https://www.justice.gov/opa/pr/department-justice-statement-us-citizens-taken-hostage-abroad.

17 See 31 U.S.C. § 5312(a)(2) and (c)(1).

exception, US$2,000 for money services businesses) or more in funds or other assets and involves funds derived from illegal activity, or attempts to disguise funds derived from illegal activity;
- is designed to evade BSA regulations;
- lacks a business or apparent lawful purpose; or
  involves the use of the financial institution to facilitate criminal activity.[18]

Thus, qualifying 'financial institutions' must report extortive demands for a ransom payment to FinCEN through a SAR. Generally, SARs must be filed within 30 days of the detection of the suspicious activity. The wilful failure to timely file a SAR could carry a civil monetary penalty not to exceed the greater of the amount involved in each transaction (capped at US$233,313, as adjusted for inflation) or US$58,328, as adjusted for inflation.[19] Negligent violations are subject to a penalty of US$1,180, as adjusted for inflation.[20] Notably, each day that the violation continues is considered a separate violation.[21]

Even victims of ransomware attacks that are not 'financial institutions' subject to the BSA, and therefore not required to file a SAR, should be aware of the filing requirement, as third parties involved in the payment of a ransom could be required to submit a report. This risk could arise, for example, if the victim attempts to convert fiat currency into cryptocurrency, which is often a condition demanded by attackers in making a ransomware payment. Financial institutions that submit SARs are required to keep them confidential, and the subject of the SAR would not be informed that a report had been filed.

Response best practices

Companies should consider the following best practices when responding to an attack. It is highly recommended that at-risk companies consider these steps and how they might be tailored to the company's specific business before a ransomware attack occurs.

Create a plan and response team

Even before a ransomware attack occurs, it is critical that at-risk businesses develop a formal response plan, designate internal and external personnel who will form the response team, and clearly identify the responsibility of each team member. Among other things, the response plan should identify a reporting hierarchy to streamline decision making, as ransom payments are often demanded under intense time pressure. The response team should include key internal personnel, including, as appropriate, the company's chief legal officer, chief information security officer, chief information technology officer and chief operating officer. The response team should also include external resources, including external counsel specialising in compliance and data privacy issues, a cybersecurity firm, a digital forensics or investigations firm, media relations specialists, and other third parties as necessary. Once the response plan is formulated, it should be distributed to relevant employees, and regular training should be conducted to educate employees on how to identify and escalate potential issues.

18 See FinCEN Advisory at 6-7.
19 See 31 U.S.C. § 5321(a)(1); 31 C.F.R. § 1010.820(f).
20 See 31 U.S.C. § 5321(a)(6)(A).
21 See 31 U.S.C. § 5321(a)(1).

Gather information and conduct screening

As soon as a ransomware attack is discovered, the response team should gather all relevant information to enable decisions on how to respond. Depending on the time allotted for a response, this information should include, among other things, identifying which data or systems are compromised and evaluating whether the form and characteristics of the attack or malware used are similar to any prior known ransomware attacks. The OFAC advisory identifies several categories of key information to be evaluated, including:

> *relevant email addresses, Internet Protocol (IP) addresses with their respective timestamps, login information with location and timestamps, virtual currency wallet addresses, mobile device information (such as device International Mobile Equipment Identity (IMEI) numbers), malware hashes, malicious domains, and descriptions and timing of suspicious electronic communications.*[22]

However, ransomware victims should be aware that some groups attempt to mask their identity by using similar techniques as rival cybercriminal organisations. Further, given the rise of RaaS, the nature of the malware used may not always be indicative of the identity of the attacker.

The company should then conduct screening of the attacker using whatever information may be available. If a company, with the assistance of external resources, is able to determine that the attack is similar to other known prior attacks, the company should screen the name of the known or suspected perpetrators of the prior attacks against sanctions lists and assess whether they are affiliated with government actors that may be subject to sanctions. The payment information for the ransom should also be screened, as OFAC includes on its sanctions lists the digital wallet addresses of some well-known ransomware attackers.

Consider notifying law enforcement and relevant agencies

Contemporaneously with gathering information and screening, a ransomware victim should consider notifying law enforcement and OFAC of the attack. Among other benefits, law enforcement, who will have access to non-public information, may be able to assist with identifying the likely perpetrators of the attack, which will in turn be able to better inform the victim of whether a payment is prohibited. Timely notice to law enforcement is also viewed favourably by OFAC in making enforcement decisions, in the event a ransom is paid and it is later discovered that the attackers are subject to sanctions. The OFAC Advisory, for example, states:

> *OFAC will also consider a company's self-initiated, timely, and complete report of a ransomware attack to law enforcement to be a significant mitigating factor in determining an appropriate enforcement outcome if the situation is later determined to have a sanctions nexus. OFAC will also consider a company's full and timely cooperation with law*

22 See *Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments*, No. FIN-2020-A006, U.S. Dep't of the Treas., at 7 (Oct. 1, 2020), https://www.fincen.gov/sites/default/files/advisory/2020-10-01/Advisory%20Ransomware%20FINAL%20508.pdf.

> *enforcement both during and after a ransomware attack to be a significant mitigating factor when evaluating a possible enforcement outcome.*[23]

Separately and apart from the involvement of law enforcement, if a payment is made to a ransomware attacker, and a company is unable to determine that the attacker is sanctioned, the victim could consider filing a protective voluntary self-disclosure with OFAC. As a matter of policy, OFAC will reduce the maximum civil penalties applicable to a violation by half, and voluntary self-disclosures often result in no penalties, especially for companies with no prior violations in the past five years. The self-disclosure could then provide the relevant details regarding the nature and characteristic of the attack, the information available to the victim, and the screening and diligence results based on that information. The self-disclosure could further describe the victim's ransomware response plan procedures and actual response to the attack, including whether any specialised law firms or cybersecurity firms were used. To be considered 'voluntary', a self-disclosure must be submitted before OFAC opens its own investigation into a transaction. For this reason, a victim planning to make a self-disclosure may wish to do so prior to or at the same time as notifying other law enforcement.

Government investigations

Whether or not a payment is made in response to a ransom, there is a risk of subsequent government investigations. This could be the result of the victim notifying law enforcement (as discussed above), of a SAR being filed by a third party, or of other non-public intelligence available to law enforcement. Inquiries could range from informal requests for information to formal subpoenas or search warrants. Ransomware victims should therefore consider procedures for handling requests from law enforcement and other government agencies. Among other things, employees should be instructed to refer all requests to the appropriate corporate officers, such as the in-house legal department. It is also strongly recommended that victims receiving a request for information from law enforcement, whether formal or informal, consider the involvement of specialised external legal counsel to allow for the application of the attorney–client privilege.

Investigate and address vulnerabilities

Once an initial response has been made, whether or not it involves the payment of a ransom, a victim of an attack should conduct a full investigation into the root causes of the attack and take mitigating steps to avoid future similar attacks. Among other things, it is possible that malware could remain on infected systems and the point of entry for the attackers into the systems could remain open. Considering the rise of repeat attacks, these vulnerabilities should be identified and remediated as soon as possible. A sophisticated cybersecurity firm and digital forensics firms should be able to assist with this exercise.

In addition to identifying the root causes of the attack, the follow-on investigation should include confirmation of whether any compromised data was actually disclosed. Even if a ransom was paid, it is possible that attackers could still seek to sell a victim's data. A third-party cybersecurity firm can assist with conducting scans of the dark web and other

23 OFAC Advisory at 4.

common repositories of stolen data to identify whether any of the compromised data is present (and if so, whether that data can be linked back to the ransomware attack, or may be the result of a separate security breach). Depending on the data and the jurisdictions involved, there may be a legal obligation to make notifications of the breach to the data owners or government authorities.

Conclusion

Ransomware attacks are unfortunately a growing commercial reality that will continue for the foreseeable future. US sanctions, terrorist financing and anti-money laundering laws make no distinction between transactions conducted by victims of a crime or otherwise, and ransomware victims who choose to pay demanded sums to their attackers face a myriad of legal risks. Through understanding the common forms of ransomware attacks, the legal framework regulating the payments and the best practices in responding, victims can better judge their specific risks and navigate the complex regulatory backdrop to avoid government penalties on top of the potentially significant financial and reputational harm brought by an attack.

Part II

Jurisdictional, Regional and Sectoral Nuances

10

US Litigation Considerations and Landscape

Kevin Angle, Richard Batchelder, Jr, Nameir Abbas, Danielle Bogaards, Anne Conroy, and Sara Ramsey[1]

Introduction

Almost inevitably, often within hours of the announcement of a data breach involving the personal information of any large number of individuals, plaintiffs start filing class action lawsuits seeking recovery for the incident. Even incidents potentially involving the personal information of a comparatively modest number of individuals can follow the same path.

This chapter canvasses the typical causes of action that plaintiffs assert in these cases in the United States and developing trends reflected in litigation regarding recent incidents.[2] The chapter also highlights key considerations in cybersecurity litigation that can drive strategy. Finally, the chapter reviews the latest case law as to the requisite 'injury' necessary for standing purposes following a data breach.

Typical causes of action in US litigation

Class action claims asserted in the data breach context typically fall into five broad categories: contract, negligence, other common law theories, US state unfair and deceptive practices statutes, and other federal or state statutes. In large incidents involving public companies, stock purchaser and shareholder derivative plaintiffs are also filing complaints with seemingly greater frequency.

Data breach theories of liability

Plaintiffs who bring claims arising from the potential exposure of personal information in a data breach typically allege lack of care, misrepresentation or lack of prompt notice. To

1 Kevin Angle is a counsel, Richard Batchelder, Jr is a partner and Nameir Abbas, Danielle Bogaards, Anne Conroy and Sara Ramsey are associates at Ropes & Gray LLP. The authors would like to recognise the work of Mark Szpak, a retired partner, who was a key contributor to the previous edition of this chapter.

2 US government enforcement actions are covered in Chapter 11 of this book.

survive a motion to dismiss, plaintiffs will need to show how their factual allegations state a claim for each theory advanced.[3]

Contract-based theories

Contract claims are common when there is a written agreement and contractual privity between the plaintiff (whose data was allegedly exposed) and the defendant (who incurred the breach), such as, for example, when the plaintiff has entered into a service contract with the defendant subject to written terms and conditions. If the written agreement contains an express contractual undertaking by the defendant to protect the security of the plaintiff's personally identifiable information (PII),[4] the contract claim is likely to turn on the specific language of the undertaking and how the defendant allegedly breached it.[5]

---

3 Apart from litigation brought on behalf of individuals whose personal data was allegedly exposed in an incident or shareholders in companies who incurred the breach, other types of litigation following such an incident (which are beyond the scope of this chapter) may include business-to-business lawsuits between the breached entity and service providers or business partners arising from disputes about responsibility for the incident or associated losses, or failure to maintain security as to the other party's data. For example, when retail businesses incur payment card breaches, complaints against the retailer have frequently been filed not only by cardholders claiming injury from the breach but also by financial institutions that may have issued the payment cards that were allegedly exposed, by which the financial institutions seek to obtain recovery from the retailer for claimed fraud losses following the breach or for costs allegedly stemming from replacing the cards, or both. See, e.g., *Community Bank of Trenton v. Schnuck Markets*, 887 F.3d 803, 807 (7th Cir 2018). Other types of litigation (also not addressed in this chapter) include disputes with insurers about cover.

4 Notably, a number of courts have held that a company privacy policy is not enforceable under a breach of contract theory when it is not expressly incorporated into a contract. See, e.g., *In re: Anthem, Inc. Data Breach Litig.*, 162 F. Supp. 3d 953, 980 and 981 (ND Cal 2016) ('Plaintiffs can not bring a breach of contract claim . . . based on language from documents that might not even have been part of the alleged contract.'); *Abdale v. N. Shore Long Island Jewish Health Sys., Inc.,* 19 N.Y.S. 3d 850, 860 (NY Sup Ct 2015) (finding plaintiffs failed to allege a contractual relationship with defendants despite privacy statement); *In re: Zappos.com, Inc.*, No. 2357, 2016 WL 2637810, at *6, n.3 (D Nev 6 May 2016) (finding that defendant's 'Safe Shopping Guarantee' language and lock-shaped icon on its website were unilateral statements and thus insufficient to show the existence of a contractual obligation). But see *In re Marriott Int'l, Inc., Customer Data Sec. Breach Litig.*, 440 F. Supp. 3d 447, 484 (D. Md. 2020) (finding that privacy statements were objective offers to protect data security); *Kuhns v. Scottrade, Inc.*, 868 F.3d 711, 717 (8th Cir 2017) (finding that the privacy policy was incorporated in the relevant contract, but plaintiffs failed to allege a breach); *In re: Premera Blue Cross Customer Data Sec. Breach Litig.*, No. 3:15-MD-2633-SI, 2017 WL 539578, at *11 (D Or 9 Feb 2017) (finding that complaint adequately alleged that defendant's privacy notice was (1) attached to and incorporated in the relevant contract, and (2) contained sufficient language to support the breach of contract claim).

5 See, e.g., *Scottrade*, 868 F.3d at 717 (dismissing contract claim based on defendant's privacy statement that 'we use [data] security measures that comply with federal law' in part because plaintiffs failed to identify an applicable law or regulation that defendant allegedly violated); *Dolmage v. Combined Ins. Co. of Am.,* No. 14 C 3809, 2015 WL 292947, at *7 (ND Ill 21 Jan 2015) (dismissing contract claim from initial complaint because plaintiff failed to allege facts demonstrating defendant breached its privacy pledge, which stated that it 'guard[s] [its customers'] personal information'). In cases where plaintiffs allege that a company's privacy policy can form an express contract, limitations within those policies may also block claims. See, e.g., *Pena v. British Airways, PLC (UK)*, No. 18-cv-6278 (LDH) (RML), 2020 WL 3989055, at *6 (EDNY 30 Mar 2020) (dismissing contract claim where 'Defendant's Privacy Policy explicitly states that it is "not contractual and d[oes] not form part of [plaintiff's] contract with [defendant]"') (internal citation omitted); *Bass v. Facebook, Inc.*, 394 F. Supp. 3d 1024, 1037 (ND Cal. 2019) (dismissing contract claims where Facebook's terms of service included an applicable limitation-of-liability clause); *In re Equifax, Inc.*, 362 F. Supp. 3d 1295, 1332 (ND Ga 2019) (rejecting claim

If a written agreement exists but has no written term as to the handling of personal data, or if there is no written agreement at all but the plaintiff is still in contractual privity with the defendant, the cause of action is typically styled as a breach of implied contract. Implied contract claims have received mixed treatment from courts. Some find that the typical purchase transaction does not include a promise to protect the PII that may have been obtained (e.g., payment card information in a retail purchase). In these cases, the courts hold that any implied contract, if it existed, 'involved only the provision of and payment for [the items in question], not a promise to safeguard the customer's [data]'.[6] Other courts accept that a defendant's receipt of consumer PII in connection with interactions of particular types can be sufficient to plead an implied contract covering the PII as well. These courts reason that 'it is difficult to imagine how, in our day and age of data and identity theft, the mandatory receipt of Social Security numbers or other sensitive personal information would not imply the recipient's assent to protect the information sufficiently'.[7]

Finally, in cases without a written contract or privity between the parties, contract claims can be difficult to sustain. This situation commonly arises when the party receiving personal data from a plaintiff provides it to a third party for processing or handling, who suffers the breach. Absent direct dealings between the plaintiff (whose data was involved, albeit in the hands of a third party) and the third party (who incurred the breach), direct claims against the third party in contract tend to fail for inability to allege or show the requisite 'meeting of the minds'.[8]

---

where privacy policy stated defendant would not be liable for damages based on information found on the site). But see *In re Yahoo! Inc. Customer Data Sec. Breach Litig.*, No. 16-MD-02752-LHK, 2017 WL 3727318, at *45 (ND Cal 30 Aug 2017) (declining to dismiss contract claims where statements like using the service was 'AT YOUR OWN RISK' were contradicted by statements regarding security measures in place).

6 *Lovell v. P.F. Chang's China Bistro, Inc.*, No. C14-1152RSL, 2015 WL 4940371, at *3 (WD Wash 27 Mar 2015). See also *In re: SuperValu, Inc.*, 870 F.3d 763, 771 n.6 (8th Cir 2017) (rejecting breach of implied contract claim); *Longenecker-Wells v. Benecard Servs. Inc*, 658 F. App'x 659, 662 (3d Cir 2016) (same); *In re Equifax, Inc.,* 362 F. Supp. 3d at 1332 (same); but see *In re Target Corp. Data Sec. Breach Litig.*, 66 F. Supp. 3d 1154, 1176 and 1177 (D Minn 2014).

7 *Castillo v. Seagate Tech., LLC*, No. 16-CV-01958-RS, 2016 WL 9280242, at *9 (ND Cal 14 Sep 2016). See also *Sackin v. TransPerfect Glob., Inc.*, 278 F. Supp. 3d 739, 750 and 751 (SDNY 2017) (denying motion to dismiss breach of implied contract claim); *Enslin v. Coca-Cola Co.*, 136 F. Supp. 3d 654, 675 (ED Pa 2015) (same).

8 *Hammond v. The Bank of New York Mellon Corp.*, No. 08 CIV. 6060, 2010 WL 2643307, at *11 (SDNY 25 June 2010) (rejecting consumers' breach of implied contract claim on grounds that plaintiffs failed to allege direct dealings with defendant); *Willingham v. Global Payments, Inc.*, No. 1:12-CV-01157-RWS, 2013 WL 440702, at *20 and *21 (ND Ga 5 Feb 2013) (rejecting consumers' breach of implied contract claim because plaintiffs provided their personally identifiable information [PII] to a merchant, not to the defendant). See also *Community Bank of Trenton v. Schnuck Markets*, 887 F.3d 803, 819 and 820 (7th Cir 2018) (rejecting implied contract claim brought by financial institution because 'the only business activity between the plaintiff banks and [defendant] happened (nearly instantaneously) through the indirect route of the card payment system, not in a direct face-to-face retail transaction'); *In re: Heartland Payment Sys., Inc. Customer Data Security Breach Litig.*, 834 F. Supp. 2d 566 (SD Tex 2011), rev'd in part *sub nom. Lone Star National Bank, N.A. v. Heartland Payment Systems, Inc.*, 729 F.3d 421 (5th Cir 2013) (same); but see *In re Cap. One Consumer Data Sec. Breach Litig.*, 488 F. Supp. 3d 374, 412 (ED Va 2020) (finding lack of privity did not bar unjust enrichment claim).

Negligence-based theories

Individuals alleging injury from the exposure of their personal information in a data breach almost always include a claim for negligence (i.e., that the breached entity acted negligently by failing to prevent the data from being accessed or acquired by an intruder). Of course, the merits of such claims, if litigated to a conclusion, often involve highly factual determinations and possibly expert testimony as to the adequacy of the defendant's security measures. However, cases rarely get that far.

The first question litigants must answer is whether the company had any duty to the plaintiff. The answer varies from state to state.[9] Courts in some cases have found no common law duty to safeguard personal information to exist under the law of the state in question.[10] At the same time, courts in other cases have concluded that a common law duty to safeguard personal information to have been sufficiently alleged, at least in certain factual contexts.[11]

Even when a duty of care is found to exist as a matter of law, the factual parameters of the standard for meeting that duty remain largely undefined. Though 'reasonableness' plays a prominent role in tort law generally, courts have not yet fully addressed how to determine 'reasonableness' in the data breach context.[12] Plaintiffs, for example, may frame the test as

9 Compare *In re Marriott Int'l, Inc., Customer Data Sec. Breach Litig.,* 440 F. Supp. 3d 447, 478 (D Md 2020) (declining to find duty of care under Illinois law); *Dep't of Labor v. McConnell*, 828 S.E.2d 352, 358 (Ga 2019) (no duty to safeguard personal information under Georgia law); *Irwin v. Jimmy John's Franchise*, LLC, 175 F. Supp. 3d 1064, 1071 (CD Ill 2016) (no common law duty owed to customers under Arizona law), with *In re: Experian Data Breach Litig.*, No. SACV 15-1592 AG, 2016 WL 7973595, at *3, *5, *7 and *8 (CD Cal 29 Dec 2016) (denying motion to dismiss negligence claims brought by consumers under New York, Ohio, California or Illinois laws finding that plaintiff had alleged a duty under each state's law); *Hapka v. Carecentrix, Inc.*, No. 16-2372-CM, 2016 WL 7336407, at *5 (D Kan 19 Dec 2016) (denying motion to dismiss negligence claim brought by employees under Kansas law); *In re: Target Corp. Customer Data Sec. Breach Litig.*, 64 F. Supp. 3d 1304, 1176 (D Minn 2014) (denying motion to dismiss negligence claims brought by customers under various state laws).

10 See, e.g., *Attias v. CareFirst, Inc.*, 365 F. Supp. 3d 1, 17–18, 23–24 (D DC 2019) (dismissing negligence claim against insurer because parties had no special relationship). *Dolmage*, 2015 WL 292947, at *5 and *6 (dismissing with prejudice plaintiff 's negligence claim because Illinois law imposed no duty to safeguard PII in the absence of legislation imposing such a duty); *McConnell*, 828 S.E.2d at 358; *Jimmy John's*, 175 F. Supp. 3d 1064, 1071. Compare *Schnuck Markets*, 887 F.3d at 816 (breached supermarket owed no duty to banks under Illinois or Missouri law); *Citizens Bank of Pennsylvania v. Reimbursement Technologies, Inc.*, 609 F. App'x 88, 93 (3d Cir 2015).

11 See, e.g., *In re Cap. One Consumer Data Sec. Breach Litig.*, 488 F. Supp. 3d 374, 400 (ED Va 2020) (finding that bank had assumed a duty of care based on its actions); *Hapka*, 2016 WL 7336407, at *5 (finding duty under state law to exercise reasonable care to protect employee personal information where harm is foreseeable); *Dittman v. UPMC*, 196 A.3d 1036, 1047 and 1048 (Pa 2018) (finding employer had duty to use reasonable care to safeguard 'sensitive' employee information against potential breach where collected as a condition of employment).

12 See, e.g., *In re: The Home Depot, Inc., Customer Data Sec. Breach Litig.,* No. 1:14-MD-2583-TWT, 2016 WL 2897520, at *3 and *4 (ND Ga 18 May 2016) (finding that defendants had a duty to safeguard PII but not expanding on the standard to meet that duty other than to note defendant's knowledge of a substantial security risk and failure to implement reasonable security measures constitutes a breach); compare *In re: Arby's Rest. Grp. Inc. Litig.*, No. 1:17-CV-0514-AT, 2018 WL 2128441, at *9 and *10 (ND Ga 5 Mar 2018) (finding that plaintiffs had sufficiently pleaded a beach of common law duty, in part, by alleging defendant failed to comply with standard industry security practices). Defining the contours of a 'reasonable' duty to safeguard PII may prove difficult, at least prospectively. See *LabMD, Inc. v. Fed. Trade Comm'n*, 894 F.3d 1221, 1230,

a comparison of the conduct in question with 'industry practice' or 'industry standards', whereas defendants may note that 'reasonableness' at the time of the conduct in question must include an evaluation of whether the expected cost of safeguarding the information was outweighed by the benefit of doing so as perceived at the time relevant decisions were made. Outcomes (if fully litigated) will in any event be heavily dependent on the facts of each case.

Note that, in some states, the negligence line of attack can fall flat even if there is a clear duty of care. The economic loss doctrine generally provides that a contracting party alleging purely economic consequences (e.g., possible loss of future business) must seek a remedy in contract, not tort. Arguments for dismissal based on this doctrine are dependent on the doctrine's strength and contours in each state.[13]

Other common law theories

There are a number of other common law theories of liability usually found in class action complaints following a data security incident. However, the success rate for plaintiffs in bringing such claims is mixed at best.

For example, invasion of privacy claims are often dismissed because courts find there is no 'publication' of private information by the defendant.[14] Bailment claims are typically dismissed because plaintiffs cannot allege that they transferred their property to defendants, that defendants promised to return 'property' or that defendants wrongfully retained the information.[15] Misrepresentation claims often fail because plaintiffs rarely can allege that they justifiably relied on a false statement.[16] Finally, unjust enrichment claims usually, though not

1235 and 1236 (11th Cir 2018) (finding that the Federal Trade Commission's cease and desist order based on LabMD's failure to implement 'reasonable security measures to protect sensitive consumer information' to be unenforceable owing to vagueness).

13 Compare *Aguilar v. Hartford Accident & Indem. Co.*, No. CV 18-8123-R, 2019 WL 2912861, at *2 (CD Cal 13 Mar 2019) (dismissing negligence claim based on economic loss doctrine); *In re: Lenovo Adware Litig.*, No. 15-md-02624, 2016 WL 6277245, at *9 (ND Cal 27 Oct 2016) (dismissing negligence claims under New York and California law as barred by the economic loss doctrine), *Schnuck Markets*, 887 F.3d at 816 (dismissing negligence claim under Illinois law as barred by the economic loss doctrine), with *In re: The Home Depot, Inc.*, 2016 WL 2897520, at *3 (declining to dismiss negligence claim under Georgia law).

14 See, e.g., *Galaria v. Nationwide Ins. Co.*, 998 F. Supp. 2d 646, 661 and 662 (SD Oh 2014), rev'd on other grounds, No. 15-3386/3387 (6th Cir 12 Sep 2016) (dismissing claim when defendant did not publish plaintiffs' PII); *Smith v. Triad of Alabama, LLC*, No. 14-cv-324, 2015 WL 5793318, at *13 (MD Ala 29 Sep 2015) (same); but see *In re: Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig.*, 45 F. Supp. 3d 14, 33 (DDC 2014) (finding plaintiff sufficiently pleaded invasion of privacy by alleging that her unlisted phone number and medical records were exposed by a data breach and that she had subsequently received unsolicited phone calls regarding her specific medical condition).

15 See, e.g., *Galaria v. Nationwide Mut. Ins. Co.*, No. 2:13-cv-118; 2:13-cv-257, 2017 WL 6375803, at *3 and *4 (SD Oh 13 Dec 2017); *In re: Target Corp. Data Sec. Breach Litig.*, 66 F. Supp. 3d 1154, 1177 (D Minn 2014).

16 See, e.g., *Lovell v. P.F. Chang's China Bistro, Inc.*, No. C14-1152RSL, 2015 WL 4940371, at *5 and *6 (WD Wash 27 Mar 2015) (dismissing omissions-based misrepresentation claim); but see *In re: Anthem, Inc. Data Breach Litig.*, No. 15-MD-02617-LHK, 2016 WL 3029783, at *38 (ND Cal 27 May 2016) (giving plaintiffs leave to amend fraudulent misrepresentation claim noting that allegations that plaintiffs 'viewed, heard, or read [d]efendants' privacy policies, and thus relied on the[ ] policies' would suffice to plead the claim).

always, fail because plaintiffs cannot allege they paid for cybersecurity protection[17] or because the existence of a contract (express or implied) prevents a parallel unjust enrichment claim.[18]

Consumer protection statute theories

State consumer protection statutes provide another source of claims that plaintiffs frequently use in bringing cases against breached companies. These statutes, while varying from state to state, commonly allow for claims based on any of three grounds: unlawfulness, unfairness or deception.

Unlawfulness claims, when available under state consumer protection statutes, typically require a showing that the conduct in question violates an established legal prohibition. No 'deception' or 'unfairness' is required; only that, for example, the conduct contravenes a particular statute.[19]

By contrast, unfairness claims under state consumer protection statutes require no showing of any specific statutory violation, but rather that the conduct in question is 'unfair'. Critically, most of these statutes provide little guidance as to what conduct qualifies. Some courts have looked to the factors that define 'unfairness' under Section 5 of the Federal Trade Commission (FTC) Act.[20] Other courts require that plaintiffs allege that a defendant's acts were (1) 'systematically reckless', (2) 'aggravated by [a] failure to give prompt notice', and (3) 'cause[d] widespread and serious consumer harm'.[21] Yet other courts, more troubling to

17 Compare *Community Bank of Trenton v. Schnuck Markets*, 887 F.3d 803, 820 (7th Cir 2018) (dismissing unjust enrichment claim), *Irwin v. Jimmy John's Franchise, LLC,* 175 F. Supp. 3d 1064, 1072 (CD Ill 2016) (same), with *In re Cap. One Consumer Data Sec. Breach Litig.*, 488 F. Supp. 3d 374, 411-12 (ED Va 2020) (denying motion to dismiss unjust enrichment claim), *Flynn v. FCA US LLC*, No. 15-CV-0855, 2017 WL 3592040, at *3 and *4 (SD Ill 21 Aug 2017) (same), *Weinberg v. Advanced Data Processing, Inc.*, 147 F. Supp. 3d 1359, 1368 and 1369 (SD Fl. 2015) (same); *Resnick v. AvMed, Inc.*, 693 F.3d 1317, 1328 (11th Cir 2012) (same). See also *In re: Target,* 66 F. Supp. 3d at 1177 and 1178 (rejecting overpayment theory but finding plaintiffs' unjust enrichment claim had merit on grounds that it was plausible plaintiffs 'would not have shopped' at Target had they known of the then-current breach).

18 Compare *Schnuck Markets,* 887 F.3d at 820 (dismissing unjust enrichment claim), *In re: Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 996 F. Supp. 2d 942, 984 (SD Cal 2014) [*Sony II*] (same), with *Fero v. Excellus Health Plan*, 236 F. Supp. 3d 735, 769 and 770 (WDNY 2017) (declining to dismiss unjust enrichment claim); *In re: Arby's Rest. Grp. Inc. Litig.*, No. 1:17-CV-0514-AT, 2018 WL 2128441, at *17 (ND Ga 5 Mar 2018) (same).

19 See, e.g., *In re: Anthem, Inc. Data Breach Litig.*, 162 F. Supp. 3d 953, 989 (ND Cal 2016) ('Generally, violation of almost any law may serve as a basis for a [California unfair competition law] claim.') (quoting *Antman v. Uber Tech., Inc.*, 2015 WL 6123054, at *6 (ND Cal 19 Oct 2015) (citation omitted)).

20 See *Camacho v. Automobile Club of Southern California*, 142 Cal. App. 4th 1394, 1403 (2006) (applying the FTC Act factors: '(1) the consumer injury must be substantial; (2) the injury must not be outweighed by any countervailing benefits to consumers or competition; and (3) it must be an injury that consumers themselves could not reasonably have avoided'); see also *In re: Anthem*, 162 F. Supp. 3d at 989 and 991.

21 *In re: Michaels Pin Pad Litig.*, 830 F. Supp. 2d 518, 526 (ND Ill 2011) (quoting *In re: TJX Cos. Retail Sec. Breach Litig.*, 564 F.3d 489, 496 (1st Cir 2009)).

defendants, have declined to dismiss claims alleging merely 'unreasonable' or 'inadequate' cybersecurity,[22] or violations of 'established' public policy.[23]

Consumer protection statute claims based on 'deception' are similar to common law misrepresentation claims in that they often are premised on alleged materially misleading statements in user agreements[24] or alleged omissions about cybersecurity defects at the time of sale.[25] Contrary to their common-law counterparts, however, not all state consumer protection statutes require the plaintiff to allege or show reliance, and not all state consumer protection statutes require a resulting injury.[26]

Note also that state consumer protection statutes often impose other requirements or restrictions. For example, it is common for the statutes to require that the action arise from a sale of goods or services or a consumer-oriented practice.[27] It is also common that statutes limit relief to transactions that have a significant connection to the state.[28] Certain state statutes prohibit or restrict class relief (at least for actions brought and pending in the courts of that state).[29]

Other statute-based theories

Finally, class action complaints following a data breach can also include an array of allegations attempting to support causes of action asserted under other state or federal statutes. A main impetus for class action plaintiffs to assert such other statutorily based claims is that they

22 *In re: Home Depot, Inc. Cust. Data Sec. Breach Litig.*, No. 1:14-md-2583-TWT, 2016 WL 2897520, at *5 (ND Ga 18 May 2016); *In re: Target*, 66 F. Supp. 3d at 1162 (refusing to dismiss claim for failure to maintain 'adequate' data security practices).

23 See *In re: Anthem, Inc. Data Breach Litig.*, 162 F. Supp. 3d. 953, 990 (ND Cal 2016).

24 *Grigsby v. Valve Corp.*, No. C12-0553JLR, 2013 WL 12310666, at *2 (WD Wash 18 Mar 2013); *Sony II*, 996 F. Supp. 2d at 985; *Abdale v. N. Shore Long Island Jewish Health Sys., Inc.*, 19 N.Y.S. 3d 850, 854 (NY Sup Ct 2015).

25 *Edenborough v. ADT, LLC*, No. 16-CV-02233-JST, 2016 WL 6160174, at *2 (ND Cal 24 Oct 2016); In re: Target, 64 F. Supp. 3d 1304, 1162 and 1163 (D Minn 2014); *In re: Adobe Sys., Inc. Privacy Litig.*, 66 F. Supp. 3d 1197, 1229 (ND Cal 2014).

26 See, generally, *Sony II*, 996 F. Supp. 2d 942 (dismissing negligent misrepresentation claims and Michigan and Texas consumer protection claims for failure to plead reliance or causation, but allowing certain other claims under California, Missouri, Florida and New Hampshire statutes with lesser or no causation requirements); see also generally *In re: Experian Data Breach Litig.*, No. SACV 15-1592 AG, 2016 WL 7973595 (CD Cal 29 Dec 2016) (dismissing California statutory claims for failure to allege reliance and an Illinois fraud-based statutory claim for failure to allege causation, while allowing New York statutory claim based on mere showing of materiality); *In re: Anthem, Inc. Data Breach Litig.*, 162 F. Supp. 3d 953, 996 and 997 (ND Cal 2016) (citing New York case in which a plaintiff's allegations supported the causation element of a deceptive-practices claim but did not support the reliance element needed for a common law claim).

