THE CYBER INVESTIGATIONS GUIDE

THIRD EDITION

Editors
Benjamin Powell and Shannon Togawa Mercer

The Cyber Investigations Guide

Third Edition

Editors

Benjamin A Powell

Shannon Togawa Mercer

Published in the United Kingdom by Law Business Research Ltd
Holborn Gate, 330 High Holborn, London, WC1V 7QT, UK

www.globalinvestigationsreview.com

Enquiries concerning reproduction should be sent to: insight@globalinvestigationsreview.com.
Enquiries concerning editorial content should be directed to the Publisher –
david.samuels@lbresearch.com

ISBN 978-1-80449-253-6

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

Acknowledgements

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

Anderson Mōri & Tomotsune

BCL Solicitors LLP

Clifford Chance US LLP

Cravath, Swaine & Moore LLP

Jones Day

K&L Gates LLP

Nyman Gibson Miralis

Ropes & Gray LLP

Wilmer Cutler Pickering Hale and Dorr LLP

Publisher's Note

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

It aims to fill a gap in the literature by providing 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 seventh 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 Cyber Investigations Guide 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 Cyber Investigations Guide* as the close-up.

The Cyber Investigations Guide 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.

David Samuels
Publisher
May 2023

Introduction: Preventing, Mitigating and Responding to Data Breaches

Benjamin A Powell and Shannon Togawa Mercer[1]

Today, it is almost impossible to read the news 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 the then director of the Federal Bureau of Investigation, 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 Mandiant's M-Trends 2022 report, cyber criminals continue to conduct advanced ransomware and cyber extortion attacks at a higher pace, including through increased targeting of virtualisation environments.[3]

---

1 Benjamin A Powell is a partner and Shannon Togawa Mercer is a senior associate at Wilmer Cutler Pickering Hale and Dorr LLP.

2 Kroll, 'Global Fraud and Risk Report 2019/20' (www.kroll.com/en/insights/publications/global-fraud-and-risk-report-2019 (last accessed 11 April 2023)).

3 Mandiant Services, 'M-Trends 2022: Insights into Top Cyber Trends and Attacks' (19 April 2022) (https://www.