27 *In re: Experian Data Breach Litig.*, 2016 WL 7973595, at *4 and *7; *In re: The Home Depot,* 2016 WL 2897520, at *5.

28 *Irwin v. Jimmy John's Franchise*, LLC, 175 F. Supp. 3d 1064, 1069 and 1070 (CD Ill 2016) ('A nonresident plaintiff may sue under the [Illinois Consumer Fraud and Deceptive Business Practices Act] only if the circumstances giving rise to the cause of action occurred "primarily and substantially in Illinois".'); *In re: Sony Gaming Networks and Cust. Data Sec. Breach Litig.*, 903 F. Supp. 2d 942, 964 and 965 (SD Cal 2012) [*Sony I*] (dismissing non-resident plaintiffs' claims brought under California statutes).

29 See *In re: Anthem*, 162 F. Supp. 3d 953, 999 and 1000; *In re: Target*, 64 F. Supp. 3d at 1163; *Sony II*, 996 F. Supp. 2d 942, 1003.

often provide for statutory damages, which if applied per class member on a class-wide basis, raise the prospect of huge damage awards.

For example, the Fair Credit Reporting Act (FCRA) requires 'reasonable procedures' as to the handling of consumer reports in certain respects[30] and includes a private right of action permitting recovery of between US$100 and US$1,000 in statutory damages per violation of the statute generally.[31] Plaintiffs in a variety of breach cases have thus invoked the FCRA to seek class-wide relief in an effort to obtain statutory damages.[32] The Stored Communications Act (SCA) also provides for statutory damages, at a minimum of US$1,000 per violation, although some courts have recognised that plaintiffs may claim the statutory amount only upon a showing of having incurred at least some actual damage as well.[33] To date, however, courts in data breach cases have usually found that those statutes target specified harms other than those underlying the claims in question. Claims under the FCRA, thus, have been rejected in the data breach context because the statute applies only to 'consumer reporting agencies' and addresses only 'furnishing' of data.[34] Similarly, alleged violations of the SCA have been rejected because the statute applies only to covered providers of covered communications who 'knowingly divulge'[35] the data in question.[36] Claims based on the violation of other federal statutes imposing data security requirements or restricting disclosure of personal information also fail if the relevant statute does not provide a private right of action.[37]

30 15 USCA Section 1681e(a).

31 Note that if a person knowingly violates the statute, liability increases to the greater of actual damages sustained by the consumer or US$1,000. 15 USCA Section 1681n(a)(1)(A) and (B).

32 See, e.g., *Tierney v. Advocate Health & Hosps. Corp.*, 797 F.3d 449, 450 (7th Cir 2015); *In re Equifax, Inc., Customer Data Sec. Breach Litig.*, 362 F. Supp. 3d 1295, 1313 (ND Ga 2019); *Sony II*, 996 F. Supp. 2d at 959.

33 18 USCA Sections 2702 and 2707(c); *Vista Marketing, LLC v. Burkett*, 812 F.3d 954, 965 and 967 (11th Cir 2016) (interpreting the language of the statute to provide damages only to plaintiffs who experienced actual damages); but see *Cline v. Reetz-Laiolo*, 329 F. Supp. 3d 1000, 1045 (ND Cal 2018) (noting that district courts in the Ninth Circuit have held that plaintiffs can obtain damages under the SCA without a showing of actual damages).

34 See, e.g., *Tierney*, 797 F.3d at 451 and 452; *Sony II*, 996 F. Supp. 2d at 1011; *In re Equifax, Inc., Customer Data Sec. Breach Litig.*, 362 F. Supp. 3d 1295, 1312 (ND Ga 2019).

35 18 USCA Section 2702(a)(1) to (3).

36 *In re: Yahoo! Inc. Customer Data Sec. Breach Litig.*, No. 16-MD-02752, 2017 WL 3727318, at *41 and *42 (ND Cal 30 Aug 2017) (plaintiffs failed to allege that defendants knowingly divulged any information); *Burrows v. Purchasing Power*, LLC, No. 12-CV-22800, 2012 WL 9391827, at *4 and *5 (SD Fla 18 Oct 2012) (plaintiff failed to plead facts showing that defendant was a covered entity under the SCA or that defendant knowingly divulged plaintiff's PII).

37 See, e.g., *In re: Anthem, Inc. Data Breach Litig,* 162 F. Supp. 3d, , 897 and 898, 980 and 981 (ND Cal 2016) (claim failed because the Health Insurance Portability and Accountability Act of 1996 [HIPAA] has no private right of action); *Weinberg v. Advanced Data Processing, Inc.*, 147 F. Supp. 3d 1359, 1368 and 1369 (SD Fla 2015) (same); *Abdale v. N. Shore Long Island Jewish Health Sys., Inc.*, 19 N.Y.S. 3d 850, 859 (NY Sup Ct 2015) (same under the Health Information Technology for Economic and Clinical Health Act). But see *In re: Premera Blue Cross Customer Data Sec. Breach Litig.*, 198 F. Supp. 3d 1183, 1202 and 1203 (D Or 2016) (lack of a private right of action under HIPAA did not preclude causes of action under state law even if an element of the state claim required showing a HIPAA violation). Well-pleaded violations of these statutes have in some instances survived motions to dismiss if styled as causes of action for negligence *per se*. Compare *First Choice Fed. Credit Union v. Wendy's Co.*, No. CV 16-506, 2017 WL 9487086, at *3 and *4 (WD Pa 13 Feb 2017), report and recommendation adopted, No. CV 16-506, 2017 WL 1190500 (WD Pa 31 Mar 2017) (declining to dismiss negligence *per se* claim premised on alleged violation of the FTC Act), with *Community Bank of Trenton v.*

In addition to federal statutes, plaintiffs may attempt to assert claims under various state laws. As of 2018, all 50 states and the District of Columbia have data breach notification statutes of varying scope.[38] Yet even when those statutes provide a private right of action,[39] claims for insufficient or untimely notice often fail for lack of claimed injury stemming from the insufficiency or untimeliness itself.[40] Similarly, a number of state statutes also include provisions imposing security standards with respect to protecting personal information[41] and some permit private rights of actions to be asserted – either directly or indirectly – for non-compliance.[42]

The landscape of state statutes changed dramatically in January 2020 when the California Consumer Privacy Act (CCPA) became operational. The CCPA provides a private right of action to California consumers[43] for certain failures to maintain 'reasonable security' resulting in a data breach and, significantly, provides for statutory damages of between US$100 and US$750 'per consumer per incident'.[44] The statute provides defendants an opportunity to cure any breach within 30 days, but it is unclear in practice how defendants would do so. Private litigation invoking the CCPA has begun, though as of yet decisions interpreting the CCPA are sparse. Defendants have raised questions concerning the scope and application of the private right of action, such as whether it applies retroactively to incidents before 1 January 2020[45] and whether defendants were provided adequate notice and opportunity to cure.[46] Defendants have also raised arguments regarding whether the data at issue is 'personal

Schnuck Markets, 887 F.3d 803, 819 n.7 (7th Cir 2018) (dismissing negligence *per se* claim based on alleged violation of the FTC Act).

38 See Security Breach Notification Laws, Nat'l Conf. of State Legs. (19 Sep 2018), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

39 The Alabama statute, for example, expressly states that it does not provide for a private right of action. 2018 Ala. Laws Act 2019-396 Section 9(a)(1) (SB 318) (setting forth notification requirements in the event of a data breach but expressly noting that '[a] violation of this act does not establish a private cause of action').

40 See, e.g., *Gordon v. Chipotle Mexican Grill, Inc.*, 344 F. Supp. 3d 1231, 1253 to 1255 (D Colo 2018) (claim under state breach notification statute for failing to promptly notify customers dismissed as to plaintiffs who had learned of and taken action regarding fraudulent transactions before defendant learned of breach, and who thus could not allege harm due to delay in notice); *In re Yahoo! Inc. Customer Data Sec. Breach Litig.*, 16-MD-02752, 2017 WL 3727318, at *37 and *38 (ND Cal 30 Aug 2017) (dismissing delay claim by Yahoo! plaintiffs for 2013 breach because liability arises only from delay and not from breach itself, and plaintiff failed to allege when 2013 breach was discovered); ibid., at *40 and *41 (discussing other cases in which delay claims failed for lack of direct injury, but holding that delay claims by Yahoo! plaintiffs as to 2014–2016 breaches adequately alleged a direct connection between alleged incremental damages and the claimed delay).

41 See Data Security Laws – Private Sector, Nat'l Conf. of State Legs. (4 Jan 2019), www.ncsl.org/research/telecommunications-and-information-technology/data-security-laws.aspx.

42 Ca. Civil Code, Section 1798.81.5(b); Ill. Comp. Stat. 815 ILCS 530/45(a); Md. Code. Ann. Com. Law 14-3503(a).

43 Ca. Civil Code, Section 1798.140(g) (defining 'consumer' as 'a natural person who is a California resident').

44 Ca. Civil Code, Section 1798.155(b).

45 See, e.g., *Gardiner v. Walmart, Inc.*, No. 4:20-cv-04618-JSW (ND Cal 5 Mar 2021) (dismissing claim because breach may have occurred before 1 January 2020).

46 See, e.g., *Guzman v. RLI Corp. et al.,* No. 2:20-cv-08318 (CD Cal 22 Oct 2020) (Doc. 26-1) (arguing plaintiff did not comply with notice and cure provision).

information', which is defined more narrowly with respect to the private right of action than under the statute as a whole.[47]

At the close of 2020, California voters passed a ballot initiative, Proposition 24, known as the California Privacy Rights Act (CPRA) that will go into operation in 2023. Of relevance to the data-breach cause of action, it will eliminate the right to cure. Legislative proposals are also pending in other states that may include new rights of action.[48]

Emerging trends in litigation: securities litigation

While the most common cybersecurity actions continue to be class actions brought by individuals whose information was allegedly compromised under the foregoing theories, recent years have seen an increase in shareholder derivative and securities fraud actions as well.

Shareholder derivative actions

Shareholder derivative actions have followed most prominent data breaches since at least the Target breach in 2013. In these actions, plaintiffs allege that directors and officers breached their fiduciary duties, committed gross mismanagement, wasted corporate assets or abused their control in failing to oversee the company's cybersecurity posture.[49] Thus far, plaintiffs have had limited success with these allegations,[50] with one some exceptions.[51]

Defendants often succeed in dismissing shareholder derivative actions because plaintiffs must plead with particularity that either (1) the board of directors wrongfully refused to bring the suit, or (2) it would have been futile to request that the board bring such an action.[52] This leaves plaintiffs in a challenging position. Under Delaware law, if plaintiffs ask the board to bring the action, when the board says no (which is likely to be the case), the plaintiff must prove the board's decision was outside the bounds of the business judgement

47 See, e.g., *Walmart, Inc.*, No. 4:20-cv-04618-JSW (ND Cal 5 Mar 2021) (finding failure to allege disclosure of personal information meeting definition under privacy right of action).

48 See, e.g., SD 341, 2019 Sen., 191st Sess. (Mass 2019); SB 179, 54th Leg., Reg. Sess. (NM 2019); S. 0234, 2019 Gen Assembly (RI 2019).

49 See, e.g., Complaint at paras. 3 to 7, *Davis v. Steinhafel*, No. 14-cv-00203 (D Minn 21 Jan 2014); *In re: The Home Depot Inc. S'holder Derivative Litig.*, 223 F. Supp. 3d 1317 (ND Ga 2016).

50 See, e.g., *Corp. Risk Holdings LLC v. Rowlands*, No. 17-cv-5225(RJS), 2018 WL 9517195, at *6 (SDNY 28 Sept 2018) (dismissing claims of breach of fiduciary duty where plaintiffs plead 'nothing more than industry-wide generalisations about cybersecurity risks, not company-specific evidence of misconduct or compliance failure necessary to sustain a claim for director liability'.).

51 *In re Equifax Inc. Securities Litigation*, 357 F.Supp.3d 1189 (ND Ga 2019) (denying motion to dismiss claims against Equifax's former CEO and chairman of the board based on allegations of personal knowledge of inadequate cybersecurity practices, and knowingly and recklessly making false and misleading about Equifax's data security). Similarly, in the matter *In re: Yahoo! Inc. Shareholder Litigation*, No. 17-cv-307054 (ND Cal 9 Jan 2019), the court approved an US$29,000,000 shareholder settlement on 9 Jan 2019. The settlement marked the first time that shareholders were awarded monetary damages in a derivative lawsuit relating to a data breach.

52 See Fed. R. Civ. P. 23.1(b)(3); *Palkon v. Holmes*, No. 2:14-CV-01234 SRC, 2014 WL 5341880, at *2 (DNJ 20 Oct 2014) (plaintiff brought suit alleging board wrongfully refused to bring action); Complaint at para. 7, *Graham v. Peltz*, No. 1:16-cv-1153 (SD Oh 16 Dec 2016) (plaintiff alleged that it would have been futile to request the board bring the action); *In re: the Home Depot*, 223 F. Supp. 3d at 1324 (same).

rule – an exceedingly difficult task.[53] However, if the plaintiffs argue that demand would be futile, they have to show that the majority of directors were conflicted owing to a significant likelihood that the directors faced individual liability or that the board failed to inform themselves to the extent appropriate under the circumstances.[54]

Stock purchase class action complaints

Securities fraud litigation following a data security incident is also on the rise. In fact, in 2017 and 2018, plaintiffs filed 23 federal securities class actions based on a data security incident, compared to zero in 2016.[55] The widely publicised data breach at Marriott International (Marriott) demonstrates how popular these types of actions had become by the end of 2018. Marriott publicly announced that it had suffered a data security incident on Friday, 30 November 2018, and the first securities class action lawsuit was filed the next day.[56] Similarly, in 2019 and 2020, plaintiffs continued to file such class actions with respect to notable data security incidents including the Capital One breach.[57]

While complaints like the one filed in Marriott frequently lack extensive *scienter* allegations, and sometimes even lack evidence of a significant drop in stock price, plaintiffs' lawyers hope to defeat a motion to dismiss by alleging two (non-exclusive) theories. First, plaintiffs, like those in *Marriott*,[58] will allege that public statements were materially false or misleading because the company overstated its cybersecurity abilities, or otherwise failed to inform investors that the company was susceptible to a cyberattack.[59] Second, similar to a traditional

53 See, e.g., *Palkon*, 2014 WL 5341880, at *3 (dismissing claims under Delaware law because plaintiffs failed to plead reasonable doubt regarding business judgement rule); *Zapata Corp. v. Maldonado*, 430 A.2d 779, 785 (Del 1981) ('To allow one shareholder to incapacitate an entire board of directors merely by leveling charges against them gives too much leverage to dissident shareholders.') (citation omitted).

54 See, e.g., *In re: The Home Depot*, 223 F. Supp. 3d at 1325 (stating the Delaware law requirement for testing board's independence as a showing that board engaged in conduct 'so egregious on its face that board approval cannot meet the test of business judgment, and a substantial likelihood of director liability therefore exists'). See also *Marx v. Akers*, 666 N.E. 2d 1034, 1040 (NY Ct App 1996) (stating demand excuse requirements under New York law).

55 'Securities Fraud Claims Get Boost from EU Data Privacy Rules', Bloomberg Privacy & Security Law Report (BNA) (1 Feb 2019).

56 Complaint, *McGrath v. Marriott International, Inc.*, No. 18-cv-06845 (EDNY 1 Dec 2018) [*Marriott* Complaint]. Notably, the first consumer class action was filed even more quickly – on 30 November 2018, the same day the breach was announced.

57 *Minsky v. Capital One*, No. 1:19-cv-05594 (EDNY 2 Oct 2019); for a broader list, see *The Stanford Law School Securities Class Action Clearinghouse*. Stanford Law School, https://securities.stanford.edu/current-topics.html#collapse1 (last visited 10 March 2021).

58 The *Marriott* plaintiffs alleged that Marriott's Form 10-Q filed with the Securities and Exchange Commission gave the 'misleading impression' that systems storing customer data were secure. *Marriott* Complaint, at paras. 17 to 22. News of the breach broke before trading opened on 30 November 2018; by the end of the trading day, Marriott's stock fell more than 5.5 per cent; ibid., at paras. 24 and 25.

59 See *Kim v. Advanced Micro Devices, Inc.*, No. 18-cv-00321, 2018 WL 2866666, at *1 (ND Cal 11 Jun 2018); *In re: Equifax Inc. Sec. Litig.*, No. 17-cv-3463, 2019 WL 337807, at *9 (ND Ga 28 Jan 2019); Complaint at para. 4, *In re: Intel Corp. Sec. Litig.*, No. 18-cv-00507 (ND Cal 23 Jan 2018) [*In re: Intel Corp*. Complaint]; *Marriott* Complaint, at para. 23.

consumer class action, plaintiffs will allege that the company knew about a cyberattack, but did not disclose it to the market in a timely manner.[60]

While not necessary to bring a securities fraud action, allegations of insider stock sale prior to the public disclosure of the breach can accompany Section 10b-5 claims.[61]

Key strategic considerations in litigation

Non-litigation focused decisions made after a cyberattack may be critical

After a cyberattack, an affected party may want to reassure partners, customers and the general public that any damage was minimal, that it has strong cybersecurity to prevent further attacks, and that it will mitigate the harm caused. However, such actions taken in the first few days (or even hours) of learning of a breach can have a profound effect on litigation that will inevitably follow, and thus those actions must be considered carefully.

A company that is aware of a data security incident should pay special attention to any public statements about the company's data security. This includes statements in routine public filings. As noted above, deception and implied contract-based claims turn, in part, on the company's statements relating to its data security. As a result, when considering whether and how much to disclose, companies should be mindful that the disclosures may eventually be cited in support of an allegation that the company overstated or misled consumers as to its practices.

When a company has disclosed a data security incident, it should be equally cautious about how it describes the extent of a breach. While defendants have had success in challenging plaintiffs' standing to bring suit, recent court decisions demonstrate that a company's public comments can undercut arguments regarding a lack of standing as a ground for dismissal. For example, in the aftermath of a breach, Zappos urged 'affected customers to change their passwords on any other account where they may have used the same or similar password' as for their Zappos account.[62] The Ninth Circuit pointed to that statement to establish that the plaintiffs sufficiently alleged an injury based on a substantial risk that the hackers would commit identity fraud or theft.[63]

Another hard question a company may face after a breach is deciding whether to offer affected customers free credit monitoring.[64] This is often seen as good customer service (and, depending on the circumstances and the information affected, may be required by a number of state data breach notification laws). From a litigation perspective, if there is harm, credit monitoring could mitigate it, and some courts have found that free credit monitoring elimi-

60 *In re: Equifax*, 2019 WL 337807, at *14 and *15.

61 See, e.g., Amended Consolidated Complaint at para. 199, *In re: Equifax Inc. Sec. Litig.*, No. 17-cv-3463 (ND Ga 14 May 2018) (alleging that three high-level executives sold millions of dollars of Equifax stock before publicly disclosing the incident); *In re: Intel Corp*. Complaint at para. 9 (alleging that Intel's Chief Executive Officer sold US$24 million worth of the company's stock and options after Intel was informed of data security vulnerabilities but before that information was disclosed publicly).

62 *In re: Zappos.com, Inc.*, 888 F.3d 1020, 1027 and 1028 (9th Cir 2018) (quotation marks and footnote omitted).

63 ibid., at 1029.

64 Note that, in a few states, an offer of some period of identity protection or remediation services to residents of those states is in any event now required by statute for a set period of years. Conn. Gen. Stat. Ann. Section 36a-701b(b)(2)(B) (two years); Del. Code Ann. tit. 6, Section 12B-102(e) (one year); Mass. H. 4806 (2018) (18 months).

nates the need for plaintiffs to purchase their own and thus removes one means by which a plaintiff can demonstrate injury-in-fact.[65] However, some courts have treated an offer for free credit monitoring as an admission that consumers face a substantial risk of harm.[66] Notably, some courts that take the former view observe that to use an offer of credit monitoring to establish standing would discourage organisations from offering these services.[67]

Finally, in the aftermath of a cyberattack, and as discussed further in Chapter 3 on The 'Art' of Investigating, a company is likely to want to (and should) act quickly to investigate the cause of the attack and its potential ramifications. However, the structure of any internal investigation – whether it is intended to inform counsel in providing legal advice or for a different purpose – may affect whether related documents and communications are protected by the attorney–client privilege or work-product doctrine. A company responding to a breach should therefore consider designing and executing an internal investigation to protect the company's claim to privilege to the fullest extent.[68] In particular, a company should consider recent decisions regarding the application of the work-product doctrine and attorney–client privilege to forensic reports generated by third parties when determining how to structure an investigation and engage a third party.[69]

Judicial Panel on Multidistrict Litigation

In the wake of a large data breach in particular, corporations should anticipate that actions will be filed in multiple jurisdictions and should devise strategies to consolidate those actions in a jurisdiction with laws that are the most appropriate for the case.

When cases are filed in a single judicial district, judges frequently entertain motions to consolidate. When cases are filed in multiple jurisdictions – a common occurrence when the pool of potential plaintiffs is geographically diverse – a defendant or plaintiff can seek to transfer and consolidate the federal cases before one district court for pretrial purposes via a centralisation motion filed with the Judicial Panel on Multidistrict Litigation (JPML). The seven circuit and district judges on the JPML, appointed by the Chief Justice of the United States, have the authority to transfer federally pending cases involving 'common questions

65 *Falkenberg v. Alere Home Monitoring, Inc.*, No. 13-341, 2014 WL 5020431, at *4 (ND Cal 7 Oct 2014) (dismissing claims under California law).

66 *Galaria v. Nationwide Mut. Ins. Co.*, 663 F. App'x 384, 388 (6th Cir 2016) ('Nationwide seems to recognize the severity of the risk [of fraud and identity theft], given its offer to provide credit-monitoring and identity-theft protection for a full year.'). Query if that rationale holds where the offer is required by statute. See footnote 58 and accompanying text.

67 *Beck v. McDonald*, 848 F.3d 262, 276 (4th Cir 2017).

68 Compare *In re: Target Corp. Customer Data Sec. Breach Litig.*, No. 14-2522, 2015 WL 6777384, at *2 and *3 (D Minn 23 Oct 2015).

69 See, e.g., *In re Target Corp. Customer Data Sec. Breach Litig.*, MDL No. 14-2522 (PAM/JJK), 2015 WL 6777384, at *1-2 (D Minn 23 Oct 2015 (holding the attorney client privilege and work product document applied to communications from third-party forensic consultant retained to assist counsel in conducting investigation); *Genesco, Inc. v. Visa U.S.A., Inc.*, 302 F.R.D. 168, 190–93 (MD Tenn 2014) (same). But see *In re Capital One Consumer Data Sec. Breach Litig.*, 2020 WL 3470261 (ED Va 25 June 2020) (holding work product doctrine did not protect forensic report Capital One argued was prepared for counsel); *Guo Wengui v. Clark Hill*, PLC, et al., 2021 WL 106417 (DDC 2021) (finding the same with respect to the work product doctrine and attorney–client privilege).

of fact' for consolidated or coordinated pretrial proceedings.[70] The jurisdiction of the JPML, however, does not extend to cases pending in state court. Therefore, unless the state cases are removable to federal court, defendants may be forced to litigate the same claims on two fronts, or at least incur additional expenses seeking to coordinate proceedings across the federal and state systems.[71]

Choice of law variances

The importance of the state law applied to a data breach litigation cannot be overstated. For example, in November 2018, the Supreme Court of Pennsylvania held in *Dittman v. UPMC* that an employer has a legal duty to exercise reasonable care to safeguard the sensitive personal information about employees that is stored on any internet-accessible computer system.[72] In contrast, Illinois cases have declined to impose any duty to safeguard PII from disclosure[73] and the Georgia Court of Appeals has similarly found no duty under Georgia law to safeguard personal information.[74] The *Dittman* court further held that Pennsylvania's economic loss doctrine provides recovery for purely pecuniary damages under a negligence theory, provided that the plaintiff can establish the defendant's breach under common law is independent of any duty assumed pursuant to contract.[75] Unlike Pennsylvania, courts applying New York and California law find that the economic loss doctrine bars negligence claims for purely pecuniary damages.[76]

Interestingly, choice of law provisions sometimes require one court to apply the law of multiple states in the same action. This can happen, for example, when geographically diverse plaintiffs were all injured in their home states. Defendants in class actions generally are starting to point to these plaintiff-specific variances to defeat class certification under Federal Rule of Civil Procedure 23(b)(3), which permits class actions only if 'the court finds that the questions of law or fact common to class members predominate' over those affecting only

70 28 USC Section 1407(a). See, e.g., *In re: Marriott International, Inc., Customer Data Sec. Breach Litig.*, No. MDL 2879, 2019 WL 623593 (JPML 6 Feb 2019) (centralising both consumer class actions and stockholder securities actions stemming from Marriott's data security incident).

71 See, e.g., *In re: Uber Techs., Inc., Data Sec. Breach Litig.*, 304 F. Supp. 3d 1351, 1354 (JPML 2018) (granting centralisation of pending federal data breach class actions in single federal district, while noting the continuing pendency of parallel state court actions).

72 *Dittman v. UPMC*, 196 A.3d 1036, 1047 (Pa 2018).

73 *Cooney v. Chicago Pub. Sch.*, 943 NE 2d 23, 28 and 29 (Ill App Ct 2010); see also *In re: SuperValu, Inc., Customer Data Sec. Breach Litig.*, No. 14-MD-2586 ADM/TNL, 2018 WL 1189327, at *14 (D Minn 7 Mar 2018) ('Federal courts interpreting Illinois law have consistently declined to impose a common law duty to safeguard personal information in data security cases.' (citation omitted)).

74 *McConnell v. Dep't of Labor*, 828 S.E.2d at 358 (Ga 2019); but see *In re: The Home Depot, Inc., Customer Data Sec. Breach Litig.*, No. 1:14-MD-2583-TWT, 2016 WL 2897520, at *4 (ND Ga 18 May 2016) (footnotes omitted).

75 *Dittman*, 196 A.3d at 1056.

76 See footnote 13 and accompanying text.

individual members.[77] Given the range of differences between the common law and statutory causes of action asserted by plaintiffs, the same rationale would apply in data breach cases.[78]

Class certification timing

Class certification, and the timing of it, can also have a significant effect on a case. Some courts are willing to bifurcate class certification discovery and merits discovery. If a defendant believes that it can successfully defeat class certification,[79] it can save significant time and money by using bifurcated discovery and having class certification addressed early. If the defendant wins on its opposition to class certification, it may be able to settle the action with the named plaintiffs for a minimal amount, avoiding expensive discovery on merits issues collateral to the class certification issue itself.[80]

However, plaintiffs' lawyers are often reluctant to agree to an early ruling on class certification, lest they cede the settlement leverage that the cost and burdens of discovery may afford them in the interim. Accordingly, they will frequently oppose bifurcating discovery and argue that class certification is so intermingled with the merits of the case that full discovery is required before any motions are filed.[81]

77 See *In re: Hyundai & Kia Fuel Econ. Litig.*, 881 F.3d 679, 691 to 693, 703 (9th Cir 2018), rehearing *en banc* granted *sub nom. In re: Hyundai And Kia Fuel Econ. Litig.*, 897 F.3d 1003 (9th Cir 2018) (in a putative class action regarding car manufacturers' alleged misstatements about fuel efficiency, the Ninth Circuit found that the district court abused its discretion by (1) failing to acknowledge that the laws in various states were materially different from those in California, and (2) not ruling on whether the variations would defeat predominance); *Langan v. Johnson & Johnson Consumer Cos., Inc.*, 897 F.3d 88, 98 (2d Cir 2018) (in a putative class action against the seller of baby bath products, the Second Circuit noted that the party seeking class certification has the ultimate burden of demonstrating that any variances in state laws do not predominate and that the district court must engage in a rigorous analysis of the similarities and differences in the relevant laws).

78 See, e.g., *In re: Conagra Peanut Butter Prod. Liab. Litig.*, 251 F.R.D. 689, 699 (ND Ga 2008) ('It goes without saying that class certification is impossible where the fifty states truly establish a large number of different legal standards governing a particular claim.') (quotations omitted); but see Memorandum and Order at 5 to 9, *In re: Target Corp. Customer Data Sec. Breach Litig.*, No. 14-2522 (D Minn 15 Sep 2015) (rejecting argument that because negligence claims are subject to laws of different states class treatment of those claims is inappropriate). For an example of when questions of fact did not predominate the class, see *In re: TJX Companies Retail Sec. Breach Litig.*, 246 F.R.D. 389, 395 and 396 (D Mass 2007).

79 See, e.g., *McGlenn v. Driveline Retail Merch., Inc.*, 2021 U.S. Dist. LEXIS 9532, 15 (CD Ill. Jan. 19, 2021) (denying data breach class certification, in part, because 'issues of causation and injury require individual inquiry').

80 See *Harris v. comScore, Inc.*, No. 11 CV 5807, 2012 WL 686709 (ND Ill 2 Mar 2012) (bifurcating class certification discovery from merits discovery in class action involving alleged collection and dissemination of personal information in violation of state and federal laws). See also Manual for Complex Litigation (Fourth) Section 21.14 (2018).

81 Compare *New England Carpenters Health & Welfare Fund v. Abbott Labs*, No. 12 C 1662, 2013 WL 690613, at *3 (ND Ill 20 Feb 2013) (denying bifurcation, accepting plaintiff's argument that 'merits and class certification issues inevitably overlap, bifurcation will serve only to needlessly protract this litigation') (internal quotations and citation omitted), with *comScore*, 2012 WL 686709 (granting bifurcation, rejecting plaintiffs' arguments regarding 'delay' and anticipated disagreements about the 'permissible scope of class certification discovery').

Current range of holdings on injury requirements

As with all plaintiffs seeking to bring litigation in a US federal court, data breach plaintiffs must allege an injury-in-fact sufficient to confer standing under Article III of the US Constitution.[82] Article III limits the jurisdiction of federal courts to cases or controversies in which the plaintiff demonstrates that he or she has suffered (1) an injury-in-fact (2) that is fairly traceable to the defendant's actions and (3) is likely to be redressed by the relief sought from the court.[83] In this section, we discuss two recent landmark Supreme Court decisions on Article III's injury-in-fact requirement and the resulting circuit splits regarding injury needed to sufficiently plead standing in data breach cases in federal court. This section also considers how – even when standing is satisfied – different claims of injury fare in alleging the requisite elements of the cause of action itself.

Standing: current versus future injury

Under the Supreme Court's 2013 ruling in *Clapper v. Amnesty International USA*, to establish injury-in-fact, plaintiffs must allege injury that has already accrued or threatened injury that is 'certainly impending'.[84] This decision notes that a plaintiff cannot manufacture current injury by spending money to avoid future harm, if that future harm itself is not certainly impending.[85] Circuits have subsequently split over the decision's application in litigation resulting from a data breach.

Four circuits – the D.C., Sixth, Seventh and Ninth – have held that individuals whose personal information is held in a database breached by hackers have Article III standing by virtue of substantial risk of future out-of-pocket injury.[86] As explained by the DC Circuit: 'simply by virtue of the hack and the nature of the data that the plaintiffs allege was taken', plaintiffs have experienced a substantial risk of harm that is sufficient to establish injury.[87] In contrast, under a range of factual circumstances, the First, Second, Third, Fourth and Eighth Circuits have held that the mere risk of data misuse is too speculative to create standing

82 Note that constitutional standing concerns do not arise in shareholder derivative or stock purchase cases, since the ownership or purchase of the stock in and of itself suffices to provide standing to challenge the actions of the company or its officers and directors with respect to the breach in question. Fed. Rule Civ. Pro. 23(b)(1) (detailing standing requirements to bring a derivative action); *Blue Chip Stamps v. Manor Drug Stores*, 421 U.S. 723, 753 and 754 (1975) (finding Congress intended to limit standing in cases brought under the Exchange Act to plaintiffs who had purchased stock).

83 *Spokeo, Inc. v. Robins*, 136 S.Ct. 1540, 1547 (2016) (quoting *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560 (1992).

84 *Clapper v. Amnesty Int'l USA*, 133 S.Ct. 1138, 1143 (2013).

85 ibid., at 1151; see also *Stasi v. Inmediata Health Grp. Corp.*, No. 19cv2353 JM (LL), 2020 WL 2126317, at *9 (SD Cal 2020) ('Plaintiffs cite no case in which the expenditure of time or money to prevent future identity theft was sufficient in and of itself to support standing without a finding that the threat of identity theft was imminent.').

86 *Attias v. CareFirst*, 865 F.3d 620, 629 (DC Cir 2017); *In re Office of Pers. Mgmt. Data Sec. Breach Litig.*, 928 F.3d 42, 54-61 (DC Cir 2019); *Galaria v. Nationwide Mutual Ins. Co.*, 663 F. App'x 384, 388 and 389 (6th Cir 2016); *Remijas v. Neiman Marcus Grp. LLC*, 794 F.3d 688, 693 (7th Cir 2015); *Lewert v. P.F. Chang's China Bistro, Inc.*, 819 F.3d 963, 967 (7th Cir 2016); *In re: Zappos.com*, 888 F.3d 1020, 1025 and 1026 (9th Cir 2018); see also *In re: Horizon HealthCare Servs. Inc. Data Breach Litig.*, 846 F.3d 625, 630, 638 and 639 (3d Cir 2017) (finding standing based on de facto injuries under a federal privacy law).

87 *Attias*, 865 F.3d at 629.

because no injury is 'certainly impending' nor is there a 'substantial risk' of injury.[88] The Eleventh Circuit has held similarly in an unpublished decision.[89]

Standing: tangible versus intangible injury

The Supreme Court's 2016 decision in *Spokeo, Inc. v. Robins* addressed a slightly different question: what makes an injury sufficiently concrete to confer standing. The Court explained that, to be concrete, the injury must 'actually exist' and that 'risk of real harm' could satisfy the concreteness standard.[90]

While out-of-pocket loss that is actually and already incurred is considered sufficient tangible harm to establish injury-in-fact, other alleged injuries have been found intangible and insufficient to confer standing. For example, some courts find that alleged anxiety, inconvenience and lost time caused by a data breach are not particularised and are not sufficiently concrete to confer standing, though that finding is not universal.[91] Courts often reject standing based on a diminished value of PII; although, some recent decisions have accepted the theory.[92]

Increasingly, plaintiffs allege they have suffered a concrete harm because they 'overpaid' for a good or service. This theory is premised on the idea that because the purchase of goods or services created the circumstances in which the purchaser's personal data was potentially affected by a subsequent breach, the purchaser overpaid for the goods or services.[93] The overpayment theory is attractive to plaintiffs because, apart from standing, it may also provide a basis for establishing uniform damages across the class. Yet if the plaintiff fails to allege any defect in the product or service itself, or that security itself was identified as part of the

88 See *Katz v. Pershing*, LLC, 672 F.3d 64, 80 (1st Cir 2012); *Whalen v. Michaels Stores, Inc.*, 689 F. App'x 89, 90 (2d Cir 2017); *Reilly v. Ceridian Corp.*, 664 F.3d 38, 42-43 (3d Cir 2011) (no standing under common law principles); *Beck v. McDonald*, 848 F.3d 262, 274 (4th Cir 2017); *In re: SuperValu, Inc.*, 870 F.3d 763, 771 (8th Cir 2017).

89 *Tsao v. Captiva MdVP Restaurant Partners*, 2021 U.S. App. LEXIS 3055 (11th Cir 4 Feb 2021).

90 *Spokeo*, 136 S.Ct. 1540, 1548 and 1549.

91 Compare, *Whalen*, 689 F. App'x at 90; *Fero v. Excellus Health Plain, Inc.*, 236 F. Supp. 3d 735, 754 (WDNY 2017), on reconsideration *sub nom. Fero v. Excellus Health Plan, Inc.*, 304 F. Supp. 3d 333 (WDNY 2018), with *Bass v. Facebook*, 393 F. Supp. 3d 1024, 1034 (ND Cal 2019 (loss of time in responding to breach sufficient for standing).

92 *In re Uber Techs., Inc., Data Sec. Breach Litig.*, No. CV182970PSGGJSX, 2019 WL 6522843, at *5 (CD Cal 19 Aug 2019) (rejecting diminution of value theory where plaintiff had not established an impairment of his ability to participate in that market for personal information); *Mount v. PulsePoint, Inc.*, No. 13 CIV. 6592, 2016 WL 5080131, at *6 (SDNY 17 Aug 2016), aff'd, 684 F. App'x 32 (2d Cir 2017), as amended (3 May 2017) (rejecting diminished value of PII theory on grounds that it was too conjectural); *Khan v. Children's Nat'l Health System*, 188 F. Supp. 3d 524, 533 (D Md 2016) (allegation that data breach diminished the value of PII rejected as a theory to support standing because the breach did not deprive plaintiff of her PII). But see *In re Experian Data Breach Litig.*, No. SACV 15-1592 AG (DFMx), 2016 WL 7973593, at *5 (CD Cal 29 Dec 2016) ('A growing number of federal courts have now recognized Loss of Value of PII as a viable damages theory.').

93 See *Lewert*, 819 F.3d at 968 (product itself must be defective and purchaser must claim they would not have bought it had they known of the defect); *Neiman Marcus,* 794 F.3d at 694 (noting in *dicta* that it is 'dubious' overpayment allegations alone suffice for standing).

product or service being purchased, efforts to use allegations of 'overpayment' alone to satisfy standing in data breach cases have so far not had great success.[94]

Alleging solely the violation of a statute to establish standing, moreover, could suffice under *Spokeo* if (1) there is a 'close relationship' between the harm alleged and 'a harm that has traditionally been regarded as providing a basis for a lawsuit in English or American courts'; and (2) the statute being enforced reflects Congress' judgment that the alleged harm meets minimum Article III requirements.[95] Acknowledging that Congress can elevate an intangible harm to a concrete injury through legislation, the Third Circuit currently leaves open the possibility of rejecting 'mere technical violations' of a statutory procedural requirement in determining injury-in-fact.[96] In any event, standing after *Spokeo* continues to be a significant jurisdictional issue that federal courts must consider and address and that can be raised at any level of litigation.[97]

Actionable injury: sufficiency for the cause of action

The fact that a plaintiff's injury is sufficient to confer Article III standing does not mean it is sufficient to state a claim for damages under Rule 8(a)(2) of the Federal Rules of Civil Procedure. Indeed, separate and apart from standing issues, and even if the theories of liability as laid out in 'Typical causes of action in US litigation' (above) are otherwise sustained, a notable stumbling block for many cybersecurity plaintiffs has long been, and continues to be, the failure to allege injury sufficient to state a claim.[98] For example, costs incurred from actual misuse of stolen information have been held actionable only if there is an actual out-of-pocket loss.[99] A mere increased risk of future identity theft can be rejected as insufficient as actionable injury,[100] while credit monitoring costs, lost time and other mitigation measures

94 See, e.g., *Lewert*, 819 F.3d at 968 (failing to allege defect); *Neiman Marcus*, 794 F.3d at 694 (same); *Cox v. Valley Hope Ass'n*, No. 16-CV-04127-NKL, 2016 WL 4680165, at *3 and *4 (WD Mo 6 Sep 2016) (failing to allege that defendant represented cost of services as including data security measures).

95 *Spokeo*, 136 S.Ct. at 1549 (citations omitted).

96 *In re: Horizon HealthCare Servs. Inc. Data Breach Litig.*, 846 F.3d at 638 to 641 (court does not opine on the types of 'mere technical violations' that would be insufficient to confer standing).

97 After granting writ of *certiorari* and hearing oral arguments in *Frank v. Gaos*, the Supreme Court declined to reach the merits of the case, instead remanding it to the courts below to address plaintiffs' standing in light of *Spokeo. Frank v. Gaos*, 139 S.Ct. 1041, 1046 (2019) (*per curiam*).

98 See, e.g., *Kuhns v. Scottrade*, 868 F.3d 711, 716 and 717 (8th Cir 2017) (plaintiffs with Article III standing nevertheless failed to allege harm sufficient to state a breach of contract claim); *Krottner v. Starbucks Corp.*, 406 Fed. App'x 129, 131 (9th Cir 2010) (same for claim of negligence); *Moyer v. Michaels Stores, Inc.*, No. 14 C 561, 2014 WL 3511500, at *6 and *7 (ND Ill 14 July 2014) (same for breach of contract and consumer fraud claims); but see *Dieffenbach v. Barnes & Noble, Inc.*, 887 F.3d 826, 828 (7th Cir 2018) ('To say that the plaintiffs have standing is to say that they have alleged injury in fact, and if they have suffered an injury then damages are available.').

99 See, e.g., *Sony I*, at 942, 962 and 963 (plaintiffs' negligence claim failed due to absence of allegations of misuse or un-reimbursed charges or alleged problems with game consoles post-breach); *In re: Hannaford Bros. Co. Customer Data Sec. Breach Litig.*, 613 F. Supp. 2d 108, 133 to 135 (D Me 2009), aff'd in part, rev'd in part *sub nom. Anderson v. Hannaford Bros. Co.*, 659 F.3d 151 (1st Cir 2011) (fraudulent charges that are reversed or reimbursed held insufficient to meet injury elements of claim for negligence, breach of contract or violation of Maine Unfair Trade Practices Act).

100 See, e.g., *Krottner*, 406 Fed. App'x 129, at *1 (9th Cir 2010) (finding '[t]he mere danger of future harm' insufficient to support a Washington common law claim of negligence); *Pisciotta v. Old Nat'l Bancorp*, 499 F.3d

receive mixed treatment.[101] Claims of injury alleging that a plaintiff 'overpaid' or 'wouldn't have shopped' for products or services later associated with a data breach have also had mixed results.[102] Claims that a plaintiff's personal information itself suffered a loss in value as a result of the breach are usually rejected as implausible.[103] Similarly, an alleged loss of ancillary benefits that may have become unavailable because of the breach is usually, though not always, deemed too speculative to survive a motion to dismiss.[104] Finally, as in other contexts, allegations of mere anxiety or emotional harm are usually held to be non-cognisable absent physical injury.[105] Even if complaints in this area thus manage to succeed in otherwise navigating the various theories for framing the causes of action asserted in a particular case, the need also to plead and show injury as an element of the causes of action continues to pose challenges in many actions.

629, 639 and 640 (7th Cir 2007) (same under Indiana law); *Alonso v. Blue Sky Resorts*, LLC, 179 F. Supp. 3d 857, 885 and 886 (SD Ind 2016) (same under Kentucky common law); Moyer, 2014 WL 3511500, at *7 (same under Illinois common law and consumer protection claim).

101 Compare *Pisciotta*, 499 F.3d at 639 (not actionable), *Welborn v. Internal Revenue Serv.*, No. 15–1352, 2016 WL 6495399, at *11 and *12 (DDC 2 Nov 2016) (same), *Dugas v. Starwood Hotels & Resorts Worldwide, Inc.*, No. 16-cv-00014, 2016 WL 6523428, at *11 (SD Cal 3 Nov 2016) (same); *Pruchnicki v. Envision Healthcare Corp.*, 439 F. Supp. 3d 1226, 1233–34 (D Nev 2020) (same), with *Dieffenbach v. Barnes & Noble, Inc.*, 887 F.3d 826, 829 and 830 (7th Cir 2018) (credit monitoring costs and 'significant' lost time held actionable under relevant state laws); *Anderson v. Hannaford Bros. Co.*, 659 F.3d 151, 162 (1st Cir 2011) (mitigation damages held actionable for foreseeable harms for claims under Maine law); *In re: Premera Blue Cross Customer Data Sec. Breach Litig.*, 198 F. Supp. 3d 1183, 1204 and 1205 (D Or 2016) (similar for claims under Washington law); *Corona v. Sony Pictures Entm't, Inc.*, No. 14-cv-09600, 2015 WL 3916744, at *5 (CD Cal 15 Jun 2015) (similar for claims under California law); *In re Marriott Int'l, Inc., Customer Data Sec. Breach Litig.*, 440 F. Supp. 3d 447, 460 (D Md 2020) ('time and money [spent] to mitigate harms' for breach where personal information was at risk of actual or threatened harm was sufficient to establish injury-in-fact).

102 Compare *Moyer*, 2014 WL 3511500, at *7 (insufficient allegation that pricing covered added costs of data security), *Bell v. Blizzard Entm't Inc.*, No. 12-cv-09475, 2013 WL 12132044, at *8 (CD Cal 11 Jul 2013) (alleged loss of resale value unavailing where resale not available), with *In re: Anthem, Inc. Data Breach Litig.*, 162 F. Supp. 3d 953, 986 (ND Cal 2016) (allegation that medical fees covered data security sufficient for 'benefit of the bargain' theory); *Sony II*, at 942, 991, 993, 1007 (allegation sufficient for omissions-based claims under California law, but not Texas or Florida law); *Grigsby v. Valve*, No. C12–0553JLR, 2013 WL 12310666, at *3 (WD Wash 18 Mar 2013) (overpayment allegation sufficient under Washington law); *In re: Target Corp. Data Sec. Breach Litig.*, 66 F. Supp. 3d 1154, 1078 and 1177 (D Minn 2014) ('overpayment' allegation rejected but 'would not have shopped' allegation accepted).

103 *Dugas*, 2016 WL 6523428, at *11 (allegation that value of PII was effective held insufficient under California statute); *Sony II*, at 994 (alleged valuing of PII unavailing under Florida law); *Burrows v. Purchasing Power, LLC*, No. 12-CV-22800, 2012 WL 9391827, at *3 (SD Fla 18 Oct 2012) (same). But see *Claridge v. RockYou, Inc.*, 785 F. Supp. 2d 855, 865 (ND Cal 2011) (allegations of lost value sufficient for common law claim but not statutory claim).

104 See *Anderson*, 659 F.3d at 167 (lost opportunity for rewards points not actionable under Maine law). But see *In re: Arby's Rest. Grp. Inc. Litig.*, No. 1:17-CV-0514-AT, 2018 WL 2128441, at *11 (ND Ga 5 Mar 2018) (alleged loss of ancillary opportunity for earning payment card 'rewards' accepted for purposes of pleading injury).

105 *Sion v. Sunrun*, No. 16-cv-05834, 2017 WL 952953, at *2 (ND Cal 13 Mar 2017) (FCRA); *Belle Chasse Auto. Care, Inc. v. Advanced Auto Parts, Inc.*, No. 081568, 2009 WL 799760, at *4 (ED La 24 Mar 2009) (Louisiana law).

Conclusion

The expanding scope and frequency of data breaches, in combination with the complex and changing legal landscape evidenced by the judicial decisions and statutory developments referenced in this chapter, promise to provide fertile ground for plaintiffs to continue to initiate litigation following such incidents. Companies that are subject to data breaches are accordingly well advised to engage skilled and experienced defence counsel as lawsuits ensue, especially given the significant potential exposure arising from the aggregate liability theories and procedures that plaintiffs typically seek to advance or exploit.

11

FTC Investigations and Multistate AG Investigations

Benjamin A Powell and Kirk Nahra[1]

Introduction

Significant data breaches and privacy mistakes are likely to draw the attention of many regulators, including the Federal Trade Commission (FTC) and the State Attorneys General (State AGs), which view themselves as the consumer protection watchdogs when it comes to privacy and data security issues.

Both the FTC and State AGs are remarkably active in this space. In July 2017, FTC Chairman Joe Simons told Congress, in Commission testimony, that 'privacy and data security top the list of [the FTC's] consumer protection priorities'.[2] The FTC demonstrated this priority by initiating or resolving nearly 30 data security or consumer privacy actions from 2017–2018 alone, and 65 cases since 2002.[3] The FTC is also seeking to expand its authority and recently advocated for Congress to provide it with the authority to issue implementing rules for privacy and data security, and the authority to issue civil penalties.[4]

1 Benjamin A Powell and Kirk Nahra are partners at Wilmer Cutler Pickering Hale and Dorr LLP.

2 'Oversight of the Federal Trade Commission' – Prepared Statement of the Federal Trade Commission [FTC] before the Committee on Energy and Commerce, Subcommittee on Digital Commerce and Consumer Protection and US House of Representatives (18 July 2018), www.ftc.gov/system/files/documents/public_statements/1394526/p180101_ftc_testimony_re_oversight_house_07182018.pdf.

3 Joseph Barloon et al., 'Recent Trends In FTC Consumer Protection', *Law360* (13 Feb 2019), www.law360.com/articles/1128562/recent-trends-in-ftc-consumer-protection-enforcement.

4 Hearing on 'Oversight of the Federal Trade Commission', Subcommittee on Digital Commerce and Consumer Protection, 115th Congress (18 July 2018), https://energycommerce.house.gov/committee-activity/hearings/hearing-on-oversight-of-the-federal-trade-commission-subcommittee-on (past hearings).

State AGs, likewise, have prioritised data security enforcement in recent years.[5] These settlements can involve hundreds of millions of dollars.[6] The National Association of Attorneys General, an organisation of 56 state and territorial attorneys general in the United States, has established an internet safety, cyber privacy and security committee to 'examin[e] issues related to ensuring a safe online environment for children and consumers; issues related to protecting the privacy of users of Internet and mobile applications; and issues related to the security of personal, business and government digital data'.[7]

This chapter seeks to provide an overview of practical considerations when defending a client in an FTC or State AG data security investigation while highlighting key distinctions between the two that may affect counsel's strategy. As a starting point, FTC investigations often can be more procedurally formal by virtue of their voluminous regulations and guidance, and well-developed administrative and federal case law. Conversely, State AG investigations can be more informal in light of their comparatively brief statutory authority and scant case law.

Key differences

Politics

The FTC is an independent agency headed by five commissioners, nominated by the President and confirmed by the Senate, each serving a seven-year term. No more than three commissioners can be of the same political party. The President chooses one commissioner to act as chairman. State attorneys general are elected by popular vote or appointed by the governor.[8] Many State AGs have subsequently been elected to the US Senate, governorships and other higher government offices.

Authority

The FTC relies on its Section 5(a) authority to investigate privacy and data security matters, using its general authority to regulate 'unfair or deceptive' practices. By contrast, all 50 State AGs are empowered to investigate suspected violations of similar, state-level unfair and deceptive practices laws, and also have the ability to enforce under state data breach notification statutes. These statutes allow the AGs to investigate and enforce against companies that are found not to have notified affected individuals or the proper authorities of a breach within the required statutory period.

---

5 See, e.g., Divonne Smoyer et al., 'Beware the Growth of State AG Enforcement Efforts', Corporate Counsel (22 May 2015), www.corpcounsel.com/id=1202727264255/Beware-the-Growth-of-State-AG-EnforcementEfforts.

6 Aisha Al-Muslim, 'Uber to Pay $148 Million Penalty to Settle 2016 Data Breach', *The Wall Street Journal* (26 Sep 2018), www.wsj.com/articles/uber-to-pay-148-million-penalty-to-settle-2016-data-breach-1537983127; '50 State Attorneys General Secure $600 Million from Equifax in Largest Data Breach Settlement in History', (22 July 2019), available at https://www.doj.state.or.us/media-home/news-media-releases/50-state-attorneys-general-secure-600-million-from-equifax-in-largest-data-breach-settlement-in-history/.

7 Hedda Litwin, Internet Safety/Cyber Privacy and Security Committee: Mission Statement, National Association of Attorneys General, https://www.naag.org/naag/committees/naag-special-committees/internet-safetycyber-privacy-and-security-committee.php (last visited 13 March 2019).

8 Except Maine, wherein the State AG is elected by a secret ballot of the legislature and in Tennessee by the state supreme court.

External counsel

The FTC does not work with private external counsel to investigate or bring consumer protection cases.[9] State AGs may retain law firms to represent their states in consumer protection matters, including data security cases.[10]

Confidentiality

FTC investigations are confidential and the information and materials produced to the FTC during the course of an investigation are generally protected from disclosure under the Freedom of Information Act, with limited exceptions; by contrast, State AGs' offices frequently publicly announce the initiation of an investigation, and protections from third-party disclosure vary greatly by state statute.[11] Typically, FTC closures of investigation without enforcement activity are not public.

Civil penalties

Most state statutes allow State AGs to immediately seek civil penalties of US$5,000 per violation. The FTC can only impose civil penalties if a company has violated a consent order or a trade regulation rule promulgated by the Commission.

Introduction to the Federal Trade Commission

Authority

The FTC enforces the Federal Trade Commission Act, Section 5(a) of which prohibits 'unfair or deceptive acts or practices in or affecting commerce'.[12] This language serves as the basis for the FTC's jurisdiction over consumer protection matters, including those relating to consumer privacy and data security. Since 2002, the FTC has brought more than 65 enforcement actions against companies who have experienced data breaches with unfair or deceptive trade practices on the theory that the breaches were the result of the companies' failure to adopt reasonable security measures.[13]

This authority has been affirmed by federal courts, perhaps most notably in *FTC v. Wyndham Worldwide Corp*, in which the Third Circuit held that certain data security practices could be considered 'unfair' under Section 45(a), and that the relevant provision, in this instance, provided Wyndham fair notice that its practices opened it up to liability under the Act.[14]

9 An executive order even bars federal agencies, including the FTC, from hiring outside lawyers on a contingency-fee basis. See Exec. Order No. 13,433, Protecting American Taxpayers from Payment of Contingency Fees, 72 Fed. Reg. 28441 (16 May 2007).

10 See Eric Lipton, 'Lawyers Create Big Paydays by Coaxing Attorneys General to Sue', *The New York Times* (18 Dec 2014), www.nytimes.com/2014/12/19/us/politics/lawyers-create-big-paydays-by-coaxing-attorneys-general-to-sue-.html.

11 See, e.g., Fla. Stat. 119.071 to .0714 compared to Tex. Govt Code Ann. 552.101 to 158.

12 15 USC Sections 41 to 58.

13 FTC, Privacy and Data Security Update (2019), https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2019/2019-privacy-data-security-report-508.pdf.

14 *FTC v. Wyndham Worldwide Corp*., 799 F.3d 236 (3d Cir 2015).

Initiation of an investigation

The FTC has broad statutory authority to 'gather and compile information concerning, and to investigate from time to time the organization, business, conduct, practices, and management of any person, partnership, or corporation engaged in or whose business affects commerce'.[15] Although FTC staff do not typically disclose the catalyst of an investigation, investigations may be initiated in response to consumer or industry complaints, blog posts by advocates or security researchers, other government agency requests, court referrals or independent investigations by the Commission. FTC investigations are also typically confidential[16] but there are several exemptions to this rule, including disclosure to a Congressional committee or to other law enforcement agencies.[17]

The FTC typically initiates an investigation by serving a hold letter, with an access letter (otherwise known as a 'demand for information'), or a civil investigative demand (CID) on the target.[18] A hold letter typically only requires the recipient to preserve certain documents or information (see following paragraph for a discussion of document holds). Access letters are informal requests for information or testimony (oral or written).[19] Similar to an access letter, a CID requests information or testimony (oral or written); however, the Director of the FTC's Bureau of Consumer Protection and one Commissioner's office must approve the issuance of the CID. In the event a target does not comply with a CID, the FTC may seek enforcement in court through the Department of Justice under Section 16 of the FTC Act.[20]

Another tool in the FTC's investigative belt is Section 6 of the FTC Act, which permits the Commission to require the filing of 'annual or special reports or answers in writing to specific questions' for the purpose of obtaining information about 'the organization, business, conduct, practices, management, and relation to other corporations, partnerships, and individuals' of the entities to whom the inquiry is addressed.[21] These reports do not necessarily have a law enforcement purpose.

Upon receipt of a letter or CID from the FTC, a target should first put in place a document hold to preserve any relevant documents and information. The letter or CID may reflect specific topics or documents of concern; however, the target should consider whether to broaden the hold to cover any documents or custodians with potentially relevant documents. For many clients, a document hold involves both (1) notifying and requesting acknowledgement from custodians of the hold and (2) placing a technical hold on the back end of any systems that may roll over, including email and other data storage.

15 FTC, 'A Brief Overview of the Federal Trade Commission's Investigative and Law Enforcement Authority' (July 2008), https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority.

16 15 USC Section 57b-2.

17 See, e.g., 16 CFR Section 4.11.

18 Subpoenas are not available in consumer protection matters. 15 USC Section 57b-1.

19 FTC, Operating Manual, Chapter 3, Section 3.6.6.1 at 20, https://www.ftc.gov/sites/default/files/attachments/ftc-administrative-staff-manuals/ch03investigations_0.pdf.

20 15 USC Section 57(b)1(e).

21 FTC Act, Section 46 (Sec. 6) para. (b). As with subpoenas and CIDs, the recipient of a 6(b) order may file a petition to limit or quash, and the Commission may seek a court order requiring compliance.

Meet-and-confer

After reviewing the letter or CID (or both), counsel should reach out to the FTC staff handling the case to acknowledge receipt and schedule a meeting to discuss a response timeline. Although it is prudent to reach out early in the investigation to staff in any event, if a target receives a CID, the company is required to schedule a meet-and-confer within 14 days of receipt.[22]

To prepare for the meeting, it is important to understand the basic facts of the case and identify the employees with relevant knowledge or involvement and key documents. In addition, counsel will need to understand the scope of the letter or CID requests and the burden on the client in responding to these requests. Some documents and information may be easy to provide quickly to the FTC, while other information sought may not be kept in the normal course of business and require vast amounts of time and resources to compile. For other requests, the volume of documents alone may be nearly impossible to produce by the return date stated in the letter or CID.

Negotiating the timing and scope of the productions is the main objective at the meet-and-confer, but it also provides an opportunity to converse with the FTC staff about the focus of the investigation. This focus will guide the discussion and help the parties to identify priorities and agree on a reasonable production schedule. The FTC staff may agree to modify the timeline and scope of the production; however, it is typically without prejudice to come back and request full compliance, especially in the case of a CID.

Timing

Letters and CIDs typically include a deadline that is impossible to meet. Often, the FTC staff will agree to a rolling production of materials if the target can provide cogent explanations as to why the deadline included in the letter is not realistic, and further provide that the target make an initial production by the return date on the CID or access letter. Here, it can be helpful to understand which requests are of greatest priority to the FTC staff and schedule accordingly.

Scope

Often, the FTC will seek 'any and all' documents or 'any and all' information relating to a specific topic. Consider alternative proposals such as (1) providing documents 'sufficient to show', (2) limiting the number of custodians, (3) limiting the document by agreed search terms, (4) providing a narrative response in lieu of documents and (5) limiting the response time limit. Providing a convincing argument why the FTC staff should accept your proposal is critical, considering arguments such as 'this custodian is most likely to have the documents of interest' or 'this few month period is the most relevant one' or 'we will simply drown in the millions of documents responsive to these requests over the multi-year period it will take for [the company] to produce them'. While the burden to your client in producing the materials can be considered, the FTC staff are more likely to be amenable to proposals designed to provide the most relevant materials as quickly as possible, without prejudice to seek more later.

22 16 CFR Section 2.7(k).

The FTC staff will typically record the production schedule in writing after the meeting. This mitigates the likelihood of a misunderstanding regarding timelines and makes the company accountable. If an agreement regarding the timing or scope of a subpoena cannot be reached, the target can move to quash the CID. The target must file the motion to quash with the Commission before the sooner of 20 days after service of the CID or the return date of the CID.[23]

Understanding the investigation

Once the recipient understands the focus of the investigation, it is advisable to conduct a privileged, internal investigation led by counsel to understand the conduct of potential interest. This will assist in understanding potential liability, developing defensive and advocacy strategy, and, if warranted, take advance corrective action if an issue is identified. See Chapter 3 for additional considerations in an internal investigation.

Document production

Once a production schedule is agreed, document collection can begin. Depending on the scope of the production, it may require conducting collection interviews, during which the custodians discuss with counsel leading e-discovery each of the places the individual may have stored responsive documents, including those stored locally, in the cloud, on shared drives, and certain requests may even extend to chats or other client-specific means of communication (e.g., Slack).

Counsel should review all documents before production to the FTC staff. In addition to confirming responsiveness and screening for privilege, this review can help inform the company's internal investigation and gain insight into potential theories of liability the FTC staff may develop. If a client is concerned about cost, consider developing ways to review a sampling of the documents, or craft search terms for documents that are most likely to give rise to liability for the client.

Many clients are very concerned about keeping their documents confidential. This is particularly true in a data security context if requested materials may reflect sensitive security documents such as incident response plans, threat assessments or network diagrams. The FTC Act prohibits disclosure of confidential information, testimony and materials submitted pursuant to a CID, and materials otherwise marked confidential.[24] It is required to label sensitive documents and information as confidential, and you should request these documents and information be returned or destroyed by the FTC at the conclusion of the investigation.

Counsel should only agree to production deadlines that are realistic, but of course, unanticipated issues arise to delay production. Reaching out to the FTC staff as soon as reasonably practicable about a potential delay (preferably not the day the production is due), with a clear explanation and a new deadline, can help maintain goodwill and credibility with FTC staff.

23 16 CFR Section 2.10.

24 15 USC 46(f); 15 USC 57b-2(b); 15 USC 57b-2(c).

Written and oral testimony

FTC staff may request written responses to interrogatories or accept a written response in lieu of document production. Written responses should seek first to answer the question posed but should also be viewed as an opportunity for affirmative advocacy. You can include information designed to allay staff concerns, providing an overview of added protections or industry comparisons.

Consider whether to include materials supporting the authority of the written statements. If relying on employee statements, provide information about why that employee knows the most about the topics and should be trusted. If speaking to general practices, consider the submission of ordinary course of business documents that support the proposition. In some cases, documents alone may be more persuasive than a written submission, and the rules of practice dictate that you may submit documents in lieu of a written response if the documents meet the substance of the interrogatory specifications.[25]

The FTC may also take oral testimony during investigative hearings. However, this is an infrequent practice, most often seen in fraud and national advertising cases.[26]

Advocacy

Advocacy is intentionally included after document production and written and oral testimony in this chapter. Each interaction with the FTC staff is an opportunity for advocacy to explain and contextualise issues; however, FTC staff may be unwilling to fully engage with white papers and presentations (or other materials that are solely advocacy-focused) until they have received responses to their questions and at a least a large portion of the requested documents. Launching into advocacy before the FTC staff feel that they understand the facts is likely to undercut its efficacy, and perhaps even annoy them.

In addition to conversations with FTC staff, looking to recent FTC enforcement actions and staff speeches may help to identify the focus of the investigation and place it in the context of the FTC's enforcement priorities. Understanding these priorities should inform negotiation and advocacy tactics.

The form of the advocacy will depend on the facts of the matter and the preferences of the FTC staff. While a long-form white paper with witness declarations and expert reports can provide greater detail on a subject, a presentation with visuals may have greater impact.

Resolution

At the conclusion of an investigation, and based on the recommendation of the FTC staff, the Commission may vote to (1) close the investigation, (2) seek a consent order, (3) file a complaint in administrative court or (4) authorise the FTC staff to file a complaint and litigate in federal court. Before an enforcement recommendation is presented to the Commission, the FTC staff typically present the company with a draft complaint or consent decree, providing the company an opportunity to advocate to the FTC staff and, if needed, escalate

25 16 CFR Section 3.35.

26 FTC, Operating Manual (see footnote 20), Section 3.6.7.6 at 32-36. These hearings are similar to depositions, except counsel is not allowed to object to lines of questioning. However, time-outs with the witness are permitted.

to the Director of the Bureau of Consumer Protection, and demonstrate that enforcement is unwarranted or to negotiate more favourable terms of the proposed consent decree.

Voluntary closure

The Commission may close the case if it finds there was no violation of law, an enforcement action would not further the public interest, or it would be likely to lose if the matter proceeded to litigation. If the investigation was initiated with an access letter, no formal vote is required to close. Instead, discretion to close is left to the FTC staff. The FTC may also recommend the company take certain corrective action in connection with the closure, but without a formal consent decree (and thus, formal enforcement mechanism).

A company may request a formal closing letter but beware that such a letter goes on the public record.[27] If your client wishes the investigation to remain confidential, you can also request that the FTC staff forgo issuing a closing letter.

Consent agreements

A consent agreement may be negotiated between the FTC staff and the company to conclude the investigation. These agreements provide relief similar to a cease-and-desist order, and include a proposed complaint and decision and order. An admission of liability is not required. Agreements typically impose an injunction prohibiting the practices alleged in the draft complaint, a privacy- or security-by-design programme, biannual audits by a qualified independent third party for 20 years, a compliance report, and standard record-keeping and reporting requirements. These agreements may also include 'fencing in' provisions, designed to prevent the company from engaging in similar misconduct.

Once drafted, a proposed agreement is reviewed by the Commission and, if accepted, the proposed order, complaint and consent agreement are put on the public record for a 30-day comment period.[28] Following the comment period, the Commission may issue the complaint and order, withdraw its acceptance of the agreement or modify the order. Orders are considered final 60 days after issuance.[29]

Consent agreements can help clients avoid the cost and potential embarrassment associated with a protracted litigation. Depending on the conduct at issue and the goodwill and credibility built up with the FTC staff, you may be able to help craft the complaint. You may also negotiate the language of the agreement although much of the privacy and data security agreements are standardised. Fruitful considerations for negotiating a consent include (1) the scope of the injunction, (2) definitions, (3) the frequency and scope of the reporting requirements, (4) the duration of the record-keeping requirements and (5) the entities covered.

27 16 CFR Section 14.9(b)(4)(ii).

28 16 CFR Section 2.34(c). This is also true for consent agreements resolving cases filed in administrative court. However, it does not apply to order files in federal court under Section 13(b).

29 FTC, 'A Brief Overview of the Federal Trade Commission's Investigative and Law Enforcement Authority' (July 2008), www.ftc.gov/about-ftc/what-we-do/enforcement-authority.

Administration hearing (Part 3 adjudication)

If, by a majority vote, the Commission determines that it has reason to believe that the law has been violated and that a proceeding would be in the public interest, it may issue a complaint to be litigated by FTC staff before an administrative law judge (ALJ), according to the FTC's Rules of Practice for Adjudicative Proceedings.[30] At the conclusion of the hearing, the ALJ will issue an initial decision with findings of facts and conclusion of law and will recommend either an entry of a cease-and-desist order or dismissal of the complaint. Cease-and-desist orders are substantively similar to consent agreements, and typically include the same types of provisions, including a 20-year sunset period. Civil penalties are not available in first instance administrative proceedings.[31]

The ALJ's decision, if appealed, is reviewed de novo by the Commission.[32] The Respondent may appeal the Commission's final order to a federal circuit court, which will review the Commission's legal conclusions de novo.[33] Critics of the Part 3 adjudication proceedings argue that because the FTC effectively serves as investigator, prosecutor and arbitrator, the proceedings are inherently unfair.[34]

Federal court (Section 13(b))

The FTC may also file a complaint and seek an order in federal court.[35] Pursuant to Section 13(b), the FTC may seek preliminary and permanent injunctions and other equitable relief if a violation of the FTC Act is ongoing or likely to occur.[36] According to the FTC, most consumer protection enforcement is now conducted directly in court under Section 13(b) rather than by means of administrative adjudication because 'in such a suit, the court may award both prohibitory and monetary equitable relief in one step'.[37] Although the resulting

30 16 CFR Sections 3.1 to 3.83.

31 15 USC Section 45(1) authorises penalties for violations of an administrative order, such a consent decree or cease-and-desist order.

32 16 CFR Section 3.52.

33 Courts review the FTC's legal decisions de novo but give 'some deference to [its] informed judgment that a particular commercial practice is to be condemned as "unfair"'. *FTC v. Ind. Fed'n of Dentists*, 476 U.S. 447, 454, 106 S Ct 2009, 2016 (1986).

34 Maureen K Ohlhausen, Administrative Litigation at the FTC: Effective Tool for Developing the Law or Rubber Stamp, Journal of Competition Law & Economics, 1-37 (2016), https://www.ftc.gov/system/files/documents/public_statements/1005443/ohlhausen_administrative_litigation_at_the_ftc_effective_tool_for_developing_the_law_or_rubber.pdf ('Nevertheless, the FTC's administrative litigation process, examined in Part III.A, stands accused of being a rigged system. In a Part 3 proceeding, the FTC serves prosecutorial and adjudicative roles.').

35 FTC, Brief Overview (see footnote 16). (Section 16 of the FTC Act, 15 USC Section 56, authorises the Commission to represent itself by its own attorneys in five categories of cases: (1) suits for injunctive relief under Section 13 of the FTC Act, 15 USC Section 53; (2) suits for consumer redress under Section 19 of the FTC Act, 15 USC Section 57b; (3) petitions for judicial review of FTC rules or orders or a cease-and-desist order issued under Section 5 of the FTC Act, 15 USC Section 45; (4) suits to enforce compulsory process under Sections 6 and 9 of the FTC Act, 15 USC Sections 46, 49.3; and (5) suits to prohibit recipients of compulsory process from disclosing the existence of the process in certain situations, Section 21a of the FTC Act, 15 USC Section 57b-2a.)

36 *U.S. Oil & Gas Corp.*, 748 F.2d 1431, 1434 (11th Cir 1984) (quoting *H. N. Singer, Inc.,* 668 F.2d 1107, 1113 (9th Cir 1982)).

37 FTC, Brief Overview (see footnote 16); see also *FTC v. World Travel Vacation Brokers, Inc.*, 861 F.2d 1020, 1024-28 (7th Cir 1988); *U.S. Oil & Gas*, 748 F.2d at 1432-35 (per curiam); H. N. Singer, 668 F.2d at 1110-13.

orders from such litigation may be substantively similar to an administrative cease-and-desist order, they do not typically include the 20-year sunset provision.

Recent developments

The FTC's authority to impose requirements in an order is not without limits. The US Court of Appeals for the Eleventh Circuit vacated a cease-and-desist order by the FTC issued against LabMD, Inc arising from an FTC enforcement action alleging that LabMD's data security programme was unreasonable and therefore constituted an unfair act or practice under Section 5 of the FTC Act.[38] The court found that it 'mandates a complete overhaul of LabMD's data-security program and says precious little about how this is to be accomplished' and in turn held that 'the prohibitions contained in cease and desist orders . . . must be specific'.[39] Counsel should cite to this ruling when negotiating a settlement or order that is overly broad and not specific to the conduct at issue.

In April 2021, the US Supreme Court held that Section 13(b) of the FTC Act does not authorise the Commission to pursue equitable monetary relief.[40] The Court held, based on the Act's language and structure, that Section 13(b) authorises the FTC to seek injunctions but makes no mention of monetary relief. The Court emphasised that other FTC Act sections – notably Sections 5(l) and 19 – do authorise the FTC to pursue monetary remedies, subject to identified limitations.

State AG investigations

Authority

State attorneys are given authority to investigate businesses or individuals suspected of engaging in unfair, deceptive or abusive practices (UDAP). These provisions are sometimes referred to as 'little FTC Acts'[41] and the dearth of regulations and case law provides substantial power to the State AGs on how they are to be interpreted.[42] In the data security context, AGs bring UDAP claims on a similar theory to the FTC; namely that by suffering a breach, a company has failed to keep its promises to consumers to keep their data safe, which is

38 *LabMD, Inc. v. FTC*, No. 16-16270 (11th Cir 2018); see also Kim Phan et al., 'Eleventh Circuit Concludes FTC Data Security Order Unenforceable Because Standards Not Specific Enough', WilmerHale (12 June 2018), www.wilmerhale.com/en/insights/client-alerts/20180612-eleventh-circuit-concludes-ftc-data-security-order-unenforceable-because-standards-not-specific-enough.

39 *LabMD, Inc. v. FTC*, No. 16-16270 (11th Cir 2018).

40 *AMG Cap. Mgmt., LLC v. FTC*, 593 U.S.__, No. 19-508 slip op. at 1 (2021).

41 Jack E Karns, 'State Regulation of Deceptive Trade Practices Under "Little FTC Acts": Should Federal Standards Control?', 94 Dick. L. Rev. 373, 374 (1989–1990).

42 See, for example, Cal. Bus. & Prof. Code Section 17500, which makes it unlawful 'for any person, . . . corporation . . . or any employee thereof with intent directly or indirectly to dispose of real or personal property or to perform services . . . or to induce the public to enter into any obligation relating thereto, to make or disseminate . . . before the public in this state, . . . in any newspaper or other publication . . . or in any other manner or means whatever . . . any statement, concerning that real or personal property or those services . . . which is untrue or misleading, and which is known, or which by the exercise of reasonable care should be known, to be untrue or misleading'; see also Massachusetts Section 2 of Chapter 93A, which declares unlawful any '[u]nfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce'; N.Y. Gen. Bus. Law, Sections 349, 350.

an unfair and deceptive practice. In addition to this UDAP authority, 50 states have laws requiring entities to notify individuals of breaches involving personally identifiable information; 23 of these states require entities to notify the attorney general of a breach. AGs can investigate and bring a claim against companies for failing to notify under these state statutes.

Initiation of an investigation

State AGs, as chief legal officers, are empowered, among other things, to investigate and enforce the consumer protection laws of their respective state.[43] As such, their investigatory powers are broad and they are generally authorised to demand production of information and materials that are 'reasonably related' to their investigation.[44] State AG investigations can be triggered by media coverage, consumer complaints, whistle-blowers or even a perceived risk to consumers. In the data security context, an AG's office may see media coverage of an incident or, if the state requires AG notification in the event of a breach, receive a letter from a company notifying them of an incident.

A State AG may initiate an investigation by sending a litigation hold, an informal letter, a CID or a subpoena for information and documents. Immediately upon notice of receipt, the company should place a hold on relevant custodial documents. See 'FTC: Initiation of an Investigation' (above) for considerations in drafting and executing a document hold.

Confidentiality protections are weaker in State AG investigations than FTC investigations. As mentioned above, an AG's office may announce publicly it is investigating a company or incident.[45] Additionally, materials produced to a State AG's office may not be protected from disclosure. State open records laws, also known as 'sunshine laws', vary greatly, and it is important to determine whether there are any applicable exemptions shielding documents from disclosure, including for investigatory materials provided in response to a subpoena.[46] Some states, however, will only exempt trade secret or other confidential business material from public disclosure.[47]

Counsel should discuss with the AG's office staff handling the matter whether they would consider entering into a confidentiality agreement before the company produces any documents. This agreement should include provision for the circumstances under which documents may be shared with other government entities or AG offices, notice in the event that the AG receives an open records request, and how to handle the documents at the conclusion of the investigation. Some offices will decline to enter into an agreement, citing sufficient protection from the state statutes, while others may decline simply as a matter of practice.

43 See, e.g., N.Y. Gen. Bus. Law, Sections 349, 350.

44 See, e.g., *Fielder v. Berkeley Props. Co.,* 23 Cal. App. 3d 30, 38 to 39, 99 Cal. Rptr. 791, 796-97 (Ct App 1972) ('Insofar as the prohibition against unreasonable searches and seizures can be said to apply at all it requires only that the inquiry be one which the agency demanding production is authorized to make, that the demand be not too indefinite, and that the information sought be reasonably relevant.').

45 See, e.g, Dan M Clark, NY AG Announces Probe of Marriott Data Breach and Its Failure to Report Incident, *New York Law Journal* (30 Nov 2018), https://www.law.com/newyorklawjournal/2018/11/30/ny-ag-announces-probe-of -marriott-data-breach-and-its-failure-to-report-incident/; Reuters, 'US attorneys general investigating Google data breach', *New York Post* (9 Oct 2018), https://nypost.com/2018/10/09/us-attorneys-general-investigating-google-data-breach/.

46 See, e.g., Mass. Gen. Laws ch. 93A, Section 6.

47 See, e.g., Fla. Stat. Section 815.045.

Note that no matter what confidentiality protection has been negotiated in the agreement, case law may prohibit the offices from entering into confidentiality agreements that would override or supersede these open record statutes.[48]

Multistate investigations

AGs can also leverage resources by working together and forming multistate investigations, with an executive committee typically consisting of two to eight states taking the investigatory lead. Multistate investigations are most common in large-scale data breaches that affect large numbers of consumers in multiple states.[49] However, some AG offices have expressed their dissatisfaction with the multistate model, pointing to delays in investigations or settlements resulting from coordination issues.

If possible, negotiate so that the company is producing materials only to the executive committee to decrease the risk of a document leak or successful open records request. Relatedly, confidentiality agreements are particularly important in multistate investigations where the state laws will vary widely. AGs are typically more willing to enter into confidentiality agreements in the multistate context, and some AG offices will agree to apply the confidentiality obligations of the state from which they are receiving the documents if their own state laws provide less protection.

Initial response and document production

There is no requirement to meet-and-confer with AG staff within a set number of days. However, CIDs and subpoenas typically include a response date (generally, 30 or 45 days) by which a company should make at least an initial, good faith production. To produce all the required documents to the AG within the time limit, it is advisable to reach out to the AG's office to negotiate scope a few weeks before the deadline. (See 'FTC: Meet-and-confer' for

48 See, e.g., *Nat'l Collegiate Athletic Ass'n v. Associated Press*, 18 So. 3d 1201, 1207 (Fla Dist Ct App 2009), review denied, 37 So. 3d 848 (Fla 2010), in which the court held that a confidentiality agreement entered into by a private law firm on behalf of a state university with the National Collegiate Athletic Association [NCAA] that allowed access to records contained on the NCAA's secure custodial website that were used by the university in preparing a response to possible NCAA sanctions, had no effect on whether these were public records, stating that '[a] public record cannot be transformed into a private record merely because an agent of the government has promised that it will be kept private'. See also *City of Pinellas Park v. Times Publ'g Co.*, No. 00-008234CI-19 (Fla 6th Cir Ct 3 Jan 2001) ('there is absolutely no doubt that promises of confidentiality [given to employees who were asked to respond to a survey] do not empower the Court to depart from the public records law').

49 Press release, Office of AG Maura Healey, AG Healey Leads Multistate Coalition in Reaching $148 Million Settlement With Uber Over Nationwide Data Breach, Mass.gov (26 Sep 2018), https://www.mass.gov/news/ag-healey-leads-multistate-coalition-in-reaching-148-million-settlement-with-uber-over; see also B Colby Hamilton, 'Nationwide reaches $5.5M data breach settlement with 33AGs', *Property Casualty 360°* (11 Aug 2017), www.propertycasualty360.com/2017/08/11/nationwide-reaches-5-5m-data-breach-settlement-wit/?slreturn=20190212205913; News release, Office of AG Ken Paxton, 'AG Patton Announces $1.5 Million Settlement with Neiman Marcus over Data Breach' (8 Jan 2019), www.texasattorneygeneral.gov/news/releases/ag-paxton-announces-15-million-settlement-neiman-marcus-over-data-breach; Press release, Office of AG Letitia James, 'A.G. Schneiderman Announces $18.5 Million Multi-State Settlement With Target Corporation Over 2013 Data Breach' (23 May 2017), https://ag.ny.gov/press-release/ag-schneiderman-announces-185-million-multi-state-settlement-target-corporation-over.

tips on negotiating the scope of a letter, CID or subpoena.) AG offices may be more willingly than FTC staff to have a flexible, rolling production schedule.

Document requests will frequently seek 'any and all documents' concerning a certain topic, but the office may agree to reduce the requirements based on reasonable search terms and custodians most likely to have the relevant documents. The AG office may not request the search terms and custodian list itself; however, any cover letters accompanying the production should make clear you are providing relevant documents identified by running search terms over certain custodial documents.

As with FTC productions, counsel should ensure all potentially relevant documents are collected, review the documents before they are submitted to the AG, label confidential documents as such, and meet any agreed production deadlines.

If an agreement on a production schedule cannot be reached with the office, counsel should review local practice and civil procedure to determine whether it would be appropriate to file a motion to quash the subpoena. Most state civil procedure requires AG offices to file a motion to compel before a motion to quash may be filed, but it is important not to miss the window.[50]

Strategy and advocacy

As in FTC investigations, each interaction with the AG's office is an opportunity to advocate for your client. Assess whether a white paper or presentation (or both, perhaps) most effectively lays out your clients' defences. Generally, it is advisable to find time to have a meeting with the AG's office to discuss any potential concerns in the case after the bulk of information or documents have been produced and a written advocacy piece has been submitted. Hearing from the AG's office directly what is of most concern provides counsel with an opportunity to provide immediate feedback.

In multistate investigations, it can be difficult because of scheduling conflicts and budget constraints to meet all the states, or even just the executive committee, in person. However, these in-person discussions with the AGs are invaluable and offer counsel an opportunity to efficiently address any concerns and make sure the different offices are on the same page.

Resolution

State AG data security investigations are typically voluntarily closed or resolved with a settlement (although State AGs often do not indicate as a formal matter that an investigation is closed – the target just may not hear from them again). The AG's office may close the investigation if it finds there is no violation of law or the company has voluntarily made modifications to its data security programme to rectify any perceived failures or deficiencies.

The majority of State AG settlements are formal legal documents, filed in state court and typically styled as an assurance of discontinuance, an assurance of voluntary compliance or a stipulated judgment.[51] Stipulated judgments typically differ from assurances of discontinuance and assurances of voluntary compliance only in that they typically include findings of fact and violation of law. In multistate AG investigations, the document may also be styled as

50 See, e.g., Cal. Gov't Code, Sections 11187, 11188.

51 See, e.g., VCPA, Section 59.1-202; D.C. Code, Section 28-4512; RCW 19.16.480.

a 'consent decree', which is then filed in various state courts as a stipulated judgment. These settlements are not considered an admission of guilt (and many such agreements have 'neither admit nor deny' provisions) but, if violated, the agreements have the same force of law as an injunction, judgment or final court order.

State AG settlements typically reflect similar provisions as FTC settlements, including prohibiting the company from making misrepresentations regarding the extent to which the company protects the privacy, confidentiality, security or integrity of personal information, and requiring the company to cease any violative conduct, implement privacy and security programmes and perform regular independent assessments of the company's data practices, to be reported to the AGs at regular intervals. Notably, these settlements typically include fines ranging from US$20,000 to much higher numbers as in the *Uber* and *Equifax* matters.

State AG data security cases rarely proceed to litigation. To bring a UDAP claim, many State AGs do not have to show that the unfair or deceptive conduct resulted in actual harm or injury to receive injunctive relief and do not have to demonstrate monetary harm to consumers to receive civil penalties.[52] These statutes typically authorise the AGs to bring damages up to US$5,000 per violation – and how 'violation' is determined is open to interpretation.[53] Moreover, State AG cases generally cannot be consolidated, relegating a company to responding to suits in several state courts at once. The relatively low bar for bringing a successful claim coupled with the potentially high civil penalties available make many clients reluctant to litigate, even if they believe they have a good case.

Practice points

Rising cost of compliance

Compliance with a request from the FTC or an AG can be extremely expensive for a client, even if the matter results in a voluntary closure. The advent of e-discovery makes it easy for the FTC or AG staff to ingest hundreds of thousands of documents and search for those of greatest interest using key words, instead of paging through hard copies. Conversely, it is expensive for a client to dedicate the resources necessary to identifying the right documents, collecting the documents and having counsel review the documents prior to production.

52 See, e.g., D.C. Code Ann., Section 28-3904 (West 2015) (stating that a person violates the law 'whether or not any consumer is in fact misled, deceived or damaged thereby'); Md. Code Ann., Com. Law Sections 13-301(1), 13-302 (West 2013) (providing that the capacity or tendency to deceive establishes a violation 'whether or not any consumer in fact has been misled, deceived, or damaged as a result of that practice'); *People ex rel. Lockyer v. Fremont Life Ins. Co.,* 128 Cal. Rptr. 2d 463, 470 to 471 (Cal Ct App 2002) (finding the test is 'whether the public is likely to be deceived . . . even if no one was actually deceived, relied upon the fraudulent practice, or sustained any damage') (citing *State Farm Fire & Cas. Co. v. Super. Ct.*, 53 Cal. Rptr. 2d 229, 235 (Cal Ct App 1996)); *State ex rel. McLeod v. Brown*, 294 S.E.2d 781, 783 (SC 1982) (finding a tendency to deceive and mislead without proof of actual deception is sufficient to establish liability); *Goshen v. Mutual Life Ins. Co. of N.Y.*, 98 N.Y.2d 314, 324 (NY 2002) ('Unlike private plaintiffs, the Attorney General may, for example, seek injunctive relief without a showing of injury . . . On its face, General Business Law § 349(a) declares deceptive conduct unlawful without reference to whether it has actually caused specific pecuniary harm to consumers in general . . . [T]he deception itself is the harm that the statute seeks to remedy[.]'); *Rule v. Fort Dodge Animal Health, Inc.*, 607 F.3d 250, 255 (1st Cir 2010) (noting that Mass. Gen. Laws ch. 93A, Section 2(a) claim brought by consumer requires injury, although ch. 93A claim brought by the Commonwealth does not).

53 Mass. Gen. Laws, ch. 93A, Section 4; N.Y. Gen. Bus. Law, Section 350-d.

Accordingly, the strategy for defending an investigation has become increasingly focused in recent years on alleviating the burden on the client.

Importance of compliance planning

Because of these high costs, companies should pay careful attention to their compliance programmes and decision-making related to privacy and data security. Effective legal advice (and advice from privacy and compliance officers) often will raise issues of concern before business decisions are made, to avoid situations that likely are of interest to these enforcement officials.

Beware collateral consequences

In determining whether to proceed to litigation if parties are unable to come to an agreement, the client should be aware of potential collateral consequences, including bad press coverage and private litigants. Class action follow-on lawsuits are becoming increasingly common in the data security context.

Importance of building rapport, credibility and goodwill

Keeping in mind the staff's constrained time and resources, it is generally advisable to over-communicate with them at the outset of an investigation to build rapport and underscore that the company is taking the investigation seriously. Responding quickly to concerns raised by staff, including taking efforts or steps to correct potentially problematic processes or behaviour, can further build credibility. A good relationship with the staff can go a long way towards reaching a favourable outcome for your client.

12

Cyber Trends and Investigations in Europe: A Practitioner's Perspective

Rohan Massey, Kevin Angle, Edward Machin and Raffi Teperdjian[1]

Cyber requirements under EU law and laws in the UK

Many organisations in the European Union and the United Kingdom, and those in the rest of the world that offer products or services to individuals in the EU or UK, associate cybersecurity with four letters: GDPR. However, the General Data Protection Regulation and its counterpart in the UK, the UK GDPR,[2] are only one thread in a patchwork of cybersecurity laws and best practices in the EU and UK that, when viewed together, comprise some of the most comprehensive security requirements faced by businesses in any region of the world. The challenge of complying with these laws is compounded by their extraterritorial effect. For example, a company with a single office in California offering holiday packages to individuals in the EU or UK may be subject to the GDPR.[3] Accordingly, the extent to which digital business is now borderless means that the influence and scope of cybersecurity laws in the EU and UK is no longer a strictly regional concern.

The development of the EU's and UK's cybersecurity framework has coincided with a wider appreciation of, and anxiety about, the value – monetary and otherwise – of personal information. Of particular alarm to individuals is the regularity with which data

1 Rohan Massey is a partner, Kevin Angle is a counsel, Edward Machin is an associate and Raffi Teperdjian is an associate at Ropes & Gray LLP. The authors would like to recognise the work of Rosemarie Paul who was a key contributor to the previous edition of this chapter.

2 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC – the General Data Protection Regulation [GDPR]. With respect to the UK, 'UK GDPR' refers to the definition in the Data Protection Act 2018, as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019). For ease of reading, the GDPR and the UK GDPR will be referred to in this Chapter as the 'GDPR'.

3 The GDPR significantly extends the scope of the previous regime – Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data – which applied only to controllers and processors with an EU presence.

is compromised. These concerns are not unwarranted: in January 2021, it was reported that nearly 281,000 personal data breaches had been notified since the introduction of the GDPR on 25 May 2018.[4] Even though cybersecurity is now firmly a board-level issue,[5] many businesses still have insufficient procedures in place to address the loss or disruption caused by cyberthreats. This chapter discusses how important it is that businesses address these gaps, as a matter of priority.

General Data Protection Regulation

The concept of personal data security in the EU and UK does not begin with the GDPR. Indeed, in requiring that data controllers and processors implement 'appropriate technical and organisational measures' to ensure a level of security appropriate to the risks of their data processing, the GDPR[6] closely tracks the language of the previous legislation (Directive 95/46/EC, the Data Protection Directive (DPD)), which states:

> *Member States shall provide that the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.*[7]
>
> *Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.*[8]

The difference in approaches between 1995 and today is largely one of context, particularly given the change and the degree to which we interact with technology now. Cybersecurity did not rank highly on legislative, corporate and public agendas in 1995. By contrast, high-profile hacks and the misuse of personal data are now so commonplace that enforcement actions arising from organisations' cybersecurity failings have become a key priority for data protection authorities (DPAs), and one that all levels within a business need to engage with. Enforcement by DPAs in the EU and UK indicate that there continues to be a growing appetite to investigate and penalise infringements of the GDPR's security principles,[9] with

4 'DLA Piper GDPR data breach survey: January 2021' (www.dlapiper.com/en/uk/insights/publications/2021/01/gdpr-data-breach-survey-2021/) [DLA Piper, 'GDPR data breach']. Last accessed on 23 March 2021.

5 Department for Digital, Culture, Media and Sport, 'Cyber Security Breaches Survey 2018' (https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/702074/Cyber_Security_Breaches_Survey_2018_-_Main_Report.pdf). Last accessed on 23 March 2021.

6 Article 32(1) of the GDPR.

7 Article 17(1) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

8 Article 17 of the GDPR.

9 For example, Resolución De Procedimiento Sancionador, Air Europa Lineas Aereas, SA., PS/00179/2020 (15 March 2021) (Spain); Penalty Notice, Marriott International Inc., COM0804337 (30 Oct. 2020) (United Kingdom), available at https://ico.org.uk/media/action-weve-taken/mpns/2618524/marriott-internationa l-inc-mpn-20201030.pdf.

fines available under the GDPR of up to €20 million or 4 per cent of global annual turnover, whichever is higher [10] (though fines of such magnitude have not been imposed and all fines must be proportionate to the offence).[11] Practitioners should take a two-pronged approach to these requirements: first, by focusing on the technical and organisational measures that comprise an appropriate (i.e., compliant) security programme; and second (and relatedly), by remaining alive to the nuances that will often be required when advising on the GDPR's mandatory data breach notification requirements.

Technical and organisational measures

Practitioners are advised to focus their assessment on an organisation's policies and procedures relating to security, whereas a review of technical requirements or measures will usually be undertaken in conjunction with a third-party security provider. Ultimately, there is no one-size-fits-all approach to GDPR compliance and whether a programme is defensible will be assessed in each case.[12] That being said, certain baseline standards are likely to apply to most organisations, including network perimeter defences, malware protection, password policies and secure configuration.[13]

Mandatory breach notification

One of the changes brought in by the GDPR is the requirement to notify data breaches to the regulator and, in certain circumstances, to the individual.[14] The regulator must be notified without undue delay and within 72 hours of becoming aware of the breach,[15] otherwise the organisation may face liability of up to €10 million or 2 per cent of global annual turnover, whichever is higher.[16] The threshold for mandatory notification to a DPA is where there is 'a risk to the rights and freedoms' of individuals;[17] the requirements for notification to affected individuals are higher still.[18] While certain breaches will be obviously reportable, some organisations appear to be struggling to assess breaches at the lower end of the spectrum

10 Article 83(1) of the GDPR.

11 Article 83(1) of the GDPR.

12 This approach has been recognised by data protection authorities in France and the United Kingdom, among others. See, e.g., Commission Nationale de l'Informatique et des Libertés (CNIL), 'Security of Personal Data', 2018 Edition (www.cnil.fr/sites/default/files/atoms/files/cnil_guide_securite_personnelle_gb_web.pdf). Last accessed on 23 March 2021.

13 Article 4(1) of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (the ePrivacy Directive) similarly requires that providers of publicly available electronic communications services 'must take appropriate technical and organisational measures' to safeguard the security of their services, having regard to 'the state of the art and the cost of implementation'.

14 In addition, Article 4(2) of the ePrivacy Directive requires providers of publicly available electronic communication services, where there is a risk of a breach to the security of the network, to inform the subscribers of such a risk.

15 Article 33(1) of the GDPR.

16 Article 83(4) of the GDPR.

17 Article 33(1) of the GDPR.

18 Article 34(1) of the GDPR: 'When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without delay.'

that may not be reportable. In such cases, practitioners should consider any guidance issued by the European Data Protection Board (EDPB) (previously the Article 29 Working Party) or public statements made, and the enforcement actions taken, by the DPA to which a report would be required. Indeed, notwithstanding that the GDPR was designed to harmonise Member States' disparate approaches to implementing the DPD, certain subtle differences in approach among DPAs are already becoming clear in the context of breach reporting.

With that said, most reportable breaches do not result in enforcement. A recent report by the UK Information Commissioner's Office (ICO) is instructive: of the 38,514 data protection complaints the ICO received in 2019/20, only 0.1 per cent resulted in an administrative fine, compliance audit or enforcement notice being served.[19] These figures should not be interpreted as meaning that the vast majority of breaches are not reportable. However, it does illustrate the point that organisations should not be overly cautious in their assessments of personal data breaches. Practitioners should be aware of the potential liability for failing to notify the regulator. However, if an organisation has undertaken a detailed and reasoned approach to investigating and analysing the breach, has carefully considered its impact (if any) and has documented why notification is not required, its assessment will often be shared by the DPA.

Network and Information Security Directive

Unlike the GDPR, which applies only to the processing of personal data, the Directive on Security of Network and Information Systems[20] (NISD) is concerned with network security and the continuity of services and applies both to personal and non-personal data. The NISD is the first EU-wide law on cybersecurity and regulates two types of entities: (1) operators of essential services, being critical organisations in the energy, transport, financial services, health, water supply and digital infrastructure sectors; and (2) providers of digital services, being online marketplaces, online search engines and cloud services providers. The NISD allows Member States to choose the maximum fines that their regulators can impose; in the United Kingdom, breaches of the NISD can result in penalties of up to £17 million.

Like the GDPR, the NISD requires covered entities to implement technical and organisational security measures that are appropriate and proportionate to the risks posed[21] and to report all incidents that have a substantial impact on the provision of their services.[22] Both laws require covered organisations to consider 'the state of the art'[23] measures and the risks posed to individuals in designing their security programmes. While both regimes require notification to the appropriate authority (within 72 hours of becoming aware of a reportable

19 For example, Guidelines 01/2021 on Examples regarding Data Breach (Draft 19 Jan. 2021) (comment period closed). https://ico.org.uk/media/about-the-ico/documents/2618021/annual-report-2019-20-v83-certified.pdf. Last accessed on 23 March 2021.

20 Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security and information systems across the Union [NISD]. The NISD was implemented in the UK prior to Brexit through the Network Information System Regulation (the 'NIS Regulation'), which remains in effect. For convenience, this chapter will refer to both the NISD and the NIS Regulation as the NISD.

21 Articles 14(1) and 16(1) of the NISD.

22 Articles 14(3) and 16(3) of the NISD.

23 Article 32 (1) of the GDPR; Articles 14(1) and 16(1) of the NISD.

incident under the GDPR, and 'without undue delay' under the NISD),[24] there are a number of key differences in the scope of these obligations. Incident reporting is stricter under the NISD, as any significant disruption of services must be notified. In contrast, although breaches under the GDPR must only be notified if the breach leads to destruction, loss, alteration, unauthorised disclosure of or access to personal data, the notification may require disclosure to a wider audience, namely DPAs and affected individuals.

A breach of one law can result in a breach of the other: for example, an avoidable hack of personal data under the GDPR could be separately enforced under the NISD. In such cases, regulatory guidance [25] suggests that dual notifications will be required. However, it is unclear whether separate but related actions will be brought by the regulators in such cases.[26] The answer to this and other questions may be addressed in proposed changes to NISD announced by the EU Commission in December 2020, which include removing the distinction between operators of essential services and digital service providers and expanding the scope of NISD to cover all medium and large companies in selected sectors that are defined by their criticality for the economy and society, as well as smaller businesses with high security-risk profiles. Additionally, there will be an enhanced Cooperation Group to shape strategic policy decisions on emerging technologies and new trends; and increases in information sharing and cooperation between Member State authorities, especially in cyber crisis management.[27]

Cybersecurity Act

On 27 June 2019, the EU Cybersecurity Act[28] came into force promoting an EU framework for cybersecurity certification and creating a permanent mandate for the European Union Agency for Network and Information Security (ENISA) to better support Member States in responding to cyberthreats and attacks. The Act strengthened the coordination and cooperation in cybersecurity across EU Member States and EU institutions. The tailored certification schemes established under the Cybersecurity Act allow companies to certify specific categories of information and communication technologies (ICT) products, processes and services only once and obtain certificates that are valid across the EU. The EU-wide cybersecurity certification framework enables companies in the ICT sector to demonstrate that their products and services meet one of three security standards (basic, substantial or high). The intention of the new rules is to improve trust for consumers, as they can choose between products (such as internet of things devices) that are cyber-secure. The one-stop-shop cybersecurity certification is expected to achieve cost savings and remove potential market barriers

24 Article 33(1) of the GDPR; Articles 14(3) and 16(3) of the NISD.

25 Information Commissioner's Office, 'The Guide to NIS: GDPR and NIS' (https://ico.org.uk/for-organisations/the-guide-to-nis/gdpr-and-nis/). Last accessed on 23 March 2021.

26 Article 8(6) of the NISD states that competent authorities must 'consult and co-operate . . . with national data protection authorities'.

27 Proposal for directive on measures for high common level of cybersecurity across the Union, 16 December 2020 (https://ec.europa.eu/digital-single-market/en/news/proposal-directive-measures-high-common-level-cybersecurity-across-union). Last accessed 23 March 2021.

28 Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No. 526/2013 (Cybersecurity Act).

for enterprises. It is hoped companies will have the incentive to invest in cybersecurity and make this a competitive advantage.

Trends

As technology moves faster than law, so technology crime continues to outpace innovations in security. Cybercriminals tend not to be sentimental – as one patch is rolled out, another vulnerability opens. That being said, we now consider some of the recurring themes in cybersecurity in the EU and UK, as well as highlighting the key trends of which practitioners should be aware.

Targets

Financial services

Given the volume and sensitivity of personal and confidential information that financial institutions process, and the increasing number and sophistication of cyberattacks, information security remains a high priority for the financial services sector.[29] As highlighted in a Report on the Risks and Vulnerabilities in the EU Financial System by the Joint Committee of the European Supervisory Authorities, a particular concern relates to the measures required to address legacy IT systems.[30] Indeed, even the process of upgrading these systems can be perilous: in April 2018, UK bank TSB's migration to a new IT platform resulted in millions of customers being unable to access their accounts for up to one week, as well as increased reports of fraud, and rectification being needed.[31] More recently, the outbreak of covid-19 has required most companies across the EU and UK financial sector and beyond to switch to remote working, resulting in an uptick of digital activity. This greater use of a virtual environment has put even more confidential data and ICT systems at increased risk of becoming targets of hackers and other cybercriminals.[32]

Consumer-facing businesses

It should come as no surprise that consumer organisations are a prime target for cybercriminals, given the volume and range of data they hold and the variety of ways in which security weaknesses can be exploited – from credit card fraud, to identity and intellectual property

29 In the banking sector, 42 per cent of respondents to a 2017 European Banking Authority Risk Assessment Questionnaire reported that these were the main drivers for increasing operational risk; European Banking Authority, 'Risk Assessment Questionnaire – Summary of Results, December 2017' (https://eba.europa.eu/documents/10180/2085616/Risk+Assessment+Questionnaire+-+December+2017). Last accessed 18 March 2019.

30 Joint Committee of the European Supervisory Authorities, 'Joint Committee Report on Risks and Vulnerabilities in the EU Financial System', 20 April 2017 (https://esas-joint-committee.europa.eu/Publications/Reports/Spring%20Joint%20Committee%20Risk%20Report%20(JC%202017%2009).pdf). Last accessed on 24 March 2021.

31 See Letter from Andrew Bailey (Chief Executive of the Financial Conduct Authority) to Nicky Morgan MP (Chair of the Treasury Committee), 30 May 2018 (https://publications.parliament.uk/pa/cm201719/cmselect/cmtreasy/correspondence/fca-to-chair-tsb-300518.pdf). Last accessed 23 March 2021.

32 Joint Committee of the European Supervisory Authorities, 'Joint Committee Report on Risks and Vulnerabilities in the EU Financial System', 4 September 2020 (www.eiopa.europa.eu/content/report-risks-and-vulnerabilities-eu-financial-system_en). Last accessed on 25 March 2021.

theft, among others. At the same time, individuals now expect businesses to have robust security measures in place to protect their data and have a better awareness of their data protection rights. Translated quantitatively, a 2020 report concluded that the average cost of a data breach in the UK is about £2.9 million[33] (even without including the additional reputational cost). The regularity with which consumer-facing companies are suffering large data breaches (Virgin Media,[34] British Airways,[35] Ticketmaster[36] and Marriott International,[37] among many others) demonstrates just how difficult it has become for these organisations to give their customers peace of mind – and why criminals continue to target them.

Internet of Things devices

Internet-connected devices offer criminals a wealth of opportunities to access personal data.[38] That much of this information reveals detailed, and often deeply personal, insights into individuals' private lives makes it especially attractive to bad actors. Approximately 305 million Internet of Things units are predicted to be in use in the EU and UK by 2025,[39] including for use in 'smart' homes, cars, hospitals, airports and cities. Data about the time we leave and return home, how long we shower, and how much electricity we use can all be used to build profiles that are valuable. The result is that this abundance of new data, being stored in systems with multiple points of entry, is increasingly becoming accessible – and valuable

33 L Irwin, 'The cost of a data breach in 2020', *IT Governance*, 3 September 2020 (www.itgovernance.co.uk/blog/the-cost-of-a-data-breach-in-2020). Last accessed on 25 March 2021. See also P Muncaster, 'Cost of UK Data Breaches Rises to £2.7 million', *Infosecurity Magazine*, 11 July 2018 (www.infosecurity-magazine.com/news/cost-of-uk-data-breaches-rises-to/). Last accessed on 25 March 2021.

34 'Virgin Media data breach affects 900,000 people', *BBC*, 5 March 2020 (www.bbc.com/news/business-51760510). Last accessed on 25 March 2021.

35 J Spero, 'British Airways says customer hack much bigger than it thought', *Financial Times*, 25 October 2018 (www.ft.com/content/f8505c34-d863-11e8-ab8e-6be0dcf18713) [J Spero, *Financial Times*]. Last accessed 23 March 2021.

36 R Jones and P Collinson, 'Identity theft warning after major data breach at Ticketmaster', *The Guardian*, 27 June 2018 (www.theguardian.com/money/2018/jun/27/identity-theft-warning-after-major-data-breach-at-ticketmaster). Last accessed 23 March 2021.

37 J Cook, 'Private data of 500 million Marriott guests exposed in massive breach', *The Telegraph*, 30 November 2018 (www.telegraph.co.uk/technology/2018/11/30/private-data-500-million-marriott-guests-exposed-massive-breach/). Last 23 March 2021.

38 In November 2020, the European Union Agency for Network and Information Security [ENISA] released a report entitled 'Guidelines for Securing the Internet of Things' outlining threats to IoT supply chains and best practices for ensuring their security. ENISA, 'Guidelines for Securing the Internet of Things', 9 November 2020 (www.enisa.europa.eu/publications/guidelines-for-securing-the-internet-of-things). Last accessed on 24 March 2021. In a December 2018 speech, the executive director of ENISA stated that there would be an estimated 20 billion operational devices by 2020. Professor Dr Udo Helmbrecht, Cybersecurity best practices', 12 December 2018 (www.enisa.europa.eu/publications/ed-speeches/cybersecurity-best-practices). In actuality, this figure was reached much sooner. By the end of 2018 there were an estimated 22 billion IoT connected devises in use around the world and forecasts suggest that by 2030 there will be 50 billion. Statista, 'Number of Internet of Things (IoT) connected devices worldwide in 2018, 2025 and 2030', (www.statista.com/statistics/802690/worldwide-connected-devices-by-access-technology/#:~:text=By%20the%20end%20of%202018,in%20use%20around%20the%20world).

39 Statista, 'Number of Internet of Things (IoT) units in the electronics industry in the European Union (EU) in 2017, 2020 and 2025' (www.statista.com/statistics/691885/iot-electronics-in-the-eu/). Last accessed on 23 March 2021.

– to cybercriminals. For this reason, the Cybersecurity Act's certification scheme will have an important role in allowing manufacturers of internet-connected devices to demonstrate to consumers that data security is a fundamental aspect of their products and services.

National infrastructure

Cyber incidents affecting critical information infrastructures can have debilitating effects on the security, economy [40] and health of societies,[41] and the protection against which is a key pillar of the NISD. With the exception of state-sponsored actors, incidents involving national infrastructure are often less focused on access to information than the widespread disruption that results – the multiple recent malware attacks on Ukraine's power grid being a case in point.[42] Mirroring the challenges faced by financial services firms, the use of outdated technology in many core infrastructure systems compounds their exposure to even relatively unsophisticated cyberattacks.

Targeted information

Financial and payment data

Hackers most commonly target credit card and debit card details, including 'skimming' data from online retailers by introducing hidden code onto their websites.[43] They do so in spite of the requirements of the revised Payment Services Directive,[44] under which payment providers must implement measures to ensure the security of payment transactions and customer data. Criminals also use social engineering techniques, such as phishing campaigns and scam emails,[45] and sell financial data to third parties in online marketplaces.[46] In 2018, total card frauds in the EU and UK grew 13 per cent from the previous year, reaching a value of €1.8 billion from 21.05 million separate incidents, of which 79 per cent were carried out online (a 39 per cent increase over five years).[47]

---

40 The economic impact of this type of cybercrime in certain Member States, e.g., Germany and the Netherlands, can be as much as 1.5 per cent of gross domestic product. ENISA, 'The cost of incidents affecting CIIs', August 2016 (https://www.enisa.europa.eu/publications/the-cost-of -incidents-affecting-ciis). Last accessed on 11 March 2019.

41 ENISA, 'The cost of incidents affecting CIIs' (footnote 44).

42 A Greenberg, "Crash Override': The Malware That Took Down a Power Grid', *Wired*, 12 June 2017 (www.wired.com/story/crash-override-malware/). Last accessed on 25 March 2021. See also 'Ukraine power cut 'was cyber-attack", *BBC*, 11 January 2017 (www.bbc.com/news/technology-38573074). Last accessed on 25 March 2021

43 See, e.g., the 2018 British Airways hack: J Spero, *Financial Times* (footnote 38).

44 Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No. 1093/2010, and repealing Directive 2007/64/EC.

45 *See* European Central Bank [ECB], 'Executive summary (sixth report on card fraud)', 13 August 2020 (https://www.ecb.europa.eu/pub/cardfraud/html/ecb.cardfraudreport202008~521edb602b.en.html). Last accessed 23 March 2021.

46 M McGuire, 'Into the Web of Profit: Understanding the Growth of the Cybercrime Economy', April 2018 (https://www.bromium.com/wp-content/uploads/2018/05/Into-the-Web-of-Profit_Bromium.pdf [M McGuire, 'Into the Web of Profit']. Last accessed on 23 March 2021.

47 See ECB, 'Executive summary (sixth report on card fraud)', (footnote 49).

Traditional personal data

Personal data is any information that relates to an identified or identifiable living individual.[48] Online digital services have helped turn this data into a financially valuable commodity. Typically, it is targeted (1) to extort individuals (i.e., the victim pays to prevent disclosure), (2) to assist other frauds, and (3) to sell via online markets.[49] Of all the different types of data targeted by hackers, personal data is the most frequently obtained.[50]

Non-traditional personal data

Big Data – the use of large data sets produced by a diverse range of sources – is viewed by the European Commission as fundamental to the future knowledge economy.[51] As part of this drive, esoteric information about all aspects of human life is being collected by governments and businesses with the aim of driving innovation and efficiency.[52] This includes data on individuals' voices, spending habits and gait, among other things, which can potentially constitute personal data.

Unethical data

Hacking is not always driven by financial or malicious intent; occasionally, 'ethical hackers' seek to expose unpopular or illegal behaviour. The targets of their activities are not limited to any particular industry or the size of the organisation. For example, in 2021, hackers exposed vulnerabilities in security cameras of hospitals, schools, factories, jails, and corporate offices to call attention to the dangers of mass surveillance.[53] In 2015, a Canadian private company was targeted because it was seen to be promoting infidelity.[54] The Panama Papers exposed a multinational industry that facilitated fraud, tax evasion and the avoidance of international sanctions.[55] The most high-profile example is Edward Snowden, who disclosed information

48 Article 4(1) of the GDPR.

49 Europol, 'Internet Organised Crime Threat Assessment 2020' (www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020). Last accessed on 24 March 2021.

50 Verizon, 'Data Breach Investigations Report', 2020 (https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf). [Verizon Data Breach Investigations Report]. Last accessed on 24 March 2021.

51 European Commission, 'Industrial applications of artificial intelligence and big data' (https://ec.europa.eu/growth/industry/policy/advanced-technologies/industrial-applications-artificial-intelligence-and-big-data_en). Last accessed 24 March 2021.

52 ENISA, 'The Value of Personal Online Data', 2018 (https://www.enisa.europa.eu/publications/info-notes/the-value-of -personal-online-data). Last accessed 24 March 2021.

53 M O'Brien and F Bajak, Security camera hack exposes hospitals, workplaces, schools', *Associated Press*, 10 March 2021 (https://apnews.com/article/hacking-california-e7b942f436f11b9feb7dc704d4eb3a6b). Last accessed 24 March 2021.

54 A Hern and S Gibbs, 'Ashley Madison hackers release vast database of 33m accounts', *The Guardian*, 19 August 2015 (www.theguardian.com/technology/2015/aug/19/ashley-madison-hackers-release-10gb-database-of-33m-infidelity-site-accounts). Last accessed 24 March 2021.

55 International Consortium of Investigative Journalists, 'Giant Leak of Offshore Financial Records Exposes Global Array Of Crime And Corruption', 3 April 2016 (www.icij.org/investigations/panama-papers/20160403-panama-papers-global-overview/). Last accessed 24 March 2021.

about the US National Security Agency and a global citizen surveillance programme.[56] Although less common than traditional hacking, cases of ethical hacking almost always hit newspapers' front pages and can cause massive reputational harm, as well as potentially legal and regulatory consequences.

Type and nature of actors and actions

Brute force attacks

Brute force attacks involve hacker programs applying trial and error to correctly identify passwords and user names and to find hidden web pages.[57] The techniques for brute force attacks are largely unsophisticated and easy to notice, which results in the vast majority being negated.[58] However, the simplicity of such methods means they are easily deployed and are increasingly popular (an estimated 80 per cent of global data breaches related to hacking in 2020 were the result of brute force attacks or use of stolen credentials).[59]

Government or state-sponsored entities

It is now widely accepted that governments engage in hostile cyber activities to undermine the information and network security of other countries.[60] The most notorious example is the 2020 SolarWinds hack, in which a major United States information technology firm was subject to a cyberattack that was spread to its many clients going undetected for months.[61] High-profile cases such as the SolarWinds hack and allegations of increases in cyber incidents involving European infrastructure have significantly raised public awareness of government-targeted hacking.[62] The unique structure of the EU and UK creates additional challenges, which is being seen in the increasing number of attacks aimed at its IT systems. For example, in 2020, ENISA reported that government administration is among the most targeted sectors for cyberattacks, and that the covid-19 pandemic has contributed to an uptick of attacks in the already strained healthcare sector.[63]

56 'Edward Snowden: Leak that exposed US spy programme', *BBC*, 17 January 2014 (www.bbc.com/news/world-us-canada-23123964).

57 Kaspersky Lab, 'What's a Brute Force Attack?' (www.kaspersky.com/resource-center/definitions/brute-force-attack). Last accessed on 24 March 2021.

58 eSentire Threat Intelligence, 'Annual Threat Report: 2019 Summary & 2020 Predictions' (www.esentire.com/resources/library/esentire-annual-threat-intelligence-report-2019-perspectives-and-2020-predictions). Last accessed on 24 March 2021.

59 Verizon Data Breach Investigations Report (footnote 54).

60 ENISA, 'Securing the Cyber Space in the Light of State Sponsored Activities', May 2017 (www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/securing-the-cyber-space-in-the-light-of-state-sponsored-activities). Last accessed on 24 March 2021.

61 I Jibilian and Katie Canales, 'Here's a simple explanation of how the massive SolarWinds hack happened and why it's such a big deal', *Business Insider*, 25 February 2021 (www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12). Last accessed on 24 March 2021

62 Associated Press, 'EU unveils revamp of cybersecurity rules days after hack', *ABC News*, 16 December 2021 (https://abcnews.go.com/Technology/wireStory/eu-unveils-revamp-cybersecurity-rules-days-hack-74756142). Last accessed on 24 March 2021.

63 ENISA, 'Main incidents in the EU and worldwide', 2020 (www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/etl-review-folder/etl-2020-main-incidents). Last accessed on 24 March 2021.

Criminal attackers

It is estimated that the 2020 cost of cybercrime reached over US$1 trillion – a more than 50 per cent increase from 2018.[64] By some estimates, cybercrime may be the third-largest economy in 2021.[65] The financial rewards, coupled with low risks and low conviction rates, means that cybercrime is an increasingly attractive prospect. Revenues are generated through online illegal markets, where criminals can buy and sell stolen information, from companies' intellectual property to personal information. Criminals also make money through extortion, whereby attackers corrupt computer files with ransomware and then exchange the remedy for money.[66] The ill-gotten gains can then be laundered through legitimate online technologies, such as payment systems and cryptocurrencies such as bitcoin.[67]

AI-assisted hacking

Artificial intelligence (AI), such as machine learning, has the potential to create computer programs that can evade even the most sophisticated cyber defence systems. Traditionally, it was assumed that only state-sponsored entities had the resources to hack using AI.[68] However, these assumptions were challenged in 2018 when the American company IBM showcased a hacking program developed with AI at a security conference.[69] As a result, security experts in the EU and UK are increasingly concerned about AI and its potential for use in hacking and cybercrime.[70]

Nuances in investigative practices and regulatory enforcement

Regulatory enforcement

Enforcement of the EU and UK's cybersecurity laws has been growing of late with the amount of GDPR fines rising 40 per cent in the past year.[71] Whereas past enforcement of security failings produced marginal consequences, more recent GDPR enforcement actions have resulted in significantly higher monetary penalties for businesses.

One of the largest fines under the GDPR (€35 million) was issued in October 2020 by the Data Protection Authority of Hamburg against H&M for the company keeping 'excessive' records regarding employees' families, religions, illnesses and details of their vacation

64 Z Smith and E Lostri, 'The Hidden Costs of Cybercrime', McAfee, December 2020 (www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-costs-of-cybercrime.pdf). Last accessed on 24 March 2021

65 Marc Wilczek, 'Cybercrime May Be the World's Third-Largest Economy by 2021', *Dark Reading*, 4 April 2020 (www.darkreading.com/vulnerabilities---threats/cybercrime-may-be-the-worlds-third-largest-economy-by-2021/a/d-id/1337475). Last accessed on 24 March 2021.

66 Check Point and Europol, 'Ransomware: What You Need to Know', 15 December 2016 (www.europol.europa.eu/publications-documents/ransomware-what-you-need-to-know). Last accessed on 11 March 2019.

67 M McGuire, 'Into the Web of Profit' (footnote 50).

68 See, e.g., the Stuxnet programme allegedly developed by the United States, which shut down Iran's uranium enrichment facilities between 2005 and 2010.

69 J Menn, 'New genre of artificial intelligence programs take computer hacking to another level', *Reuters*, 8 August 2018 (www.reuters.com/article/us-cyber-conference-ai/new-genre-of-artificial-intelligence-programs-take-computer-hacking-to-another-level-idUSKBN1KT120). Last accessed on 11 March 2019.

70 D Rafter, 'Cyberthreat trends: 2019 cybersecurity threat review' (https://us.norton.com/internetsecurity-emerging-threats-cyberthreat-trends-cybersecurity-threat-review.html). Last accessed on 11 March 2019.

71 DLA Piper, 'GDPR data breach' (footnote 5).

activities.[72] In February 2020, another large fine (€27.8 million) was issued by the Italian Data Protection Authority against Telecom Italia for several instances of 'unlawful processing for marketing purposes'.[73] The two largest security-related fines issued to date have been from the Information Commissioner's Office's (UK's Data Protection Authority), against British Airways[74] (€22 million) and Marriot (€20.4 million).[75]

If there was ever any doubt in the years leading up to GDPR's rollout, and shortly thereafter, that the legislation was capable of empowering regulators with significant enforcement abilities, those notions have clearly been dispelled by now. Indeed, the heightened regulatory focus on data security and breach notification, coupled with the substantial monetary penalties that can be issued under the GDPR and the NISD, indicate that seven- and eight-figure fines for cybersecurity failures will continue to become more commonplace.

Guidance

Along with the growing number of reported decisions in this area, practitioners have a growing body of guidance from which to draw when advising clients on how regulators are likely to view the requirements, and potential violations, of EU and UK cybersecurity laws. At the national level, numerous DPAs have been updating their security guidance to reflect the changes introduced by the GDPR, particularly around breach notification.[76] At the supranational level, in January 2021 the EDPB issued additional draft guidance on the type of personal data breaches that require notification under the GDPR. Organisations such as ENISA (in relation to the NISD as well as the wider cyber security context) and sector-specific regulators will also have an important role in helping organisations to equip themselves for the challenges they face in becoming, and staying, compliant with applicable cyber laws.

---

72 European Data Protection Board, 'Hamburg Commissioner Fines H&M 35.3 Million Euro for Data Protection Violations in Service Centre', 2 October 2020 (https://edpb.europa.eu/news/national-news/2020/hamburg-commissioner-fines-hm-353-million-euro-data-protection-violations_en). Last accessed 11 April 2021. See also 'H&M fined for breaking GDPR over employee surveillance', *BBC*, 5 October 2020 (www.bbc.com/news/technology-54418936). Last accessed on 11 April 2021.

73 European Data Protection Board, 'Marketing: The Italian SA Fines TIM EUR 27.8 Million', 1 February 2020 (https://edpb.europa.eu/news/national-news/2020/marketing-italian-sa-fines-tim-eur-278-million_en). Last accessed 11 April 2021. Last accessed 11 April 2021. See also 'Italian DPA issues 27.8M euros for GDPR violation', IAPP, 3 February 2020 (https://iapp.org/news/a/italian-dpa-fines-spa-27-8m-euros-for-gdpr-violations/#:~:text=The%20Italian%20data%20protection%20authority,promotional%20phone%20calls%20without%20consent). Last accessed on 24 March 2021.

74 'ICO fines British Airways £20m for data breach affecting more than 400,000 customers', ICO, 16 October 2020 (https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/10/ico-fines-british-airways-20m-for-data-breach-affecting-more-than-400-000-customers/#:~:text=The%20Information%20Commissioner's%20Office%20(ICO,than%20400%2C000%20of%20its%20customers.&text=The%20law%20now%20gives%20us,%2Dto%2Ddate%20security.%E2%80%9D). Last accessed on 24 March 2021.

75 'ICO fines Marriott International Inc £18.4million for failing to keep customers' personal data secure', ICO, 30 October 2020 (https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/10/ico-fines-marriott-international-inc-184million-for-failing-to-keep-customers-personal-data-secure/). Last accessed on 24 March 2021.

76 See, in particular, detailed guidance issued by data protection authorities in Ireland and Spain.

EU and UK litigation considerations

Cybersecurity litigation in the EU and UK remains small relative to longer established areas of regulation. This is to be expected, given that its two main omnibus laws have been in force for less than three years. Nevertheless, practitioners should prepare for a continuing increase in contentious activity in the coming years and beyond, particularly relating to the fallout from personal data breaches and other high-profile security incidents. In addition to the type of follow-on claims that are common in the antitrust sphere, disputes brought directly by data subjects or their representatives are likely to reshape the EU and UK's cybersecurity landscape in a way that was not contemplated (or, in some cases, possible) under the DPD. The extent to which individuals are now aware of their rights under data privacy and security laws, and the relative ease with which they can be enforced, make it likely that some of the defining aspects of US litigation – large settlement awards and group actions, among others – may become an increasingly common feature of EU and UK cyber disputes.

General Data Protection Regulation

The GDPR provides for two forms of private action. Article 79(1) entitles individuals to an effective judicial remedy when their rights are infringed by the processing of personal data by a controller or processor in violation of the GDPR. Article 79(1) has a wider application than the DPD regime in two important respects.

First, it does not limit liability for compensation to controllers, the result being that if controllers and processors are involved in data processing that infringes the GDPR, each shall be held liable to the data subject for the entire damage.[77] Second, Article 82(1) makes it clear that both material and non-material damage is actionable under the GDPR (i.e, compensation is not limited to when an individual suffers financial harm). Practitioners may be familiar with the decision in *Vidal-Hall*, in which the English Court of Appeal in 2015 interpreted that country's pre-GDPR regime as permitting compensation for non-pecuniary losses.[78] Indeed, the scope for emotional damage caused as a result of cybersecurity incidents (e.g., the distress associated with the theft of personal information) means compensation claims for non-pecuniary losses are likely to be a defining feature of the EU and UK litigation landscape in the coming years.

Article 80 of the GDPR entitles not-for-profit bodies and other public interest organisations to seek effective judicial remedy on behalf of individuals. The ability to issue group proceedings in respect of cyber incidents is a significant development for the EU and UK, and may come to represent a key tool by which controllers and processors are held to account. However, the extent to which this prospect will be realised depends in part on the Member States, as they are given discretion as to whether, and if so how, the GDPR's collective redress provisions are implemented in each territory.[79] Indeed, in early 2021, the UK government

77 Article 82(5) of the GDPR: 'Where a controller or processor has . . . paid full compensation for the damage suffered, [it] shall be entitled to claim back from the other controllers or processors involved in the same processing that part of the compensation corresponding to their part of responsibility for the damage.'

78 *Google Inc v. Vidal-Hall &* Ors [2015] EWCA Civ 311.

79 Article 80(1) of the GDPR provides that Member States (1) must permit an individual to mandate a third-party organisation to lodge a complaint against a data protection authority and/or seek judicial remedies against a controller or processor, but (2) have discretion as to whether that organisation can receive compensation on

announced that it would not allow consumer groups and other not-for-profit bodies to bring actions on individuals' behalf on an opt-out basis. At the time of writing, these provisions are also not being applied evenly across the EU and UK, with early indications suggesting that Member States are unwilling to grant not-for-profit bodies the ability to bring actions on data subjects' behalf (i.e., in a manner similar to the opt-out class actions with which US practitioners will be familiar). In the UK, for example, a court recently ruled that a law firm's costs of building a group action by soliciting potential claimants (e.g., marketing and other advertising costs) were not recoverable costs, thus likely impacting the profitability of organisations seeking to bring about these kinds of actions.[80]

Differences between EU laws and national laws

A key driver behind the introduction of the GDPR was the lack of harmonisation that had developed as a result of the diverging approaches Member States had taken in implementing the DPD.[81] Such fragmentation also exists in respect of Member States' approach to collective redress, and following Brexit this divergence may continue apace in the UK. This is particularly important in the context of cybersecurity, given that (as noted above) some national legislatures may be unwilling to implement the provision in Article 80(2) of the GDPR that permits a form of opt-out class action. A study commissioned by the European Parliament and published in October 2018 revealed the extent to which the landscape remains uneven.[82] Among other things, the Member States surveyed differed – often significantly – in the forms and scope of redress available, the standing to bring actions, and the fees and funding models. For example, contrary to their previously restrictive approach, German courts are increasingly granting significant damages in mass data litigations. To address these considerations, on 25 November 2020, the EU and UK adopted a new directive dealing with representative actions that will allow qualifying organisations to bring about collective actions on behalf of consumers throughout the EU and UK.[83] In addition to these developments, the wider emphasis on consumer protection by the EU and UK's governing bodies makes it probable that, in addition to the GDPR's provisions on collective actions, individuals will in the near future have a range of tools with which to bring mass claims in relation to cybersecurity and related incidents.

---

behalf of the individual. Article 80(2) of the GDPR provides that Member States have discretion as to whether the organisation can, independently of the data subject's mandate, lodge a complaint against a data protection authority or seek judicial remedies against a controller or processor.

80 *Weaver & Ors v. British Airways Plc* [2021] EWCA 217 (QB).

81 Whereas Member States have a significant degree of discretion in transposing the requirements of an EU Directive into national law, an EU Regulation has general application and is directly applicable and binding in its entirety.

82 Policy Department for Citizens' Rights and Constitutional Affairs, Study, 'Collective redress in the Member States of the European Union', October 2018 (www.europarl.europa.eu/RegData/etudes/STUD/2018/608829/IPOL_STU(2018)608829_EN.pdf). Last accessed on 24 March 2021.

83 Directive (EU) 2020/1828 of the European Parliament and of the Council of 25 November 2020 on representative actions for the protection of the collective interests of consumers and repealing Directive 2009/22/EC.

13

Investigations in England and Wales: A Practitioners' Perspective

Michael Drury and Julian Hayes[1]

There is no dedicated, comprehensive cybersecurity law as such in England and Wales. Rather, there is a patchwork of statute-based laws, underpinned by the possibility of civil actions at common law. These laws criminalise unauthorised interference with computers (the Computer Misuse Act 1990 (CMA)); criminalise the interception of communications (Part 1 of the Investigatory Powers Act 2016 (IPA) and the Wireless Telegraphy Act 2006 (WTA)); impose obligations to protect personal data by the application of appropriate technical and organisational security measures (the United Kingdom General Data Protection Regulation (the UK GDPR), Data Protection Act 2018 (DPA), and Network and Information Systems Regulations 2018 (NISR)); and provide state agencies with the power lawfully to interfere with personal property (Part III of the Police Act 1997 (PA) and Intelligence Services Act 1994 (ISA)).

Computer Misuse Act 1990

The CMA, implementing the Budapest Convention on cybercrime,[2] is the principal criminal law deterrent to computer interference. Its basic criminal offence is committed where (1) a person causes a computer to perform any function with intent to secure access to any program or data held in any computer, or to enable any such access to be secured; (2) the access the person intends to secure or to enable is unauthorised; and (3) the person knows at the time when he or she causes the computer to perform the function, that this is the case.[3]

1 Michael Drury and Julian Hayes are partners at BCL Solicitors LLP.

2 https://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf.

3 Section 1 of the CMA, carrying a maximum sentence of two years' imprisonment.

Securing access to a computer or a program encompasses many different actions. 'Computer' is not defined in the CMA.[4] Access is unauthorised if it is obtained by a person who is not entitled to control access to the program or data and is done without the consent of such a person.[5]

The CMA creates further offences where unauthorised access is sought with a view to committing other offences (e.g., theft or fraud);[6] or to impair the operation of a computer,[7] which would include the implanting of viruses or spyware and distributed denial-of-service (DDoS) attacks. The CMA also criminalises the obtaining, making, adapting, supplying or offering of articles for use in committing CMA offences.[8] The most serious offence under the CMA is committed if a person (1) does any authorised act in relation to a computer; (2) at the time of doing the act the person knows that it is unauthorised; (3) the act causes or creates a significant risk of serious damage of a material kind; and (4) the person intends to cause serious damage of a material kind or is reckless as to whether such damage is caused.[9] For the purposes of this offence, damage is of a 'material kind' if it is, for example, to the national security of any country.[10]

Investigatory Powers Act 2016

The IPA was introduced in response to heightened scrutiny of the surveillance activities of public authorities in the UK concerning the government's collection and use of communications and communications data. In essence, the IPA seeks to provide a comprehensive scheme for the use of investigatory powers by public authorities to obtain communications and communications data; undertake electronic surveillance more generally (including through 'hacking'); and access personal data held in large datasets. The IPA aims to ensure that the requirements of the Human Rights Act 1998 and the European Convention on Human Rights are met. Broadly speaking, these powers cover five areas of activity:

- interception warrants (specific and bulk);
- obtaining communications data (including bulk acquisition warrants);
- retention of communications data;
- equipment interference (including bulk equipment interference); and
- using bulk datasets.

A further overarching element is that a telecommunications operator[11] either based in the UK or outside the UK, can be mandated to take steps to give effect to a relevant authorisation by

4 In *DPP v. McKeown*; *DPP v. Jones* [1997] 2 Cr. App. R. 155 HL, Lord Hoffman defined a 'computer' as 'a device for storing, processing and retrieving information.' The Budapest Convention defines a 'computer system' as 'any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data.

5 Section 17(5) of the CMA.

6 Section 2 of the CMA, carrying a maximum sentence of five years' imprisonment.

7 Section 3 of the CMA, carrying a maximum sentence of 10 years' imprisonment.

8 Section 3A of the CMA, carrying a maximum sentence of two years' imprisonment.

9 Section 3ZA of the CMA, carrying a maximum sentence of life imprisonment.

10 Section 3ZA(2)(d).

11 Defined in section 261(10) of the IPA.

way of a technical capability notice (TCN)[12] (except in the case of retention of communications data or bulk datasets). When issuing a TCN, the Secretary of State must be satisfied as to its necessity and proportionality,[13] and approval must be sought from an independent Judicial Commissioner.[14]

Further, the IPA provides the framework for oversight for example by establishing the role of the Investigatory Powers Commissioner and the Investigatory Powers Tribunal.[15]

Wireless Telegraphy Act 2006

Where 'bugging' would not already be caught by the prohibition on unlawful interception contained in the IPA, it may nevertheless be criminalised by the WTA if wireless telegraphy apparatus is used without lawful authority with the intention of obtaining information about the sender, content or addressee of a message, or where information obtained in this way is disclosed.[16] The use of hidden recording devices for covert surveillance may be caught by these provisions.

UK General Data Protection Regulation

On the UK's departure from the EU, the government incorporated the GDPR into domestic legislation, creating the 'UK GDPR'. A series of amendments were then introduced to the UK GDPR by means of Schedule 1 to the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019/419. However, in reality, the data protection regime existing prior to 31 December 2020 remains the same. Pending a data protection adequacy decision by the European Commission (EC), the Trade and Co-operation Agreement (TCA) between the UK and EU stipulates that the UK data protection laws will not diverge from those of the EU for a specified period until April 2021, automatically extendable to June 2021 unless either party objects.

The UK GDPR applies to personal data processing by organisations operating within the UK, and to those operating outside the UK offering goods or services to individuals in the UK.[17] It does not apply to processing by 'competent authorities' (e.g., the police or Crown Prosecution Service) for law enforcement purposes, to intelligence service processing (e.g., the Security Service or Secret Intelligence Service), or to processing by individuals for purely domestic or household activities.[18]

Article 5 of the UK GDPR stipulates that personal data must be processed in accordance with seven principles:

- it must be processed lawfully, fairly and transparently (lawfulness, fairness and transparency);
- it must not be processed in a manner incompatible with the specific, explicit and legitimate purposes for which it was originally collected (purpose limitation);

12 Section 253 of the IPA.
13 Section 253(1) of the IPA.
14 Section 254 of the IPA.
15 See Part 8, Chapters 1 and 2 of the IPA.
16 Section 48 of the WTA.
17 Article 3(2)(a) of the UK GDPR.
18 Article 2(2) of the UK GDPR.

- it must be limited to what is necessary in relation to the purpose for which it was collected (data minimisation);
- it must be accurate and kept up to date (accuracy);
- it must not be kept for longer than is necessary (storage limitation);
- it must be processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (integrity and confidentiality) and
- data controllers must be able to demonstrate compliance with the principles relating to personal data processing (accountability).

Breaches of these principles can lead to the imposition of substantial administrative fines imposed by the Information Commissioner's Office (ICO). The ICO may also prosecute offenders in the criminal courts for offences under the DPA (see below) and CMA. Those suffering damage (including distress) from breaches of the data protection legislation may seek compensation from the controller or processor concerned.

Amplifying the lawfulness, fairness and transparency principle, Article 6 of the UK GDPR provides six bases for the lawful processing of personal data including consent, compliance with a legal obligation, legitimate interest, and the public interest.

The UK GDPR also distinguishes between personal data and 'special category' personal data, the latter including data identifying a person's sexual orientation, political opinions, ethnic origin, health data or constituting biometric data.[19] Under Article 9, the processing of such data is unlawful unless one of the exceptions in Article 9(2) applies, the most obvious being the presence of explicit consent (the word explicit implying a higher degree of consent than under Article 6).

The UK GDPR provides a comprehensive legal mechanism for modern data handling. It stipulates penalties for breaches but allows for the restriction of the scope of rights and obligations to safeguard matters such as public security, the prevention and detection of criminal offences, and other important objectives of general public interest.

Data Protection Act 2018

The DPA, as amended by Schedule 2 to the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019/419, regulates the processing of data by 'competent authorities' (e.g., the police, Serious Fraud Office, Financial Conduct Authority (FCA) and National Crime Agency (NCA) and the intelligence services). In addition, it complements, amplifies and provides exemptions from, the provisions of the UK GDPR. The DPA also contains provisions concerning the ICO, including its enforcement powers.

Subject to certain statutory defences, the DPA criminalises certain behaviour in relation to personal data, including knowingly or recklessly obtaining or disclosing it without the consent of the controller (blagging). It also makes it an offence to retain personal data without the consent of the controller from whom it was obtained; to offer or sell 'blagged'

19 Article 9 of the UK GDPR.

personal data; to 're-identify' personal data that has been de-identified (i.e., processed in such a manner that, without more, it can no longer be attributed to a particular data subject) without the controller's consent; or to process such re-identified data.[20]

Network and Information Systems Regulations 2018

The Network and Information Systems Regulations (NISR) apply to operators of essential services (OES)[21] (e.g., water, transport and energy) and relevant digital service providers (RDSPs)[22] (e.g., online search engines available to the public, online markets and cloud computing services). NISR requires appropriate and proportionate technical and organisational measures to manage the risk of disruption. Incidents significantly impacting essential service continuity must be notified to the applicable competent authority.[23] Where incidents are suspected of having a cybersecurity element, operators are also strongly encouraged to contact the National Cyber Security Centre (NCSC).

NISR was reviewed in May 2020 and the government is considering amendments to its provisions about costs recovery and appeals against Competent Authority decisions.

Police Act 1997 and Intelligence Services Act 1994

Actions that would otherwise be considered breaches of law are made lawful when conducted by state agencies principally in the interests of national security, and for the prevention and detection of serious crime, in accordance with the various authorisation regimes established under IPA, the PA and the ISA.

Part III of the PA provides for authorities to interfere with property where it is necessary and proportionate. Authorisation may be issued by an authorising officer or with prior approval of a Judicial Commissioner where the property affected is someone's home, office premises or where the action may result in acquiring knowledge of confidential, journalistic or legal professional privilege (LPP) material.

The ISA provides a mechanism, on an application by the Security Service, Intelligence Service or GCHQ, for the Secretary of State to authorise interference with property or wireless telegraphy (subject to the requirements of necessity and proportionality).[24]

Relevant law enforcement agencies and other bodies

The primary law enforcement agencies with responsibility for regulating and enforcing the UK's cyber laws are the ICO[25] and the NCA[26]. The NCSC[27] performs a preventative and coordination role in the event that serious incidents occur, deploying expert technical skills to mitigate the impact. Where national security is at risk, the UK's security and intelligence agencies will also be involved.

20 See sections 170 and 171 of the DPA.
21 See Part 3 of the NISR.
22 See Part 4 of the NISR.
23 See, for example, Regulation 11 of the NISR.
24 See sections 5–7 of the ISA.
25 https://ico.org.uk.
26 https://nationalcrimeagency.gov.uk.
27 www.ncsc.gov.uk.

The ICO enforces the DPA and the UK GDPR in the civil arena, and the DPA in the criminal sphere. It is also involved in the regulation of relevant digital service providers under the NISR (see above), regulates organisations engaging in electronic marketing or using cookies,[28] and is the supervisory body for the regulations relating to electronic signatures and online transactions.[29]

The law enforcement body with primary responsibility for investigating and prosecuting cyberattacks is the NCA. The NCA's National Cyber Crime Unit (NCCU) works in conjunction with the UK's Regional Organised Crime Units, the Metropolitan Police Cyber Crime Unit and other national and international strategic partners to tackle serious and organised crime including cyberattacks. The NCCU tackles serious cybercrime incidents both nationally and internationally and offers technical assistance within the NCA itself and to other law enforcement agencies, including through technical interception of communications. It also gathers and coordinates intelligence of serious and organised crime using traditional policing methods such as covert human intelligence sources, undercover officers and technical interception of communications.

Voluntary disclosure to the NCA of information relevant to its functions is encouraged using the information sharing gateway created by the Crime and Courts Act 2013, which absolves informants using it from actions for breach of confidence in the UK and disapplies other restrictions on disclosure.[30] As with other offences, criminal cases prosecuted by the NCA must satisfy the Full Code Test in The Code for Crown Prosecutors,[31] meaning there must be a reasonable prospect of a conviction and also that any prosecution must be in the public interest.

The NCSC protects critical services from cyberattacks, managing major incidents and improving underlying security through advice and guidance on threat reduction and incident management to all sectors, from individuals to large organisations and the public sector.[32] The NCSC has attracted widespread admiration though some observers have expressed concern that its resources may become overstretched as demand grows for its expertise and assistance to deal with swiftly evolving cyberthreats.[33] The coronavirus pandemic has added to the NCSC's burden, as it has been instrumental in ensuring the safe and effective functioning of NHS Trusts during this period.[34]

In February 2020, the UK government announced an Integrated Review of Security, Defence, Development and Foreign Policy,[35] which will help to shape the UK's national approach on cybersecurity beyond 2021. It is expected that the NCSC will play a major role in bolstering the UK's cybersecurity defences going forward.

In addition to the ICO, the NCA and the NCSC, other bodies have assumed secondary regulatory oversight roles for cybersecurity. For example, under Principle 11 of the Financial

28 Through the Privacy and Electronic Communications (EC Directive) Regulations 2003/2426, now retained EU law under the European Union (Withdrawal) Act 2018.

29 Electronic Identification and Trust Services for Electronic Transactions Regulations 2016, also retained EU law.

30 Crime and Courts Act 2013, Section 7.

31 www.cps.gov.uk/publication/code-crown-prosecutors.

32 www.ncsc.gov.uk/section/about-ncsc/what-we-do.

33 https://publications.parliament.uk/pa/jt201719/jtselect/jtnatsec/1708/170808.htm.

34 See NCSC annual report 2020: www.ncsc.gov.uk/annual-review/2020/index.html.

35 www.gov.uk/government/collections/integrated-review-ministry-of-defence.

Conduct Authority (FCA) Handbook, regulated firms must notify the FCA of 'material cyber incidents' (i.e., those resulting in significant data loss affecting a large number of customers, or result in unauthorised access to, or malicious software on, information and communications systems).[36] The FCA offers tools by which firms conducting regulated activities may assess their cyber resilience. Where a firm is registered with the Prudential Regulation Authority (PRA), it should also report cyber incidents to the PRA.[37]

ICO enforcement regime

The ICO is the independent supervisory authority responsible for monitoring the application of the UK GDPR. The ICO's tasks are enumerated in the UK GDPR,[38] and they include monitoring and enforcement, promoting awareness of the obligations of controllers and processors, and providing mutual assistance to overseas supervisory authorities.

ICO investigations may start in a variety of ways, including a complaint by a data subject, information received from other regulators,[39] or of its own volition where the ICO has a concern about a particular sector. The ICO may also commence investigations as a result of whistle-blowing information, and the Information Commissioner is a 'prescribed person' under the Public Interest Disclosure Act 1998, meaning that qualifying disclosures to the ICO (e.g., a worker's reasonable belief that a crime has been committed or that a person is failing to comply with a legal obligation) should not give rise to any detriment to the informant. Between 1 April 2019 and 31 March 2020, 427 whistle-blowing disclosures were made to the ICO, and the regulator took further action in relation to 16 per cent of these.[40]

The ICO's specific enforcement powers are detailed in Parts 5 and 6 of the DPA, and include the right to seek a warrant of entry and inspection where controllers or processors of personal data are suspected of failing to comply with certain UK GDPR provisions, or where a criminal offence under the DPA is suspected.[41] However, unless a judge is satisfied that the matter is urgent or that advance warning of the search would defeat the object of entry to the target premises, the ICO must give seven days' notice in writing to the occupier as one of several preconditions for the issue of a search warrant.[42] Nevertheless, prudent controllers and processors will have a 'dawn raid' plan in place for 'no-notice search warrants'. Such plans would include ensuring reception staff know who to contact and having an internal and external team in place to deal with incidents, including the identification of legally privileged material that is exempt from inspection and seizure.[43]

It is a criminal offence to intentionally obstruct the ICO in the execution of a search warrant, to fail to provide reasonable assistance in the execution of the search warrant without reasonable excuse, or to give a deliberately or recklessly false explanation of any document or other material found on the premises.[44] During the execution of a search warrant,

36 www.handbook.fca.org.uk/handbook/PRIN/2/1.html?date=2016-03-07.
37 https://www.fca.org.uk/firms/cyber-resilience .
38 UK GDPR Articles 57 & 58 respectively.
39 https://ico.org.uk/about-the-ico/our-information/working-with-other-bodies/.
40 https://ico.org.uk/about-the-ico/our-information/whistleblowing-disclosures/.
41 Section 154 and Schedule15 of the DPA.
42 Schedule 15, para 4 of the DPA.
43 Schedule 15, para 11 of the DPA.
44 Schedule 15, para 15 of the DPA.

occupiers should make careful records (and where possible take copies) of all information and systems accessed by the ICO. The ICO may exercise reasonable force when executing a search warrant.[45]

The ICO has published a Regulatory Action Policy (RAP),[46] listing its regulatory objectives, adumbrating on the nature of its powers, and setting out how the ICO will select appropriate regulatory activity for breaches of information rights. The RAP indicates that, as a general principle, more serious breaches (e.g., where there is a high impact, the breach was intentional, or where there are recurring breaches) may expect stronger regulatory action. In 2020, the ICO issued draft statutory guidance detailing how the regulator will take regulatory action against organisations and individuals, emphasising the ICO's risk-based approach, and explaining the method by which it calculates penalties.[47]

Article 83 of the UK GDPR sets out two categories of UK GDPR infringement, each with different penalties. The first category carries a maximum penalty of up to 2 per cent of a business' global annual turnover or up to £8.7 million, whichever is the greater. Included in this first category is a failure to take adequate security measures to protect personal data. Also included in this category are failures to comply with record-keeping obligations; failures to designate a data protection officer when required to do so; and failures to cooperate with the ICO. The second category of offence carries a maximum penalty of up to 4 per cent of a business' global annual turnover or £17.5 million, whichever is greater. Within this category are individual offences related to the processing principles, the rights of data subjects and obstruction of the ICO.[48] The lists of infringements in both categories are not exhaustive, and may be expanded in the future.

Before issuing a penalty notice, the ICO must serve a notice of intent, setting out the circumstances of the breach, the ICO's investigation findings, and the proposed level of penalty. The recipient then has 21 days in which to make representations about the imposition of a penalty and its level, before the ICO reaches its final decision.[49] In the first instance, appeals lie to the First Tier Tribunal (Information Rights).[50]

The RAP suggests that the heaviest penalties will be imposed on organisations that repeatedly and wilfully transgress their obligations, and where formal regulatory action would serve as a deterrent to others. When deciding on the level of the penalty imposed, the ICO will take into account aggravating factors (e.g., whether an organisation has made any financial gain as a result of the failure to report), and mitigating factors such as economic impact of the penalty and ability to pay. Deliberate failure, the involvement of vulnerable victims or a poor regulatory history, are likely to increase the size of the penalty imposed.

In addition to its civil enforcement powers, the ICO may prosecute criminal offences in the DPA.[51] Those convicted of such offences may only be fined.[52] However, the ICO has

45 Schedule 15, para 7 of the DPA.

46 https://ico.org.uk/media/about-the-ico/documents/2259467/regulatory-action-policy.pdf.

47 https://ico.org.uk/media/about-the-ico/consultations/2618333/ico-draft-statutory-guidance.pdf .

48 Article 83(6) of the UK GDPR.

49 See page 25 of the ICO's Regulatory Action Policy.

50 Section 162 of the DPA.

51 For example, sections 170–173 of the DPA.

52 Section 196 of the DPA.

found creative ways of overcoming this limitation, securing custodial sentences through prosecuting instead for CMA offences.[53]

ICO enforcement activity

Future data regulatory divergence between the UK and EU may render comparisons of regulatory activity between the ICO and EU Member State's respective data supervisory authorities difficult. For the time being, however, the UK and EU regulatory regimes are essentially equivalent, and meaningful comparisons remain possible. Judged by the level of GDPR penalties imposed, the ICO is one of the toughest regulators: only Italy, Germany and France imposed fines of larger overall value in the period May 2018 to January 2021, and the UK imposed the fourth and fifth largest GDPR penalties of all EU data supervisory authorities in the same period.[54]

Resourcing is a constant issue for data regulators when taking enforcement activity against some of the world's wealthiest companies; underfunding of data supervisory authorities was a universal issue mentioned by the EC in a report published in 2020 to mark the two-year anniversary of the GDPR's implementation.[55] Even the comparatively well-funded ICO was nevertheless believed to employ only 22 specialist technical investigators, and its resources were less stretched during the pandemic as regulatory activity was pared back. As activity levels normalise, the ICO anticipates that its spend will increase in key areas, heralding increased regulatory work and greater pressure on its resources.

Non-state authority investigations

Although relatively well-resourced, UK law enforcement's cyber capability inevitably faces practical limits on its ability to tackle increased levels of cybercrime. Just as other areas of crime have seen increasing interest in private prosecutions, victims of cybercrime may in future wish to take active steps to conduct their own cyber investigations, including 'active defence' (colloquially known as 'hacking back'). However, in the UK such steps are significantly hindered by the manner in which the law is cast. This is particularly so given how the broadly constituted 'unauthorised access' element of the CMA works to criminalise actions even if taken to protect the rights and properties of a 'victim', [56] the way in which the UK's data protection legislation safeguards personal data, and the requirement that prosecutions for DPA offences are brought only by the ICO or with the Director of Public Prosecutions' consent.[57] In such ways, the law provides a real barrier to an investigation by non-public entities that feel they have been wronged and suffered damage. In consequence, such entities are effectively limited to working with computers and data they either control, or to which voluntary access is given. However, voluntary access may not be forthcoming given the

53 https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/11/six-month-prison-sentence-for-motor-industry-employee-in-first-ico-computer-misuse-act-prosecution/ & https://ico.org.uk/action-weve-taken/enforcement/kim-doyle-and-william-shaw/.

54 British Airways and Marriott International Inc.

55 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0264&from=EN.

56 See sections 1 & 2 of the CMA.

57 Section 197 of the DPA.

potential liabilities that may result, not only for those giving access, but also for intermediaries facilitating it.

Without being granted voluntary access to third-party data, those undertaking private investigations will need to seek the assistance of the courts in the form of *Norwich Pharmacal* orders, obliging innocent third parties caught up in wrongdoing to disclose the identity of perpetrators of cybercrime. However, seeking such orders may still be costly and time-consuming. Alternatively, private investigators may seek the assistance of the relevant authorities, likely to be the NCA (subject always to the NCA having a necessary criminal justice justification for acting).

Privileged investigations in the United Kingdom

Regardless of whether an investigation is internal or being undertaken by external agencies, legal professional privilege is likely to be a significant consideration, and this applies equally to cyber investigations. Indeed, in some respects it is difficult to imagine an investigation that does not involve some element of electronic data and information technology and computer networks.

Whatever the genesis and form of a cyber investigation, it will be important to bear in mind the definitions of privilege and the complex rules that are features of it.

In very broad terms, legal advice privilege attaches to communications between a client and a lawyer in connection with the giving or receiving of legal advice. Litigation privilege attaches to documents created for the dominant purpose of conducting existing or reasonably contemplated adversarial litigation (here, privilege may extend to third parties as well as clients and lawyers). Crucial to establishing and maintaining either form of privilege, particularly in the face of investigations by regulators and law enforcement, are the existence of client–lawyer (including in-house lawyer) relationships and confidentiality of documentation. In most circumstances, privilege does not attach to pre-existing documents or non-privileged email attachments merely by sending such material to lawyers.

Those involved in an investigation should have the following points in mind from the earliest stages:

- External legal counsel should be engaged promptly to ensure the requisite creation of a client–lawyer relationship. While privilege attaches to communications between a client and in-house counsel, the role of such lawyers is not always exclusively the provision of legal advice. To avoid arguments about the dominant purpose of in-house counsel's communications, it may be prudent to engage external lawyers from the outset.
- The nature of the advice sought should be referred to in outline in the letter of engagement if privilege over that document is to be maintained.
- The identity of the 'client' should be carefully established from the outset, preferably in the letter of engagement. Legal advice privilege attaches only to communications between lawyers and a client (or a client's agent in certain circumstances), that is, those individuals tasked with seeking and receiving legal advice on behalf of an entity.
- Since confidentiality is a prerequisite for the existence of privilege, care should be taken to ensure privileged material is circulated only on a need-to-know basis. Before sharing detailed information with third parties such as insurers, non-disclosure agreements should be negotiated.

- Where privileged material is referenced at internal meetings, it may be prudent to record privileged discussions in a separate document rather than in general minutes. Similarly, warnings should be given about making manuscript notes of privileged advice that may in themselves not be privileged.
- All legally privileged material created during the course of an investigation should be marked appropriately, for example by including the words 'Confidential – Subject to Legal Professional Privilege'. While characterising communications in this way is not determinative of privilege, it should raise the issue in the mind of any external regulators and law enforcement, will assist subsequent identification, and may ensure caution is exercised when disseminating communications.
- Since litigation privilege attaches only where adversarial proceedings are in reasonable contemplation at the time a particular communication is made, careful consideration must be given to whether the facts give rise to the necessary circumstances.
- The use of third parties (e.g., an external IT forensic team) should be carefully considered and care must be taken to ensure their work is protected by privilege – generally by ensuring instruction through external counsel appointed to advise on or handle the investigation.

While regulators and law enforcement are not permitted to seize privileged communications, when they exercise their investigatory powers, there are inevitably circumstances in which it is not possible to separate privileged from non-privileged material onsite. In such circumstances, provision is made allowing for the uplifting and subsequent sift of such 'mixed material'.[58] Where electronic data is seized in this way, electronic search terms are often sought to identify privileged (and relevant) material. Those advising individuals and companies whose material has been seized will wish to ensure that any risk to their clients' privilege is minimised during this process.[59]

Cyber investigations – cross-border data sharing

In the context of cross-border investigations, there is now a discernible trend towards greater international sharing of information and evidence, no more so than in cyber investigations.

Recognising that increased information exchange and international cooperation is key to tackling cross-border crime, the Crime (Overseas Production Orders) Act 2019 (COPOA) has been enacted to facilitate the expedited sharing of electronic data between law enforcement bodies in the UK and countries with which the UK has a 'designated international cooperation arrangement'.[60] In reality, the COPOA was drafted specifically to provide for electronic data sharing with the US and to overcome the lengthy delays experienced with Mutual Legal Assistance requests.[61] However, there is no statutory reason that similar treaties may not be agreed with other nations. The EC has itself proposed the introduction of overseas production and preservation orders that would bring about similar cross-border

58 Criminal Justice and Police Act 2001, Part 2.

59 *R (McKenzie) v. Director of the Serious Fraud Office* [2016] EWHC 102 (Admin).

60 Crime (Overseas Production Orders) Act 2019, Section 4(2).

61 See the House of Lords Briefing on the Crime (Overseas Production Orders) Bill: file://vbclfile/Home$/jhayes/Downloads/LLN-2018-0076%20(3).pdf.

electronic data exchange throughout the EU. Before the UK departed the EU, the UK government had expressed reservations about participating in the pan-EU proposal, citing a reluctance to share data with more authoritarian EU Member States, along with a fear that participating might undermine the operation of the bilateral US–UK electronic data sharing agreement, which was seen as more significant for UK law enforcement.

Under the COPOA, appropriate officers of law enforcement agencies including the SFO, FCA and HMRC may apply to Crown Courts in England Wales for an order directly requiring overseas service providers to produce or grant access to electronic data for the purposes of investigating and prosecuting indictable or terrorist offences.[62] Respondents must be given notice of applications unless the court directs otherwise, allowing for representations on the scope of the application, and practicality of compliance before any order is made. Recipients of an order would be expected to produce the data within a specified time frame on pain of contempt proceedings.[63] Further procedural details may be found in the Criminal Procedure Rules.[64] The UK–US bilateral agreement and the COPOA are expected to begin operating during 2021.

Cyber regulatory trends

Governments around the world have been re-examining existing models of online regulation for some time, and the UK has been at the forefront of this trend, particularly in the fields of online harms.

Following a 2019 online harms consultation, the government has published its full response.[65] Aimed at both illegal online harms such as terrorist content, child sexual exploitation and abuse material, and legal but harmful material such as cyberbullying and promotion of self-harm, the proposals will introduce a duty of care on service providers to take action to prevent user-generated content or activity on their services from causing significant physical or psychological harm to individuals. All service providers will be obliged to take action against illegal content and activity. Where children may use a service providers' products, those providers must also protect children against legal but harmful content and activity. High-risk 'Category 1' providers[66] will have additional obligations in respect of legal but harmful content accessed by adults. The government has declined to include investment fraud and other financial scams in the scope of its online harms proposals, though the FCA, trade bodies and consumer groups have called for their inclusion because of their prevalence. The online harms regime will be enforced by the communications regulator Ofcom, which will have the power to impose administrative penalties of £10 million or 10 per cent of the parent company's annual global turnover (whichever is the higher). Draft legislation is expected during 2021.

62 See Sections 1–15 of the COPOA.

63 Criminal Procedure Rule 47.68.

64 Criminal Procedure Rules 47.66–47.71.

65 www.gov.uk/government/consultations/online-harms-white-paper/outcome/online-harms-white-paper-full-government-response.

66 To be determined by size and the functionalities offered.

Implications of Brexit for UK data regulation and cyber investigations

In February 2021, the EC published draft adequacy decisions in the UK's favour under the GDPR and Law Enforcement Directive,[67] which are likely to be adopted later in the year. As a 'bridging' measure to preserve the £127 billion of personal data-enabled trade between Europe and the UK,[68] the TCA agreed between the UK and EU provided that the UK shall not be treated as a 'third country' for cross-border data transfers for four months from 1 January 2021, automatically extended to six months unless either side objects. This 'holding position' was conditional on the UK not changing its data protection laws and the ICO not approving new data transfer mechanisms or codes of conduct without prior EU consent during the four to six month period.[69] UK data regulation is therefore unlikely to change in the short term.

Looking to the future, though, the government's National Data Strategy,[70] with its implicit aim of alleviating the burden of the current data regime on SMEs, its overt mission to champion international data flows, and a new Information Commissioner in office from October 2021 whose job specification emphasises the economic potential of data and avoiding unnecessary barriers to its use, suggest the UK's data protection regime will change once the EC's adequacy deliberations are concluded. The significance of such changes will only emerge over time, but divergence will mean that an adequacy decision in the UK's favour may be vulnerable not only to the risk of challenge in the Court of Justice of the European Union by data activists, but also to the possibility of withdrawal by the EC itself.[71] The economic risks posed by data inadequacy[72] may, however, moderate the UK's appetite for deviating from EU data regulation standards.

During the early stages of the Brexit talks, ministers were hopeful of continuing close cooperation between the UK and EU over cybersecurity, and the UK's expertise in this area was perceived as a negotiating advantage. However, the TCN deals only briefly with cybersecurity with the UK and EU agreeing to 'endeavour to establish a regular dialogue' in relation to such matters.[73] The UK may – by invitation – participate in certain activities with the EU's Cybersecurity Agency ENISA, CERT EU[74] and the EU CSIRT network.[75] In practice, given the international nature of cyberthreats and the UK's capability in these areas, close but low-key UK-EU cooperation will likely continue.

At a more day-to-day law enforcement level, the UK will retain access to EU passenger name records, and the Prüm database of biometric data, which may in future be expanded to include facial recognition data. The UK will no longer be a member of the EU's law enforcement agency, Europol, but it may second staff there to enhance cross-border cooperation, and UK law enforcement will have access to Europol's secure messaging service. Adequacy

67 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32016L0680.

68 www.ucl.ac.uk/european-institute/sites/european-institute/files/ucl_nef_data-inadequacy.pdf..

69 TCA, Part 7 Final Provisions, Article FINPROV 10A Interim provision for transmission of personal data to the United Kingdom.

70 www.gov.uk/government/publications/uk-national-data-strategy/national-data-strategy.

71 By means of EU GDPR Art. 45(5).

72 See footnote 67.

73 TCN Part 4 – Thematic Co-operation, Title 2 Cyber security.

74 The Computer Emergency Response Team which responds to information security incidents and cyberthreats.

75 Dealing with network and information systems.

decisions in the UK's favour should cement continued cooperation, which is surely in the interests of both the UK and EU. Significantly, however, the UK will not have access to the Schengen Information System, SIS II, Europe's largest public security information database offering 'real-time' alerts on wanted and missing persons or objects across the EU. UK police checked SIS II 600 million times in 2019, and its loss will hamper the speed and accuracy of UK law enforcement activity, as UK law enforcement is now left reliant on INTERPOL's Red Notice and diffusion databases to which not all EU Member States routinely upload.

14

Cyber Trends in China

Yan Luo, Zhijing Yu, Ashden Fein and Moriah Daugherty[1]

Cyber requirements in China

Cybersecurity law

China's Cybersecurity Law (CSL), which came into effect on 1 June 2017, is the first national law for regulating cybersecurity and data privacy. The CSL expands the Chinese government's authority to regulate many activities that were previously unregulated or addressed only in a sector-by-sector fashion.

The CSL imposes a series of affirmative cybersecurity requirements on network operators, broadly defined as owners and managers of networks and network service providers. These requirements are described under the following articles:

- Article 10: Safeguard the cybersecurity and stable operations of networks; effectively respond to security incidents; prevent illegal and criminal cyber activities; and maintain the integrity, confidentiality, and availability of network data.
- Article 21: Implement specified controls to protect networks from disturbance, damage, or unauthorised access and protect data from being divulged, stolen or altered.
  These controls include:
  - formulating an internal security management system and operating procedures, determining the persons in charge of network security and performing network security protection obligations;
  - adopting technical measures to prevent malware and network intrusions;
  - adopting technical measures to monitor and record network operation status and network security incidents, including retaining the relevant network logs for at least six months;

1 Yan Luo and Ashden Fein are partners, Zhijing Yu and Moriah Daugherty are associates at Covington & Burling LLP.

  - implementing additional controls in key areas, including data classification, backups and encryption of important data; and
  - complying with other obligations prescribed by law and administrative regulations.
- Article 25: Develop incident response plans and use such plans to respond to any cybersecurity incident that occurs; respond to security risks in a timely manner; take appropriate remedial measures to respond to cybersecurity incidents; and report any incident to the competent authorities.

Under Article 27, the CSL also prohibits network operators from taking certain actions, including: engaging in or providing programs or tools for activities endangering network security, such as illegally intruding into others' networks; disturbing the normal function of others' networks or stealing network data; and knowingly providing technical support, advertising, promotion, payment settlement, or any other assistance to any individual or organisation engaging in activities that endanger network security.

Pending legislation

On 2 July 2020, China released the draft Data Security Law for public comment. The Law focuses on the protection of important data, which is defined as data that may directly affect China's national security, economic security, social stability or public health and security once leaked. The Draft Security Law also mandates that entities carrying out data activities establish a system to ensure data security and enhance risk-monitoring capabilities.

China also released the draft Personal Information Protection Law (the Draft PIPL) on 21 October 2020, which will become China's first comprehensive law in the area of personal information protection. The Draft PIPL specifically requires individuals and organisations processing personal data to adopt organisational and technical security measures to prevent data breaches.

MPS regulations

Multi-Level Protection Scheme

In 2007, the MPS promulgated the Administrative Measures for the Multi-Level Protection Scheme of Information Security (MLPS 1.0), a regulation designed to impose enhanced cybersecurity requirements on the most critical infrastructure information systems in China.

After the promulgation of the CSL in 2016, the MPS was tasked with updating the MLPS 1.0 to fit into the broader framework established by the CSL. On 27 June 2018, the MPS released a draft of the Regulations on Cybersecurity Multi-Level Protection Scheme (the Draft MLPS Regulation) for public comment. Based on the current Draft MLPS Regulation, once enacted, the updated regulation will impose additional specific cybersecurity requirements on network operators.

All network operators will be required to have a cybersecurity programme with a series of specified policy and technical controls, including (1) limiting access to systems and data; (2) providing cybersecurity training for relevant employees; (3) ensuring personal information is encrypted; (4) establishing various monitoring and logging capabilities; and (5) establishing processes for reporting cybersecurity incidents.

The network operators responsible for the systems identified as the most critical in China will be required to meet additional and more stringent requirements, including (1) appointing a member of senior management to be responsible for cybersecurity; (2) formulating an overarching cybersecurity plan and data integrity protection strategy that is reviewed and approved by professional technical personnel; and (3) conducting annual classification testing on networks and reporting the results of that testing and any remediation measures to the MPS and other relevant regulators.

Other MPS regulations

On 30 September 2018, the MPS released the Regulation on Internet Security Supervision and Inspection by Public Security Organs, which establishes that the MPS (and its local forces, commonly referred to as public security bureaus or PSBs) has the authority to conduct cybersecurity inspections of companies that provide a broad range of internet services in China.

These inspections are designed to determine whether the company has met the MPS' requirements for companies that provide internet services in China, including whether the company has (1) implemented internal cybersecurity programmes and appointed an officer in charge of cybersecurity; (2) recorded and retained registration information and web logs of users; (3) taken measures to prevent computer viruses and cyberattacks; (4) taken measures to prevent the transmission and publication of illegal content; and (5) cooperated and provided assistance to PSBs in investigations relating to national security, terrorism and crimes.

Sectoral requirements

In addition to the requirements specified in the CSL and MPS regulations, there are sector-specific requirements relating to cybersecurity, most of which pre-date the CSL. It remains unclear if and how the post-CSL regulations implemented by the MPS will affect these requirements.

Healthcare industry

Healthcare service providers that collect and store population health information[2] and health and medical big data[3] are required to establish disaster recovery and data backup systems and to conduct regular backup and recovery testing.[4] Healthcare service providers are required to implement additional measures protecting health and medical big data, including adopting

2 'Population health information' is defined as basic demographic information, medical and healthcare services information, and other population health information generated by medical, healthcare and family planning services agencies of all types and at all levels. See Article 3, Administrative Measures for Population Health Information (Trial).

3 'Health and medical big data' is defined as health and medical data generated in the course of disease control and prevention as well as health management. See Article 4, State Administrative Measures on the Standard, Security and Service Regarding Health and Medical Big Data.

4 Article 9, Administrative Measures for Population Health Information (Trial), released by the National Health and Family Planning Commission (the current National Health Commission) on 5 May 2014. See also Article 18 of the State Administrative Measures on the Standard, Security and Service Regarding Health and Medical Big Data, released by the National Health Commission on 12 July 2018.

verification and access control measures, standardising data access management and establishing accountability measures for data breaches or other cybersecurity incidents.[5]

Financial industry

All banking financial institutions are required to implement a series of controls for data protection and cybersecurity, including establishing effective internal control systems, adopting effective technical measures to prevent data breaches, implementing training programmes and requiring all personnel who handle personal financial information to sign non-disclosure agreements and keep personal financial information confidential.[6]

All credit reporting institutions are required to establish internal security policies and procedures and to adopt effective technical measures to protect data security.[7]

All bank card clearing institutions are required to ensure the security of infrastructure used for bank card clearing services, comply with the MLPS regulations, use commercial encryption products that are approved by the government and not outsource core business systems.[8] Financial institutions are required to keep confidential consumer information and take technical measures to ensure that the consumer information is not lost, damaged, leaked or tampered with. If a security incident occurs, financial institutions are obligated to take remedial measures and notify consumers.[9]

National standards

In addition to the national and sector-specific regulations, China also has a series of cybersecurity-related national standards. Although they are not legally binding, the Chinese government has recently begun to emphasise their importance and, as such, these national standards can serve as an important barometer of the varying agencies' interpretations of laws and regulations.

The government body responsible for issuing national information security standards, the National Information Security Standardisation Technical Committee, has issued a wide range of information security technology standards (commonly known as TC260 standards) to address a wide range of data protection and cybersecurity topics, some of which provide detailed guidelines for implementing cybersecurity and data privacy requirements as specified in the CSL.

In particular, the TC260 standard GB/T 35273-2020 Information Security Technology – Personal Information Security Specification, which is commonly referred to as 'the Standard', is one of the most cited standards released after the CSL. The Standard includes detailed

5 ibid., Article 23.

6 Article 3, Notice to Urge Banking Financial Institutions to Protect Personal Financial Information, released by the People's Bank of China on 21 January 2011.

7 Article 22, Administrative Regulations on the Credit Reporting Industry, released by the State Council on 21 January 2013.

8 Article 4, Administrative Measures for Bank Card Clearing Agencies, released by the People's Bank of China and the China Banking Regulatory Commission (the current China Banking and Insurance Regulatory Commission) on 8 June 2016.

9 See Implementing Measures of the People's Bank of China for the Protection of Financial Consumers' Rights and Interests, released by the People's Bank of China on 15 September 2020, and which took effect on 1 November 2020.

security protection requirements for data controllers who collect, use, store, share, transfer and publicly disclose personal information; it also includes cybersecurity guidance, including guidance relating to breach notification.

In addition, to implement the updated MLPS framework introduced under the CSL, TC260 has also released a set of new national standards, such as GB/T 22239–2019 Information Security Technology – Baseline for Cybersecurity Multi-level Protection Scheme, providing detailed technical and organisational controls that network operators at each MLPS level must implement.

Incident notification requirements

CSL personal data breach notification requirements

China's incident notification framework is still taking shape. The CSL generally requires network operators to notify competent authorities and affected individuals of any actual or suspected leakage, loss or damage of personal data. In addition, the Standard provides further guidance on the content and timing of the notifications. Under the Standard:

- notification to a government agency shall include:
  - types of affected data subjects;
  - the volume, content and types of the data breached;
  - the potential impact of the incident;
  - the measures already taken or that will be taken in response to the incident; and
  - the contact information for the personnel handling the incident; and
- to the extent that the data breach may cause serious harm to the legitimate rights and interests of the affected individuals, network operators shall notify these affected individuals and such a notification shall include:
  - the content breached;
  - the potential impact of the incident;
  - the measures already taken or that will be taken in response to the incident;
  - suggestions for individuals to prevent and mitigate risks posed by the incident;
  - remedial measures offered to individuals; and
  - contact information for the personnel and office responsible for personal information protection.

In addition, as explained below, the MIIT and the CAC also issued separate regulations setting out incident response requirements that apply to cybersecurity incidents that do not involve personal data. Some of the requirements in these frameworks are vague and may overlap, and it is currently unclear if and how regulators will enforce these requirements.

The draft Data Security Law and the Draft PIPL also introduce certain new incident response requirements. The draft Data Security Law requires entities that carry out data activities to take remedial measures immediately after vulnerabilities are discovered and, when a security incident occurs, notify users and the competent regulator in accordance with regulatory rules in a timely manner.

For breach of personal data, the Draft PIPL specifically sets out that the notification to the affected individuals and the competent regulator shall include:

- the cause or causes of the data breach;

- the categories of the breached personal data and any potential damages caused by such a breach;
- remediation measures that have been taken;
- risk-mitigation measures that individuals may consider taking; and
- contact details of the processing entity.

Therefore, China's existing incident response rules may be subject to changes after the draft Data Security Law and Draft PIPL are enacted.

Regulations and emergency response plans

The Provisions on Protecting the Personal Information of Telecommunication and Internet Users (the MIIT Regulation) require telecommunications operators and internet information service providers to notify regulators without delay if an actual or potential data breach has resulted in or may have serious consequences.[10]

The Emergency Response Plan for Unexpected Incidents on Public Internet (the MIIT Emergency Response Plan) requires basic telecommunications service providers, domain name registration and service providers, and internet companies to notify the provincial telecommunications regulator and the MIIT Emergency Response Office immediately when cybersecurity incidents occur.[11]

The National Cybersecurity Emergency Response Plan (the CAC Emergency Response Plan) requires network operators to report any major cybersecurity incident[12] to the State Cybersecurity Emergency Response Office immediately.

Conducting cyber investigations in China

Cybersecurity investigations – whether in response to data breaches, unauthorised access to information systems or networks, or product-related, cyber-physical or destructive attacks – generally involve both traditional and cyber-specific investigation techniques; many of these techniques are also applicable when conducting investigations in China.

Traditional investigation techniques

Legal privilege

In investigations outside China, particularly those in the United States and Europe, external counsel is often retained to direct and manage investigations, resulting in many post-event communications and certain work-product being protected under applicable legal privileges to the maximum extent possible. Similarly, external counsel can help oversee the issuance of preservation and document holds to assist clients in preserving potentially relevant documents and data, including forensic images and log data relating to the cyber incident.

10 The MIIT Regulation does not define 'serious consequences' and thus the definition is presently unclear.

11 'Unexpected incidents' are defined as network interruptions, system failures, data breaches or spreading viruses caused by cyberattack, intrusion or malware that have or may result in severe social damage or other consequences and that will require the telecommunications regulator to take responsive action.

12 According to Article 1.4 of the CAC Emergency Response Plan, major cybersecurity incidents shall be determined based on damage to networks, threats to national security, and effects on social order, economic development and public interest.

Although external counsel can assist clients in China in protecting post-event communications and work-product, there are additional unique challenges. Attorneys are prohibited from sharing confidential client information with third parties, but China does not otherwise recognise the attorney–client privilege or the work-product doctrine. In addition, everyone in China can be compelled to disclose information to Chinese law enforcement – including attorneys – or to testify in Chinese courts.

Note that even though involving a qualified foreign attorney working in China in investigations will not change the fact that attorney–client privilege is not recognised in China, doing so can help to ensure that legal privileges available in other jurisdictions remain protected.

Fact-finding

In global investigations, including investigations in China, external counsel is often responsible for leading efforts to develop a clear understanding of the cyber incident to inform an appropriate response and to assess legal obligations and risks. Typically, external counsel assist with interviewing key witnesses to uncover noteworthy facts relevant to the investigation, particularly those facts that cannot be readily or adequately discovered through document review or forensic analysis. For example, witness interviews may be helpful in determining the types of data contained within a compromised email account or stored on a specific server that has been accessed by an attacker. When conducting interviews with Chinese-speaking witnesses, it is key to ensure that at least one interviewer has proficiency in Chinese, even if both the interviewer and the witness speak fluent English; otherwise, key concepts – including technical details – may inadvertently be lost in translation. External counsel also may be responsible for reviewing documents, either manually or through an e-discovery platform. Depending on the nature of the cyber incident, the volume of documents may range from small batches of information security policies to all user-generated documents belonging to multiple custodians located in many different countries.

Coordination and management

In China and globally, external counsel often serve as lead or supporting coordinators for a client's global response to an incident. Clients very often rely on external counsel to manage an entire response, including the forensic investigation, which often involves coordinating with various client departments and stakeholders globally (e.g., legal, information technology, information security, corporate governance, communications and human resources).

Cybersecurity-specific techniques

In addition to the standard investigation practices described above, in global cyber investigations, external counsel may use specialist techniques to investigate cybersecurity incidents.

Vendor selection, retention and management

As an initial matter, external counsel often retains appropriate third-party vendors to assist in the client's post-incident investigation, especially if the client does not have the adequate expertise or resources to respond to a specific cyber incident. Because these vendors serve as 'deputies' under external counsel's supervision, in some countries, including the United States, these vendors' work-product and communications with the client may be protected by

legal privilege. Moreover, if specialist vendors are required to assist in a client's investigation, external counsel often is responsible for managing and coordinating these vendors – and, for complex cases, many vendors may be required. For instance, a client may need specialist vendors to (1) conduct forensic examinations of the client's networks and systems; (2) defend the client's networks and systems against further intrusion; (3) assist the client in preserving the affected systems; and (4) conduct open-source and dark web searches to learn more about the individuals or groups potentially responsible for the incident and to identify client data that may have been disclosed in the incident.

Depending on the location of the vendor, the external counsel and the client may also need to consider China's cross-border data transfer requirements. The CSL requires a Critical Information Infrastructure (CII) operator to store personal information and important data collected or generated in the course of operations within China. If a client is considered a CII operator, it may be restricted from transferring data to vendors outside of China. Apart from the specific requirements for CII, China has also released draft rules governing cross-border data transfer by non-CII operators. Once these rules are finalised, the data transfer to vendors outside of China will be subject to additional restrictions.

In China, external counsel can assist clients in vendor selection, retention and management. This is true even though China does not recognise legal privileges (e.g., the attorney–client privilege or the work-product doctrine), particularly because, as discussed above, involving a qualified foreign attorney working in China in investigations can help to protect the investigation under applicable legal privileges outside China.

Assessing legal requirements

In many countries, including China, counsel are also often responsible for conducting assessments of any applicable post-incident legal requirements and assessing associated legal risk. For example, external counsel may be responsible for helping a client ensure its incident response complies with any applicable jurisdiction-specific regulatory requirements (including the China-specific requirements described above); advising on potential employment consequences for employees who are ultimately deemed to have participated in or facilitated the cyber incident; and considering whether any available insurance may assist the client in recovering some of the costs of responding to the incident. In addition, external counsel are frequently involved in assessing legal risks that span multiple jurisdictions, such as the risks associated with data transfers from one jurisdiction to another; this may arise, for instance, when a client would like to conduct forensic analysis in the client's home country but the relevant data resides in another country. In that situation, external counsel can evaluate legal requirements that must be met before a cross-border data transfer can occur and advise clients on the potential risks associated with the transfer. In addition, counsel may evaluate obligations to notify the affected individuals, business customers, partners and service providers, and regulators of the incident.

Regulator outreach

Finally, and crucially, in global cybersecurity investigations in China and throughout the world, external counsel often serve as the lead contact with relevant regulators and law enforcement agencies interested in obtaining information about the incident, which can include providing an initial notification of the incident, sharing indicators of compromise and other

relevant forensic data, and overseeing the client's response to follow-up requests from regulators and law enforcement. For example, in China, external counsel may assist clients in notifying any applicable regulators, including local PSBs, of a cyber incident. External counsel may also assist the client with any subsequent law enforcement investigation.

Recent notable cybersecurity incidents involving Chinese companies

Zhengzhou Sias University

In May 2020, it was reported that certain excel spreadsheets containing personal data of around 20,000 students at Zhengzhou Sias University were widely spread on social media platforms. The personal data that was leaked included name, ID number, age, major and dorm room number of the students. Some students received spam calls after this incident. The police launched an investigation after the incident.

Foxit

Foxit, the developer of Foxit Pdf Reader and Editor, notified users in 2020 that its server had been hacked and certain data was assessed without authorisation. Foxit claimed that hackers may access users' personal data, such as user name, e-mail address, phone number, user account, password and IP address.

Active regulators in China

Although the regulatory environment in China is still developing, it is clear that certain regulators will have particularly active roles in data protection and cybersecurity.

MPS

Under Article 8 of the CSL, the MPS and PSBs are responsible for the protection, supervision and administration of network security. As has already been discussed, the MPS and PSBs are in charge of enforcing the requirements under MPS-issued regulations; in addition, under Article 253a of the Criminal Law, the MPS and PSBs are tasked with investigating crimes involving the illegal obtaining and use of personal information.

CAC

The CAC is expected to play a critical part in future cyber investigations. Under Article 8 of the CSL, the CAC is responsible for coordinating issues of network security. In addition, under the CAC Emergency Response Plan, the CAC is responsible for coordinating and leading the government's response to cybersecurity incidents.

MIIT

As the regulator for the telecommunications industry, the MIIT traditionally focuses on the cybersecurity and data privacy protection pre-dating the CSL. However, Article 8 of the CSL clearly states that the MIIT has the authority to implement the CSL within the scope of its regulatory duty. As a result, the MIIT may actively enforce the MIIT Emergency Response Plan when security incidents affect the telecommunications industry.

15

Japan

Daisuke Yamaguchi, Takashi Nakazaki and Atsushi Nishitani[1]

Key cybersecurity standards and requirements

There are cybersecurity standards to be complied with, and notifications detailing such requirements have been issued by various governmental departments in Japan. For instance, the Ministry of Economy, Trade and Industries (METI) issued the Information Security Management Standards (the METI Standards) (METI Public Notice No. 112 of 2003) in 2003 and updated them in 2016 (METI Public Notice No. 37 of 2016). The Standards were formulated in accordance with international standards and practices. Furthermore, by incorporating the responses to opinions from external experts and public comments, etc., METI included the associated article numbers specified in ISO 27001; added details to the simplified descriptions found in ISO 27001; and, by including other measures, the METI Standards were formulated so that they would contribute to the smooth operation of the information security audit system. The METI Standards consist of two parts: management standards and control measures standards. The management standards part provides for the necessary items for information security management plan-do-check-act procedures, and is based on JIS Q 27001:201, while the control measures standards part provides for possible control measures to be implemented in establishing information security management and is based on JIS Q 27001:2014 Appendix A and JIS Q 27002:2014.

Furthermore, in 2018, METI formulated two additional cybersecurity-related standards: Information Security Service Standards and Standards for Examination-Registration Organizations for Information Security Services.

The Information Security Service Standards overlook:

- information security inspection;
- vulnerability diagnosis;

1 Daisuke Yamaguchi and Atsushi Nishitani are partners and Takashi Nakazaki is a special counsel at Anderson Mori & Tomotsune.

- digital forensics; and
- security monitoring and operation services.

The standards stipulate a certain level of quality to be maintained in the respective services:
- technical requirements (e.g., qualification requirements and explicit indication of specifications); and
- quality management requirements, (e.g., allocation of quality managers to appropriate duties, development of quality management manuals, and where service providers have introduced procedures for maintaining and improving quality).

Examination-registration organisations are bodies established to examine applicants as private information service providers, regarding whether or not the providers' services comply with the Information Security Service Standards, and to register appropriate providers. The Standards for Examination-Registration Organizations for Information Security Services stipulate rules that such organisations should observe, including fairness in examination and general rules for organisation management and examination procedures.

Sectoral standards

Telecommunication sector

The Ministry of Internal Affairs and Communications established the Safety and Reliability Standards of Information and Communication Network in 1987. The Security and Reliability Standards have been amended several times and the latest version was released in 2020. The Security and Reliability Standards consist of two parts (facilities standards and management standards) and contain software measures, information security measures, earthquake countermeasures, power outage measures and various other measures.

Financial sector

The Financial Services Agency (FSA) issued a summary of its policies to strengthen cybersecurity in the financial sector in 2015 and updated it in 2018. The FSA plans to:
- promote continuous dialogue with financial institutions to understand their cybersecurity risks;
- improve information sharing among financial institutions;
- implement cyberattack drills in which financial institutions, the FSA and other public authorities participate; and
- develop human resources specialising in cybersecurity, and also respond to new issues such as accelerated digitalisation and international discussions.

The FSA's guidelines require banks to, among other things, establish an organisation to handle emergencies, designate a manager in charge of cybersecurity, prepare multi-layered defences against cyberattacks and implement a periodic assessment of cybersecurity.

Summary of breach notification rules

There are no general reporting requirements of security breach under Japanese law. As for security breach of personal data, there will be reporting requirements of security breach under the Act on the Protection of Personal Information (Act No. 57 of 2003, as amended) (APPI) from April 2022; however, there are currently no legal requirements of reporting to the authorities under the APPI.

The Amendment to APPI in 2021 will require businesses to report to the Personal Information Protection Commission and notify subjects (who have suffered due to the breach) when a business recognises that there is or might possibly be a security breach that is likely to 'harm the rights and interests of individuals'. Businesses will be required to report to the relevant authority in specified time frames and to inform affected individuals in a timely manner. Reporting will be required in the following scenarios:

1 leakage of special category data (similar to sensitive data);
2 damage to property or potential risk of damage to property;
3 intentional violation of the law, such as unauthorised access; and
4 the breach affects at least 1,000 data subjects.

The amendment requires the reporting to be done twice; in other words, a prompt report must be submitted and a more detailed report submitted thereafter (the latter report must be filed within 30 days of recognising a security breach as described above in (1), (2) and (4), and within 60 days of recognising a security breach described above in (3)). Even on the occurrence of any of the events described above, a business need not report a security breach to the Personal Information Protection Commission if it has implemented sufficient security management measures for protecting the rights and interests of individuals. A typical example of sufficient security management measures would be advanced encryption. This amendment will come into effect on 1 April 2022.

Also, there are reporting requirements in some business sectors, such as the telecommunications sector and the financial sector. As for the telecommunications sector, the Telecommunications Business Act (Act No. 86 of 1984, as amended) (TBA), which is the main legislation governing that sector, requires a telecommunications carrier to report a security breach to a Minister at the Ministry of Internal Affairs and Communication (MIC). Article 28 of the TBA specifies three cases that must be reported:

1 when a telecommunications carrier suspends its telecommunications operations in part pursuant to the provisions of Article 8, Paragraph (2) of the TBA;
2 a violation of secrecy of communications; or
3 any other serious accident specified by order of MIC has occurred with respect to telecommunications operations.

As for item (2), many violations of secrecy of communications cause data breach of personal data belonging to telecommunication service users. Such reporting should be based on the guidelines on data breach reporting in the telecommunications sector, and such reporting should be carried out in accordance with the guidelines.[2] As for item (3), those serious

2 www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/denkitsushin_rouei.html.

accidents are specified in Article 58 of the Ordinance for Enforcement of the TBA. Details are available in the 'Guidelines for Application of the Telecommunications Business Act and Related Regulations on Telecommunications Accidents and Incidents.'[3] A telecommunications carrier is required to report the incident to MIC promptly after its occurrence. In addition, the carrier is required to report details of the incident to MIC within 30 days from its occurrence. The detailed report must include the following items:

- the date and time when the incident occurred;
- the date and time when the situation was remedied;
- the location where the incident occurred (the location of the facilities);
- a summary of the incident and which services were affected by the incident;
- a summary of the facilities affected by the incident;
- details of the events or indications of the incident, the number of users affected and the affected service area;
- measures taken to deal with the incident, including the persons who dealt with it, in chronological order;
- causes that made the incident serious, including how the facilities have been managed and maintained;
- possible measures to prevent similar incidents from happening;
- how the telecoms carrier responded to inquiries from users and how it notified users of the incident;
- internal rules in connection with the incident;
- if the telecoms carrier experienced similar incidents in the past, and a summary of past incidents;
- the name of the manager of the telecoms facilities; and
- the name and qualifications of the chief engineer of the telecoms facilities.

As for the financial sector, the FSA (the main authority supervising the financial sector) issues various guidelines for supervising financial sectors such as banks and insurance companies. For major banks, the FSA issues the Comprehensive Guidelines for Supervision of Major Banks, etc. The Guidelines specify that the FSA requires banks to report a cybersecurity incident immediately after becoming aware of it. The report must include the following items:

- date and time when the incident occurred and the location where the incident occurred;
- a summary of the incident and which services were affected by it;
- causes of the incident;
- a summary of the facilities affected by the incident;
- a summary of damages caused by the incident, and how and when the situation was remedied or will be remedied;
- any effect on other business providers;
- how the bank responded to inquiries from users and how it notified users, public authorities and the public; and
- possible measures to prevent similar incidents from occurring.

3 www.soumu.go.jp/main_content/000743122.pdf.

The government encourages each business industry to share security information among the relevant industry groups. Apart from reporting to the authorities, there are many Information Sharing and Analysis Centers (ISACs) in various business sectors, including the financial sector and the ICT sector. Many ISACs have been established, such as Financials ISAC Japan, ICT ISAC Japan, Japan Automobile ISAC, Software ISAC and Japan Electricity ISAC. Several business sectors have established ISACs, and encourage the relevant industry members to share security information with them. For example, Financials ISAC Japan has two core functions:

- 'collective intelligence', which focuses on intelligence sharing between members in relation to any daily incident or exposed vulnerability; and
- 'resource sharing', which, through cooperative action, pools resources to promote consideration of strategies to deal with shared issues.

A Financial ISAC consists of over 400 financial institutions as regular members and around 30 IT vendor companies as affiliate members. Financial ISACs hold cyberattack drills regularly. If a Financial ISAC finds important information, 100 members will be committed to conducting a variety of activities aimed at building a solid foundation to promote customers' peace of mind, safety and security, which lies at the heart of Japan's financial system.

Best practices for cyber-incident response

Cybersecurity Management Guidelines Version 2.0, issued by METI, indicates best practices for a cyber-incident response. The Guidelines insist that it is important to develop a cybersecurity incident response team, and that relevant procedures should be put in place to establish a response structure within the organisation (a computer security incident response team (CSIRT), etc.) to identify the scope of impact and damage; take initial action to prevent further damage and implement measures to prevent similar incidents from recurring; decide what information should be reported to whom in the case of an emergency; and support management to report that information to internal and external stakeholders appropriately. This is a checklist for best practices:

- Conserve evidence such as various logs and devices infected with malware after being victimised by a cyberattack, for swift identification and analysis of the cause of damage, giving directions to employees to cooperate with relevant organisations for joint investigation. In investigating the cause of an incident, the Guidelines recommend referring to Appendix C of the Guidelines, 'Items to organise within the organisation for the occurrence of incidents.'
- Execute drills in preparation for cyberattacks including developing measures to prevent similar incidents from recurring and reporting to relevant government agencies. The Guidelines recommend considering consulting external experts as necessary for measures to prevent recurrence.
- Prepare a list of emergency contacts (security vendors, etc.) and a list of organisations to disclose information to, including external parties, and share those lists with incident response members.
- Calculate the impact of first response on regular business operations and, based on that, make arrangements in advance with other divisions of the organisation (HR, sales, etc.) for emergencies.

- Check relevant laws and regulations and procedures to fulfil obligations described in the laws and regulations.
- Report to management the damage status and impact to other companies owing to the incidents.

Cybersecurity and Incident response trends:

Increasing number of cybersecurity incidents

As in many other countries, the number of cyberattacks found in Japan has been increasing rapidly. In 2019, 2,960 cases of unauthorised access were recognised in Japan (this is the number of cases reported to the National Police Agency),[4] which was increased by 99.2 points from the previous year. The number of phishings reported to the Council of Anti-Phishing Japan was 55,287 in 2019, which is 2.8 times larger than in 2018.[5]

On 18 December 2020, METI issued a news release 'Alerts to Company Executives to be Issued to Encourage them to Enhance Cybersecurity Efforts in Light of Situations of Recent Cyberattacks'.[6] METI warned in the release that:

- there had been a rapid expansion of diversity of cyberattack patterns targeting supply chains in which SMEs are involved;
- there had been a rapid increase in the number of ransomware victims, regardless of size of enterprise; and
- overseas connections were becoming targets of attackers wishing to steal highly sensitive information.

Challenges in Japan

One of the most crucial issues in cybersecurity areas in Japan is the shortage of cybersecurity professionals. According to a research report,[7] 86.2 per cent of Japanese companies think that they do not have enough human resources for cybersecurity, compared with 16.1 per cent of US companies and 17.1 per cent of Australian companies. Another research report[8] showed that only 22.8 per cent of Japanese companies (among 534 samples) have at least one full-time CSIRT member.

Lack of cybersecurity professionals causes various problems for Japanese companies and sometimes prevents them from quickly finding, responding to and recovering from cybersecurity issues.

4 National Public Safety Commission, Minister of Internal Affairs and Communications and Minister of Economy, Trade and Industry, 'Status of occurrence of unauthorised access and status of research and development on technologies for access-control functions' dated 5 March 2020.

5 Council of Anti-Phishing Japan, 'Phishing Report 2020' dated 23 June 2020.

6 www.meti.go.jp/english/press/2021/1218_001.html.

7 NRI SecureTechnologies, Ltd, 'NRI Secure Insight 2020' published on 15 December 2020.

8 Information-technology Promotion Agency, 'Report on survey of CISO, etc. and promotion of security measures of companies' dated 25 March 2020.

Regulatory consideration

Legal framework

The Basic Act on Cybersecurity (Act No. 104 of 2014, as amended) (BAC), which came into effect in January 2015, was the first act focusing on cybersecurity issues in Japan. The BAC provides the basic framework of government policies of cybersecurity, including basic principles; responsibilities of the Japanese government and local governments; and essential matters for cybersecurity-related policies.

The Cybersecurity Strategy of the Japanese government is determined and published pursuant to the BAC; however, the BAC does not intend to regulate the activities of private companies and individuals directly. Concurrent with enforcement of the BAC, the Cybersecurity Strategic Headquarters (CSH) and National Center of Incident Readiness and Strategy for Cybersecurity (NISC) were established in the Cabinet to promote various cybersecurity related policies and coordinate with various stakeholders in public and private.

Specific regulations and legal responsibilities regarding cybersecurity issues are stipulated in the individual laws and regulations. The following are important laws regarding cybersecurity in Japan.

Personal Data Protection Regulations

The APPI regulates handling of personal data mainly in private sectors. The APPI requires personal information-handling business operators to take necessary and appropriate action for the security control of personal data, including preventing the leakage, loss or damage of its handled personal data. The Act on the Use of Numbers to Identify a Specific Individual in the Administrative Procedure (Act No. 27 of 2013, as amended) (the 'My Number Act') also requires those who are handling of Individual Numbers[9] to take necessary measures to ensure the appropriate management of Individual Numbers, such as preventing the leakage, loss or damage of Individual Numbers.

The main regulator for the APPI and the My Number Act is the Personal Information Protection Commission (PPC), the independent regulatory body established based on the APPI. The PPC is responsible for establishing the Basic Policy on Protection of Personal Information and overseeing compliance of the APPI and the My Number Act. The PPC has issued guidelines on the APPI, providing detailed guidance on the scope and interpretation of the APPI. In addition to the PPC guidelines, relevant administrative authorities have issued guidelines for specific areas, including finance, medical, telecommunication and employment and welfare sectors. Although those guidelines are not legally binding documents, they are generally accepted by companies and legal practitioners.

Other important laws and regulations on cybersecurity

Under the Companies Act (Act No. 86 of 2005, as amended), it is understood that directors of a Japanese company have a duty to establish appropriate cybersecurity measures as part of the internal control system of the company. Breach of such duty could face civil liability (including a shareholder derivative suit) against directors.

9 The Individual Number (My Number) is a unique 12-digit number for each individual provided by the government, and used in social insurance, tax and disaster countermeasure areas within Japan.

In connection with cybersecurity management of companies, METI and the Information-technology Promotion Agency jointly published the Cybersecurity Management Guidelines in 2015, and the latest revised version (Version 2.0) was published in 2017.[10] The guidelines are aimed at the corporate management of major companies as well as small and medium-sized companies and include, from the viewpoint of protecting companies from cyberattacks, the three principles that management need to recognise and 10 important items that management should direct their executive in charge (CISO) to observe in implementing cybersecurity measures. The guidelines themselves are not legally binding, but whether they are followed or not may be an important element to consider for compliance of duty of directors (see the 'Litigation consideration' Section for details).

For the telecommunications sector, the TBA requires telecommunications carriers to maintain telecommunications facilities in conformity with the technical standard specified by the Order of the Ministry of Internal Affairs and Communications, and the technical standard includes detailed cybersecurity related requirements. From April 2020, certain security measures for IoT devices have been included in the technical standards.

As to criminal liability, the Act on Prohibition of Unauthorised Computer Access (Act No. 128 of 1999, as amended) prohibits unauthorised access to computer systems, as well as illegal collection of IDs and passwords of other people and provision thereof. Violators could face up to three years in prison or a ¥1 million fine.

The Unfair Competition Prevention Act (Act No. 47 of 1993, as amended) and Copyright Act (Act No. 48 of 1970, as amended) prohibits provision of software or devices exclusively for the purpose of circumvention of technological restriction or protection measures (i.e., copy control or access control measures). Violators could face up to three years in prison or a ¥3 million fine (under the Copyright Act), or up to five years in prison, a ¥5 million fine, or both (under the Unfair Competition Prevention Act). Acquisition of a trade secret by act of fraud (including unauthorised access stipulated in the Act on Prohibition of Unauthorised Computer Access) shall be subject to up to 10 years in prison, or a ¥10 million yen fine, or both.

The Penal Code (Act No. 45 of 1907, as amended) also prohibits certain cyberattack-related activities including:

- making or distribution of computer viruses (up to three years in prison or a ¥500,000 fine);
- skimming of credit-card information (up to three years in prison or a ¥500,000 fine);
- obstruction of the business of another by interfering with the operation of a computer or damaging electromagnetic record (up to five years in prison or a ¥1 million fine); and
- computer fraud by creating a false electromagnetic record, imputing false data or giving unauthorised commands (up to 10 years in prison).

Cybersecurity regulators

As the CSH and NISC are mainly responsible for strategy planning and coordination, there is no one-stop regulator on cybersecurity matters in Japan. As to the data protection issues, the PPC is the main regulator and has the authority to provide guidance and advice; request reports; conduct on-site inspections, offer recommendations and give orders to governmental

10 www.meti.go.jp/policy/netsecurity/downloadfiles/CSM_Guideline_v2.0_en.pdf.

institutions and business operators who handle specific personal information. For other specific areas and industries, the ministry with jurisdiction over the applicable laws and regulations should be the main regulator (for example, the MIC for telecommunications business).

Litigation consideration

A company that has suffered a cyberattack may be sued by an affected business partner or individual, or a lawsuit may be instituted by a shareholder against the company's directors and officers.

Suit against a company by a business partner or individual who has suffered damage

Claim for damages based on breach of contractual provisions

For example, a business partner enters into a business alliance agreement with Company A and discloses confidential information (technical information, customer information, etc.) to Company A. If the aforementioned confidential information is stolen as a result of a cyberattack by a foreign hacker on Company A's systems, and the business partner suffers damages thereby, the business partner may file a claim for damages against Company A based on the breach of contractual provisions (i.e., breach of obligations to safeguard and protect confidential information of the business partner, obligations for secure management of information, etc.).

Under the Civil Code of Japan, to establish breach of contract, one must prove:

- the fact that there was a default by a party;
- the reasons for which the defaulting party is to be held responsible; and
- the damage caused (Article 415 of the Civil Code).

The extent of damages that can be claimed will depend on the limitation on the compensation for damages agreed to by both the parties in the contract. However, in the absence of such a limitation clause, in addition to ordinary damages, special damages that could have been foreseen at the time of the default are also covered under the Civil Code (Article 416, Paragraph 2).

Therefore, in addition to the damages arising from the theft of technical information, in the event that the amount of sales of the products using such technical information falls, Company A will be liable to compensate the business partner for the decrease in sales as special damages.

Claim for damages based on tort

For example, if a company has an individual's personal information stolen and there is no contractual relationship between the individual and the company, the individual may file a claim under tortious liability against the company.

The facts required for claiming damages based on tort are: intention and negligence; illegality (infringement); damage; and causality (Article 709 of the Civil Code).

Unlike in the United States, one cannot claim for punitive damages in Japan.

Suit instituted by a company's shareholders against directors and officers

If a company suffers damages as a result of a cyberattack due to insufficient cybersecurity systems being put in place to protect confidential data, shareholders may institute a derivative suit against the company's directors and officers for breach of their duty of care.

At present, there have been no cases of shareholders' lawsuits being instituted for damages owing to failure to provide cybersecurity systems in Japan. However, with regard to theft of personal information, the Benesse Group experienced a personal information leak: an employee of a business operator entrusted with the management of personal information of customers illegally acquired or sold personal information. A shareholder lawsuit was instituted against the director of a holding company of the Benesse Group, for compensation of ¥26 billion.

Rejecting the appellant request of the shareholders, the appeals court found that:

- the Benesse Group had established various rules such as the Business Corporation Management Rules and, based on these, conducted a certain level of business management through participation in personnel affairs and business planning; risk assessment and examination of the group as a whole; reading of various reports, etc., to ensure compliance with laws and regulations; and established and operated an internal control system as a group of companies; and
- there was no proof that, considering the current practice of domestic listed companies at the time of this case, the establishment and operation of the Benesse Group's internal control system was below the standard.[11]

As can be seen from the above trial case, the establishment of a system to protect personal information or to promote cybersecurity constitutes a part of the duties of directors to establish and operate internal control systems (Article 348, Paragraph 3, Item 4 of the Companies Act).

The three principles and the 10 important items set forth in the Cybersecurity Management Guidelines represent a specific model of the philosophy and measures of the internal control system to be established in relation to a cybersecurity system. To prevent directors from being sued for violation of their managerial obligation of due care, it is necessary to establish and check the cybersecurity system of the company, and to establish a system that does not fall below the standard of current practice as mentioned above, especially pertaining to the above three principles and the 10 important items.

Types of threats or threat actors: criminal, nation-state, insider (intentional and accidental)

Criminals (hackers), the state and insiders are considered to be the main actors who conduct cyberattacks.

Offender

In Japan, criminals engage in illegal information access or theft of company assets through methods such as malware attacks, ransomware attacks, denial of service, distributed denial

11 Appeal court decision by the Okayama branch of the Hiroshima High Court, 18 October 2019.

of service, phishing emails, business e-mail fraud and unauthorised access or alteration of websites.

In 2015, the terminals of employees of the Japan Annuity Payments Organization were illegally accessed by means of sending an e-mail with a virus from outside, targeting the organisation; 1.25 million people's personal information (basic pension number, name, date of birth, address) were leaked.

Nation

In the *Coincheck* incident, about ¥58 billion worth of virtual currency NEM was stolen in January 2018. The *Coincheck* incident was carried out by an overseas hacker. Coincheck put the 'private key' used for transactions, such as remittance of virtual currency, in a hot wallet connected to the internet (a wallet disconnected from the internet is called a cold wallet). The private key was allegedly stolen by an outside hacker through the internet, and a large number of NEMs were stolen. The NEM Foundation, in cooperation with engineers, placed tracking mosaics on the stolen NEM wallets, keeping them under constant surveillance to prevent perpetrators from converting the stolen NEMs into other currencies. However, even with this tracking method, if the perpetrator exchanged the NEMs for another currency in the highly anonymous network called the Dark Web, identification of the perpetrator who stole the NEMs would be extremely difficult.

Insiders

Damages incurred by a company may be caused by intentional fraud or human error of the insider. Typical examples of insider fraudulent activities are as follows:

- employees send important information to personal addresses with email attachments;
- employees use apps installed on company leased smartphones to connect to the company's computer and take confidential information outside using Wi-Fi;
- removal or exchange of confidential information by a system administrator;
- leakage of customer information by an outsourced employee;
- removal or exchange of confidential information by a homeworker;
- removal of confidential information by retirees; and
- actions that are not intentional, for example, when leakage of personal information is caused due to human error such as inadvertent erroneous transmission of emails.

Damages suffered by a company due to fraud by insiders include the loss of customer information, business information and technical information that the company manages as its trade secret; economic loss resulting from liability for damages to customers; and reputational damage resulting from loss of credibility as a company.

Recent trends in types of cyberthreat, detection time, etc.

Because hacking from overseas was raised as a possibility with regard to the *Coincheck* incident (see above), administrative supervision and legislation in Japan alone cannot adequately deal with such an incident. The Financial Stability Board, which comprises financial supervisory authorities in major countries, created a contact list to help local authorities in charge of virtual currency administration in each country to understand their responsibilities. In

addition, if any cybercrime actually occurs, a system must be established to identify the culprit through international cooperation among investigative authorities and engineers in each country, and to investigate and recover assets outside Japan.

Appendix 1

About the Authors

Nameir Abbas
Ropes & Gray LLP

Nameir Abbas is an associate in the data, privacy and cybersecurity practice in Ropes & Gray's Washington, DC office. Nameir focuses his practice on complex data protection matters. His diverse practice includes counseling clients across a range of industries on issues relating to privacy compliance, cybersecurity preparedness, data breach response and due diligence.

Kevin Angle
Ropes & Gray LLP

Kevin Angle is counsel in the data, privacy & cybersecurity group, based in Ropes & Gray's Boston office. He represents a broad range of companies on privacy and cybersecurity matters, guiding clients through the existing patchwork of US federal and state laws as well as the European Union's comprehensive General Data Protection Regulation (GDPR) and other international privacy and cybersecurity laws. Kevin advises clients on privacy and cybersecurity matters arising in corporate transactions. He also assists clients in responding to data breach incidents, helping clients in assessing their legal obligations following a breach and in responding to regulatory authorities and others.

Richard Batchelder, Jr
Ropes & Gray LLP

Partner Richard D Batchelder, Jr has advised Ropes & Gray clients for 30 years in a wide range of high stakes litigation matters before courts throughout the country. In recent years, Richard has handled a number of significant contractual and indemnification disputes for life sciences and healthcare clients of the firm. He has advised many of the firm's private equity clients and their portfolio companies in numerous capacities, such as analysing litigation risk in proposed transactions, representing them in court post-acquisition, and in bankruptcy-related litigation. In addition, Richard actively participates in the data, privacy

and cybersecurity group, helping clients respond to incidents and defending them in any related proceedings. Richard's experience in this area includes defending TJX and Target in class action lawsuits brought by financial institutions in the wake of two of the largest data breaches in US history.

Andrew Beckett
Kroll, a division of Duff & Phelps

Andrew Beckett is a managing director and regional leader in Kroll's cyber risk practice. Before joining Kroll, Andrew served as head of Cyber Defense for Airbus Defense and Space. His prior service was with the United Kingdom's Government Communications Headquarters and the UN's Organization for the Prohibition of Chemical Weapons, where he was head of the Office of Confidentiality and Security. He is a visiting professor of cybersecurity at the University of South Wales.

Benjamin Berringer
Clifford Chance US LLP

Benjamin Berringer is an associate in Clifford Chance's litigation and dispute resolution group. He represents clients in cross-border investigations and complex commercial litigation, including class actions. In addition to his litigation practice, Benjamin also regularly advises on regulatory matters arising under US privacy and data protection laws, including risk mitigation strategies, data breach notification, planning and prevention, and data breach response.

Gina L Bertolini
K&L Gates LLP

Gina Bertolini concentrates her practice exclusively on health law, primarily representing academic medical centres and health systems. She counsels senior leadership on a variety of governance, operational and regulatory matters, including the Health Insurance Portability and Accountability Act (HIPAA) and other federal and state privacy, security and EHI interoperability laws and regulations. Gina has assisted multiple academic medical centre and health system clients with HIPAA breach reporting and investigations, and has managed response, reporting and investigation of healthcare ransomware attacks. Gina also assists hospital and health system clients with health information technology requirements, including the Office of the National Coordinator for Health IT's Information Blocking Final Rule. Gina advises on issues related to risk management, electronic medical records, credentialing, informed consent, release of sensitive records, treatment of minors and other patient relations issues.

Danielle Bogaards
Ropes & Gray LLP

Danielle Bogaards is an associate in the litigation and enforcement group in Ropes & Gray's San Francisco office. She focuses her practice on complex commercial litigation, government investigations and data privacy matters. Danielle's diverse practice, spanning an array of litigation and regulatory matters, includes disputes involving securities, employment, corporate

governance, compliance and commercial issues. As a participant in the data, privacy and cybersecurity practice group, Danielle assists clients respond to data security incidents and counsels clients on major data privacy and security laws and regulations, including the California Consumer Privacy Act.

Alan Brill
Kroll, a division of Duff & Phelps

Alan Brill is a senior managing director and founder of Kroll's technology and cyber risk practice. Prior to joining Kroll, he was Director at the New York City Department of Investigation and a deputy inspector general in the New York City government. He was employed by Chase Manhattan Bank and Ernst & Young, and, in government, with the NASA Manned Spacecraft Center, Houston, on the Apollo moon landing project, and served as a major in the US Army. He is an adjunct professor at Texas A&M University School of Law.

Jason C Chipman
Wilmer Cutler Pickering Hale and Dorr LLP

Jason Chipman is widely recognised as a national leader in handling complex regulatory matters associated with data security, cyber incident response, the Committee on Foreign Investment in the United States (CFIUS) and related export controls.

Mr Chipman has advised companies in nearly every sector of the economy on data security best practices and incident response, and because of his experience he is frequently asked to assist with corporate due diligence for transactions involving complex data security and privacy issues. He has helped companies large and small to navigate regulatory obligations associated with data security incidents in the United States, Europe and Asia. Mr Chipman is co-editor of *Getting the Deal Through: Cybersecurity*, a global cybersecurity guide, and he frequently speaks to groups about cyber preparedness and related issues.

Mr Chipman is a visiting fellow at the National Security Institute.

Anne Conroy
Ropes & Gray LLP

Anne E Conroy is an associate in Ropes & Gray's litigation and enforcement practice group in New York. Anne's practice focuses on complex commercial litigation, shareholder disputes, regulatory matters, and civil and criminal government enforcement matters. She has represented clients in matters involving securities laws, shareholder actions, and general commercial disputes.

Moriah Daugherty
Covington & Burling LLP

Moriah Daugherty advises clients on a broad range of cybersecurity, data privacy and national security matters, including government and internal investigations, regulatory inquiries, litigation, and compliance with state and federal privacy laws.

As part of her cybersecurity practice, Ms Daugherty specialises in assisting clients in responding to cybersecurity incidents, including matters involving advanced persistent threats targeting sensitive intellectual property and personally identifiable information. Ms Daugherty also assists clients in evaluating existing security controls and practices, assessing information security policies, and preparing for cyber and data security incidents.

As part of her litigation and investigations practice, Ms Daugherty leverages her government experience to advise clients on national security and law enforcement-related compliance issues, internal investigations and response to government enquiries.

Richard DeNatale
Jones Day

Richard DeNatale is a partner at Jones Day in the insurance recovery group. He is one of the world's leading lawyers in the field of cyber insurance and data breach coverage. He has been retained to handle insurance claims for more than 75 cyberattacks and data breach incidents, including some of the largest in history, and has helped clients recover hundreds of millions of dollars under cyber policies.

Rich has served as lead counsel for policyholders in landmark coverage cases on data breach and privacy issues. He frequently works with clients during the underwriting process to strengthen insurance programmes for cyber risk. Additionally, Rich has 25 years' experience in advising corporate policyholders on a wide range of insurance claims and litigation, throughout the United States and in Europe and Asia. He is a veteran trial lawyer who has tried more than 15 cases and won jury verdicts on coverage and bad faith claims. Rich has been named by *Chambers* in its US rankings of the top insurance coverage lawyers for the past 10 years. He has represented clients in London insurance arbitrations and has been retained as an expert witness on US insurance law.

Michael Drury
BCL Solicitors LLP

Michael Drury's expertise in data collection and surveillance matters by state entities is unparalleled in the United Kingdom. As a former director of legal affairs at GCHQ, the largest of the UK's security and intelligence agencies, for 14 years; founder member of the Serious Fraud Office; and for the last 10 years a partner in BCL providing advice on national security and criminal investigations to both corporate and individual clients, his breadth of experience both in terms of developing legislation (particularly the Regulatory Investigatory Powers Act as the forerunner to the current Investigatory Powers Act 2016) and practical casework gives him unique insights into how the law has developed and the practical consequences that follow. He has already provided advice on the US–UK Bilateral Data Sharing Agreement due to commence this autumn and brings his breadth of knowledge to bear on what is a new departure in a field that is inherently controversial.

Ryan Fayhee
Hughes Hubbard & Reed

Ryan Fayhee leads the sanctions, export controls and anti-money laundering practice group at Hughes Hubbard. Prior to private practice, Ryan served for 11 years in the DOJ, where he was a leading prosecutor handling complex investigations and prosecutions affecting the national security and foreign policy of the United States. He also previously served as the National Export Control Coordinator, the principal DOJ attorney overseeing sanctions and export control prosecutions nationally. Ryan represents companies, boards of directors, audit committees and senior executives in internal and government-facing cross-border investigations and advises clients on compliance and acquisition due diligence with a focus on sanctions, export controls, anti-money laundering, anti-corruption and cybersecurity. Ryan has significant experience assisting multinational companies facing crises and other high-profile reputational risks. Ryan is also an experienced trial lawyer and regularly represents clients in federal court and before the DOJ, federal law enforcement authorities, and trade regulators at the Office of Foreign Assets Control, the Bureau of Industry and Security and the Directorate of Defense Trade Controls.

Ashden Fein
Covington & Burling LLP

Ashden Fein advises clients on cybersecurity and national security matters, including crisis management and incident response, risk management and governance, government and internal investigations, and regulatory compliance.

As part of his cybersecurity practice, Mr Fein counsels clients on preparing for and responding to cyber-based attacks, assessing security controls and practices for the protection of data and systems, developing and implementing cybersecurity risk management and governance programmes, and complying with federal and state regulatory requirements. Mr Fein frequently supports clients as the lead investigator and crisis manager for global cybersecurity and data security incidents, including data breaches involving personal data, advanced persistent threats targeting intellectual property across industries, state-sponsored theft of sensitive US government information and destructive attacks. Additionally, Mr Fein assists clients from across industries with leading internal investigations and responding to government inquiries relating to US national security. He also advises aerospace, defence and intelligence contractors on security compliance under US national security laws and regulations including, among others, the National Industrial Security Program (NISPOM), US government cybersecurity regulations and requirements relating to supply chain security.

Before joining Covington, Mr Fein served on active duty in the US Army as a Military Intelligence officer and prosecutor specialising in cybercrime and national security investigations and prosecutions, including serving as the lead trial attorney in the prosecution of Private Chelsea (Bradley) Manning for the unlawful disclosure of classified information to Wikileaks. He currently serves as a Judge Advocate in the US Army Reserves.

Megan Gordon
Clifford Chance US LLP

Megan Gordon is a partner in Clifford Chance's US regulatory/white collar group focusing on regulatory, data privacy and cybersecurity-related matters and investigations. Megan co-heads Clifford Chance's US cybersecurity and data privacy group and is a leading member of the firm's global tech group. Her work encompasses a broad range of regulatory matters, including in relation to privacy and US data protection laws and regulations. Megan also has experience advising financial institutions and fintech companies on the use of artificial intelligence and big data in various products.

Tyler Grove
Hughes Hubbard & Reed

Tyler Grove is an associate in the Washington, DC office of Hughes Hubbard & Reed. As a member of the firm's sanctions, export controls and anti-money laundering group, Tyler advises domestic and international clients on all facets of compliance and enforcement, including cybersecurity and ransomware best practices. Tyler also advises on economic trade sanctions, export controls and anti-money laundering matters; filings with the Committee on Foreign Investment in the United States; and investigating and drafting complex voluntary disclosures submitted to the Commerce, State, and Treasury departments. Tyler also has experience representing clients in complex litigation, fact investigation and discovery in various government-facing matters, including those involving professional liability, securities, antitrust and trade issues.

Julian Hayes
BCL Solicitors LLP

Julian Hayes advises companies and individuals in the rapidly developing field of data protection, especially in the context of data breaches and law enforcement investigations, where necessary litigating to ensure that the actions of state authorities are properly constrained. A partner at BCL for four years, he has vast experience of all types of criminal inquiries, including the unlawful obtaining of data and computer misuse offences. He is well-known and highly regarded commentator on cybersecurity and privacy issues. He advises telecommunications operators on their obligations under UK investigatory powers legislation and provides practical guidance on how to handle demands placed upon them, including in establishing systems that work to ensure legal compliance and protection for the operator. He has advised in relation to US–UK Bilateral Data Sharing Agreement and forthcoming UK online harms legislation.

David C Lashway
Baker McKenzie

David Lashway is the co-chair of the global cybersecurity practice and a member of the management committee for the Washington, DC, office of Baker McKenzie. He focuses his practice in the areas of cybersecurity, crisis management, internal investigations and complex criminal, civil and administrative litigation. He advises the Fortune 100 on the full life cycle

of enterprise risks associated with information security, including before, during and after a network breach, and routinely handles federal regulatory and criminal and civil cybersecurity matters. He leads global investigations around the theft or compromise of confidential data and trade secrets, including serving as lead counsel to the cyber investigation firm in the hack of the 2016 US Presidential Election. He is a frequent speaker, listed in *Chambers*, as a Leading Lawyer by *The Legal 500* and named in the *Washingtonian* magazine as a Top Lawyer for crisis management and cybersecurity. He was awarded *Corporate Counsel Magazine*'s 2017 Gold Winner for Cyber/Privacy Counsel in its annual Best of Corporate Counsel rankings based on a survey of more than 1,500 corporate counsel and BTI recently listed his team as best at cybersecurity among all leading law firms. He is also included in the Cyber Incident Response 30 Best Lawyers 2018. Mr Lashway participates in the Yale Cyber Leadership Forum, is a member of the editorial board for LexisNexis' Privacy and Cybersecurity Law Reporter, and serves on the US Chamber of Commerce Cybersecurity Council. He is active with the Atlantic Council, the New York Cyber Task Force at Columbia University, the cyber working group at the Massachusetts Institute of Technology, and serves on the board of several not-for-profit organisations.

John H Lawrence
K&L Gates LLP

John Lawrence primarily counsels healthcare clients in responding to governmental investigations and defending False Claims Act lawsuits. He has represented both individuals and companies in investigations involving the Department of Justice, US Attorneys' Offices, and other federal and state agencies. His background also includes significant experience handling complex civil litigation inside and outside of healthcare. In addition to his litigation practice, John advises clients on healthcare regulatory matters, including those involving the Stark Law and Anti-Kickback Statute.

Michael Liftik
Quinn Emanuel Urquhart & Sullivan, LLP

Michael Liftik is a partner at Quinn Emanuel Urquhart & Sullivan, LLP in Washington, DC. His practice focuses on government and internal investigations, regulatory enforcement defence, cybersecurity, securities litigation and cryptocurrencies. Michael spent nearly a decade at the Securities and Exchange Commission (SEC), where he developed a unique depth of knowledge working on enforcement and regulatory matters at all levels of the Commission. Michael has represented clients in significant data breaches, including Congressional inquiries, SEC and other regulatory investigations, and private litigation. Michael has significant experience in crisis management and public affairs response to sensitive and high-profile matters.

Prior to joining the firm, Michael was the Deputy Chief of Staff of the SEC, where he served as a senior legal adviser to Chair Mary Jo White on all aspects of the SEC's operations, including enforcement, regulatory policy, compliance exams, and agency strategy and direction. He was also responsible for assisting the Chair in developing the agency's policies on cybersecurity disclosure and data protection for registered entities and public companies.

Before serving in the Chair's Office, Michael served in other capacities in the Enforcement Division at the SEC and began his career in private practice.

Yan Luo
Covington & Burling LLP

Yan Luo advises clients on a broad array of regulatory matters in connection with international trade, cybersecurity, and antitrust and competition laws in the United States, the European Union and China.

With previous work experience in Washington, DC, and Brussels before relocating to Beijing, Ms Luo has fostered her government and regulatory skills in all three capitals. She is able to strategically advise international companies on Chinese regulatory matters and represent Chinese companies in regulatory reviews in other markets.

Prior to joining the firm, Ms Luo completed an internship with the Office of International Affairs of the US Federal Trade Commission in Washington, DC. Her experience in Brussels includes representing major Chinese companies and the Chinese government in trade, competition and public procurement matters before the European Commission and national authorities in EU Member States.

Ms Luo is a Certified Information Privacy Professional (CIPP/Asia) by the International Association of Privacy Professionals and an active member of the American Bar Association's Section of Antitrust Law.

Brian McDonald
Jones Day

Brian McDonald is a partner at Jones Day in the insurance recovery group. He represents policyholders in major coverage disputes and has helped clients secure hundreds of millions of dollars in insurance recoveries for extraordinary losses. He also advises clients on the design, negotiation and purchase of insurance programmes. Brian counsels policyholders relating to a broad array of insurance lines, including cyber insurance, directors and officers liability, commercial general liability, employment practices liability, property and business interruption, errors and omissions, environmental, and umbrella/excess insurance.

Brian has represented policyholders in litigation and negotiations on a broad range of insurance claims, including coverage for cyber liability, securities class actions, derivative actions, complex commercial lawsuits, employee class actions, asbestos bodily injury and other toxic tort claims, product liability claims, environmental hazards and property damage claims.

Edward Machin
Ropes & Gray LLP

Edward Machin is an associate in the data, privacy and cybersecurity group, based in Ropes & Gray's London office. He provides clear and business-focused advice on a wide range of legal and regulatory issues in the rapidly evolving areas of privacy, data protection and security, e-commerce and marketing, and information law. Secondments at data-rich businesses in the life sciences and market research sectors have given Edward a deep understanding of what

clients want – and these experiences inform his approach to providing practical legal and commercial solutions to organisations across Europe, the United States and Asia.

Edward's practice encompasses regulatory compliance, advisory and transactional work for founders, start-ups, corporates, venture capitalists and asset managers across the technology, life sciences and healthcare, financial and professional services, food and beverage, consumer goods, entertainment and media sectors. He regularly advises on the development and operationalisation of global compliance programmes, new products and services, complex international data transfer issues, and emerging technologies and regulatory trends (such as the use of alternative data and covid-19-related compliance).

Rohan Massey

Ropes & Gray LLP

Rohan Massey is a leader of Ropes & Gray's data, privacy and cybersecurity practice and focuses his practice on data protection, data security, e-commerce, and IT. As well as advising on complex global data protection and security compliance programmes, Rohan also advises on issues of risk and value in relation to data and intellectual property in corporate transactions. Rohan's expertise focuses on the intersection of the extra-territorial scope of national data protection laws and data transfer issues for multinational organisations. Rohan has advised on a number of leading breach data management cases, and has assisted clients in successfully obtaining BCR approval from EU regulators. His industry-focused expertise covers asset management and financial services; life sciences and clinical trials; as well as media, sponsorship, advertising, sales promotions; and intellectual property issues, marketing issues in the sports apparel and food and drink sectors. His client base is international in scope, as he works extensively across Europe, the United States and Asia.

Kirk Nahra

Wilmer Cutler Pickering Hale and Dorr LLP

Kirk Nahra is a partner at WilmerHale. He has been a leading authority on privacy and cybersecurity matters for more than two decades. He is the winner of the 2021 Vanguard Award from the International Association of Privacy Professionals. Mr Nahra counsels clients across industries, from Fortune 500 companies to startups, on implementing the requirements of privacy and data security laws across the country and internationally. He also advocates for clients experiencing privacy and security breaches, and represents clients in contract and deal matters, enforcement actions, regulatory investigations and related litigation. Mr Nahra is best known for his work with health insurers, hospitals, service providers, pharmaceutical manufacturers and other healthcare industry participants. He has a deep understanding of the privacy and security issues healthcare companies face relating to HIPAA rules, state and federal legislation, enforcement activities, internal investigations, international principles, due diligence in transactions, data breach risk assessments and the key lines between regulated and unregulated data.

Mr Nahra also has substantial experience working with clients in the financial services and insurance industries on privacy and data security matters relating to the Gramm-Leach-Bliley Act, Fair Credit Reporting Act, Fair and Accurate Credit Transactions Act, data aggregation and sharing practices, and privacy and data security compliance under a wide range

of state and federal laws. He is an adjunct professor at the Washington College of Law at American University where he teaches courses in information privacy law and healthcare privacy and security law.

Takashi Nakazaki
Anderson Mori & Tomotsune

Takashi Nakazaki is a special counsel at Anderson Mori & Tomotsune in the IP and technology group, with broad experience in the areas of data protection, privacy, big data and IoT. He has been engaged in various cybersecurity and AI-related matters including crisis management due to cyberattacks. In addition, he regularly assists the Japanese government in cyber law and data protection areas, including the 'AI & Data Contracts Guidelines' and 'AI Governance'. Mr Nakazaki leads the technology law committee of the International Bar Association as vice chair.

Atsushi Nishitani
Anderson Mori & Tomotsune

As a partner at Anderson Mori & Tomotsune, Atsushi is in charge of crisis management and corporate matters for the firm and its clients, including cross-border cases, since he has considerable experience in advising clients in Tokyo and New York at one of the largest Japanese trading corporations. Among other things, he actively engages in various types of fraud investigations and asset tracing and recovery, including cyberattacks, financial fraud and quality-test fraud.

Evan Norris
Cravath, Swaine & Moore LLP

Evan Mehran Norris is a partner in Cravath, Swaine & Moore LLP's litigation department and a member of the investigations and regulatory enforcement practice and data security and privacy practice. He focuses on advising US and multinational companies, board members and senior executives with respect to government and internal investigations, criminal defence, regulatory compliance and related civil litigation, with particular emphasis on cross-border, multijurisdictional investigations. Mr Norris has represented clients across numerous industries in a variety of sensitive matters concerning the FCPA, corporate fraud, trade sanctions, cyber incidents, data privacy, anti-money laundering controls and securities fraud. Prior to joining Cravath, Mr Norris served for 10 years as a federal prosecutor in the US Attorney's Office for the Eastern District of New York. He was the lead prosecutor of the groundbreaking *FIFA* case, spearheading a global investigation of corruption in international soccer in one of the most far-reaching cross-border corruption cases ever brought by the DOJ. Mr Norris also served as Chief of the National Security and Cybercrime Section, in which role he was responsible for conducting and supervising matters ranging from ransomware attacks, international data breaches and corporate insider cyberattacks to counterterrorism, counterintelligence and export control cases.

Benjamin A Powell
Wilmer Cutler Pickering Hale and Dorr LLP

Benjamin Powell is a partner at WilmerHale and co-chair of the firm's cybersecurity and privacy practice. He is widely recognised as one of the country's top authorities on handling cybersecurity, data breach and related investigation matters. He has advised companies on major cybersecurity incidents and incident preparedness across virtually every sector of the economy, including banking, investment management, software, retail, energy, defence and intelligence, media and entertainment, pharmaceutical, cloud services, government contracting, aerospace, information technology, manufacturing and travel.

Mr Powell was unanimously confirmed by the United States Senate as General Counsel to the Director of National Intelligence. His background includes serving as General Counsel to the first three Directors of National Intelligence, as Special Assistant to the President and associate White House Counsel and as a United States Air Force officer, and working at the Federal Bureau of Investigation, as corporate counsel at a software company in Silicon Valley and as part of the trial team that obtained the largest antitrust jury verdict in US history. He also is regularly asked to be lead counsel on major investigations and strategic counselling in a variety of sensitive regulatory matters for the world's most prominent companies.

Sara Ramsey
Ropes & Gray LLP

Sara Ramsey is an associate in the litigation and enforcement group in Ropes & Gray's San Francisco office. At the University of California, Berkeley, School of Law, Sara served as the symposium editor for the Berkeley Law Journal of Employment and Labor Law. Sara also successfully advocated for clients in the Workers' Rights Clinic and Community Economic Justice Clinic.

David C Rybicki
K&L Gates LLP

David Rybicki is a partner at K&L Gates and a member of the firm's investigations, enforcement, and white collar practice group in Washington, DC, where he advises clients on cybersecurity, regulatory compliance and criminal enforcement matters. He recently served in the criminal division of the US Department of Justice as Acting Principal Deputy Assistant Attorney General and Deputy Assistant Attorney General, the second- and third-highest ranking positions in the division. In these roles he led the investigation, prosecution, and coordination of nationally significant matters and initiatives involving transnational organised cybercrime, healthcare fraud, corporate fraud, the Foreign Corrupt Practices Act and public corruption. He previously served as a federal prosecutor in Washington, DC, and as chief counsel on the US Senate Committee on the Judiciary.

Daniel Silver
Clifford Chance US LLP

Daniel Silver is a partner in Clifford Chance's litigation and dispute resolution group. He previously spent 10 years as a federal prosecutor, serving in several senior leadership positions

and as Chief of the National Security and Cybercrime Section within the United States Attorney's Office for the Eastern District of New York. Daniel co-heads the firm's US cybersecurity and data privacy group. He regularly counsels clients on risk mitigation strategies with respect to cybersecurity and data privacy, including incident response, data breach notification, planning and prevention, interfacing with regulators and law enforcement agencies, and related civil disputes.

Jason Smolanoff

Kroll, a division of Duff & Phelps

Jason Smolanoff is a senior managing director and Kroll's global cyber risk practice leader. Jason has more than 19 years of experience in federal law enforcement and information security and has played a leading role in some of the most significant cybersecurity investigations in history. During his career, he has specialised in supervising and investigating sophisticated computer and network intrusions conducted by state-sponsored organised crime, hacktivists and insider threat actors, often developing and maintaining productive partnerships with international intelligence and law enforcement agencies as well as private industry.

Jason directs Kroll's global team dealing with cyber risk in both preventing incidents through risk management and dealing with incidents when they occur.

Jason served with the Federal Bureau of Investigation from 1999 to 2011. He was the Supervisory Special Agent for the Cyber National Security Squad, supervising special agents and intelligence analysts in responses to all aspects of complex national cybersecurity investigations with a nexus to counterintelligence and counterterrorism matters.

From 2010 to 2011, Jason was the lead mentor of the Organized Crime Unit, Major Crimes Task Force, in Kabul, Afghanistan. This role required significant liaison with numerous Coalition, Afghan and Intelligence Community partners from the United States, United Kingdom, France and Australia, as well as Afghan prosecutors and judges.

Richard J Stark

Cravath, Swaine & Moore LLP

Richard J Stark is a partner in Cravath, Swaine & Moore LLP's litigation department. Mr Stark is recognised as a leading litigator in complex business litigation and has particular expertise in software, computer systems, microelectronics and standard-setting organisations, as well as deep litigation experience in the pharmaceuticals industry. He has a master's degree in Computer Science (machine learning) and is a registered patent attorney. He has represented clients across a range of industries, including technology, life sciences and banking. Spanning nearly three decades, his broad litigation practice and expertise encompasses multifaceted and multijurisdictional business disputes in the realm of intellectual property, antitrust, securities and general commercial litigation, as well as arbitration. Mr Stark's clients have included Qualcomm, Alarm.com, Blue Yonder, IBM, Xerox, Bristol-Myers Squibb, Sanofi-Synthelabo, GlaxoSmithKline, Mylan Laboratories, Illumina and Credit Suisse. In the federal system, Mr Stark is admitted to practise before the US Supreme Court, the Federal Circuit, the DC Circuit, the Second, Third, Seventh and Ninth Circuits, the Southern and Eastern Districts of New York, the Northern, Southern and Central Districts of California, and the District of DC (among others).

Kristin S Starr

Kristin Starr was formerly an associate at Quinn Emanuel Urquhart & Sullivan, LLP. Her practice focused on civil litigation and government investigations. Ms Starr graduated from Washington & Lee School of Law in 2014, and clerked for the Hon Mary L Cooper on the US District Court for the District of New Jersey.

David M Stuart

Cravath, Swaine & Moore LLP

David M Stuart is a partner in Cravath, Swaine & Moore LLP's litigation department. Mr Stuart represents and advises public and private companies, executives and board members in their most sensitive and complex civil, criminal and internal investigations and related securities and derivative litigation. His matters regularly involve allegations of accounting fraud, foreign corruption, insider trading, market manipulation, money laundering, trade sanctions, illicit cyber activity and sexual harassment. He has also conducted comprehensive reviews of corporate compliance programmes and advised organisations on implementation of best practices in regulatory compliance. He participates in the firm's efforts related to blockchain and financial technology (fintech). From 2000 to 2006, Mr Stuart served in the Division of Enforcement at the Securities and Exchange Commission in Washington, DC. While at the SEC, he supervised a team in the SEC's Financial Fraud Task Force and regularly coordinated multinational investigations with the FBI, the DOJ, and multiple international regulators and law enforcement agencies. For this work, he twice received the Director's Award for outstanding contribution to the enforcement of the federal securities laws. After leaving the SEC, Mr Stuart served as senior counsel of investigations and regulatory affairs for the General Electric Company before returning to Cravath.

Raffi Teperdjian

Ropes & Gray LLP

Raffi Teperdjian is an associate in the intellectual property litigation group at Ropes & Gray's Washington, DC office. Raffi's legal work includes the intersection of blockchain and emerging technologies with intellectual property, financial technology, data privacy and cybersecurity. He has published articles on the regulation of blockchain by the EU's GDPR, proposing options for United States cybersecurity regulation of smart contracts, and studying the national security implications of cryptocurrency financing. Prior to, and concurrently with, his study of the law, Raffi worked on a variety of systems development and big data analysis projects in both federal and commercial information technology consulting.

John W Woods, Jr

Baker McKenzie

John Woods, Jr is the co-chair of the global cybersecurity practice and is a partner based in Washington, DC. During the past 15 years, he has received recognition or ranking in *The Legal 500*, *Chambers Global* and *Chambers USA* guides, *Washingtonian* magazine, *Corporate Counsel* magazine and *BTI Consulting Group.* In that time, Mr Woods has led the investigative and legal response to some of the largest and most complex cybersecurity incidents and

compliance challenges. This has included overseeing the investigation into network intrusions, representing clients in post-incident disputes, and coordinating response activities with law enforcement and other government agencies. He focuses in particular on advising on the legal and compliance issues associated with pre-incident cyber resilience projects, data integrity attacks and operationally impactful malware incidents.

Daisuke Yamaguchi
Anderson Mori & Tomotsune

Daisuke Yamaguchi is a partner at Anderson Mori & Tomotsune in the corporate group. He has been engaged in various cybersecurity and AI-related matters including crisis management regarding cyberattacks, as well as various corporate matters. He is also in charge of the firm's information technology and services and legal-tech, and is a member of CSIRT.

Brian Yin
Clifford Chance US LLP

Brian Yin is an associate in Clifford Chance's litigation and dispute resolution group. He represents clients in cybersecurity and data privacy matters as well as cross-border criminal and regulatory investigations. His experience includes advising a diverse array of US clients on their compliance obligations with respect to the General Data Protection Regulation (GDPR) and US state and federal data privacy and cybersecurity requirements. This includes drafting and revising compliance policies and procedures and advising on new product launches. He also advises companies on data privacy and cybersecurity issues in multinational transactions.

Zhijing Yu
Covington & Burling LLP

Zhijing Yu is an associate in the firm's Beijing office. His practice focuses on advising major multinationals and Chinese companies on a broad array of complex matters in connection with data privacy, cybersecurity, international trade and corporate transactions. Mr Yu has represented leading companies in multiple industries, including consumer products, banking and financial services, entertainment, healthcare, internet services and pharmaceuticals.

Appendix 2

Contributors' Contact Details

Anderson Mori & Tomotsune
Otemachi Park Building
1-1-1 Otemachi
Chiyoda-ku
Tokyo 100-8136
Japan
Tel: +81 3 6775 1000
atsushi.nishitani@amt-law.com
daisuke.yamaguchi@amt-law.com
takashi.nakazaki@amt-law.com
www.amt-law.com

Baker McKenzie
815 Connecticut Avenue NW
Washington, DC 20006
United States
Tel: +1 202 452 7000
Fax: +1 202 452 7074
david.lashway@bakermckenzie.com
john.woods@bakermckenzie.com
www.bakermckenzie.com

BCL Solicitors LLP
51 Lincoln's Inn Fields
Holborn
London WC2A 3LZ
United Kingdom
Tel: +44 (0)20 7430 2277
jhayes@bcl.com
mdrury@bcl.com
www.bcl.com

Clifford Chance US LLP
31 West 52nd Street
New York, NY 10019-6131
United States
Tel: +1 212 878 8000
Fax: +1 212 878 8375
megan.gordon@cliffordchance.com
daniel.silver@cliffordchance.com
benjamin.berringer@cliffordchance.com
brian.yin@cliffordchance.com
www.cliffordchance.com

Covington & Burling LLP
2301 Tower C Yintai Centre
2 Jianguomenwai Avenue
Chaoyang District
Beijing 100022
China
Tel: +86 10 5910 0591
yluo@cov.com
zyu@cov.com

One CityCenter
850 Tenth Street, NW
Washington, DC 20001-4956
United States
Tel: +1 202 662 6000
afein@cov.com
mdaugherty@cov.com

www.cov.com

Cravath, Swaine & Moore LLP
825 Eighth Avenue
New York, NY 10019
United States
Tel: +1 212 474 1000
dstuart@cravath.com
enorris@cravath.com
rstark@cravath.com
www.cravath.com

Hughes Hubbard & Reed
1775 I Street, NW
Washington, DC 20006-2401
Tel: +1 202 721 4600
Fax: +1 202 721 4646
ryan.fayhee@hugheshubbard.com
tyler.grove@hugheshubbard.com
www.hugheshubbard.com

Jones Day
555 California Street 26th Floor
San Francisco, CA 94104
United States
Tel: +1 415 626 3939
Fax: +1 415 875 5700
bdmcdonald@jonesday.com
rdenatale@jonesday.com
www.jonesday.com

K&L Gates LLP
1601 K Street, NW
Washington, DC 20006
United States
Tel: +1 202 778 9000
david.rybicki@klgates.com

430 Davis Drive, Suite 400
Morrisville, NC 27560
United States
Tel: +1 919 466 1190
gina.bertolini@klgates.com
john.lawrence@klgates.com

www.klgates.com

Kroll, a division of Duff & Phelps
The Shard
32 London Bridge Street
London SE1 9SG
United Kingdom
Tel: +44 20 7029 5000
andrew.beckett@kroll.com

Kroll Associates, Inc
10100 Santa Monica Boulevard
Suite 1100
Los Angeles, CA 90067
United States
Tel: +1 424 249 1650
jason.smolanoff@kroll.com

Kroll Associates, Inc
2 Emerson Lane, Suite 200
Secaucus, NJ 07094
United States
Tel: +1 877 300 6816
abrill@kroll.com

www.kroll.com

Quinn Emanuel Urquhart & Sullivan, LLP
1300 I Street, NW
Suite 900
Washington, DC 20005
United States
Tel: +1 202 538 8000
Fax: +1 202 538 8100
michaelliftik@quinnemanuel.com
www.quinnemanuel.com

Ropes & Gray LLP
60 Ludgate Hill
London EC4M 7AW
United Kingdom
Tel: +44 20 3201 1500
Fax: +44 20 3201 1501
rohan.massey@ropesgray.com
edward.machin@ropesgray.com

Prudential Tower
800 Boylston Street
Boston, MA 02199
United States
Tel: +1 617 951 7000
Tel: +1 617 951 7050
richard.batchelder@ropesgray.com
kevin.angle@ropesgray.com

1211 Avenue of the Americas
New York, NY 10036-8704
United States
Tel: +1 212 596 9000
Fax: +1 212 596 9090
anne.conroy@ropesgray.com
Three Embarcadero Center
San Francisco, CA 94111-4006
Tel: +1 415 315 6300
Fax: +1 415 315 6350
danielle.bogaards@ropesgray.com
sara.ramsey@ropesgray.com

2099 Pennsylvania Avenue, NW
Washington, DC 20006-6807
United States
Tel: +1 202 508 4600
Fax: +1 202 508 4650
nameir.abbas@ropesgray.com
raffi.teperdjian@ropesgray.com

www.ropesgray.com

Wilmer Cutler Pickering Hale and Dorr LLP
1875 Pennsylvania Avenue, NW
Washington, DC 20006
United States
Tel: +1 202 663 6000
Fax: +1 202 663 6363
benjamin.powell@wilmerhale.com
jason.chipman@wilmerhale.com
kirk.nahra@wilmerhale.com
www.wilmerhale.com

Data breaches and similar incidents pose a unique challenge – those targeted must both respond and investigate simultaneously. It is an art that is impossible without preparation.

Businesses wishing to prepare will find this volume, *The Guide to Cyber Investigations*, invaluable. It identifies every issue to consider when creating a response template and implementing it, giving both the law and plenty of practical and tactical advice.

Written by leading contributors, all with broad experience of serious data incidents, it is an indispensable desktop guide and a worthy companion to GIR's larger volume on cross-border investigations, *The Practitioner's Guide to Global Investigations*.

Visit globalinvestigationsreview.com
Follow @giralerts on Twitter
Find us on LinkedIn

an LBR business

ISBN 978-1-83862-595-5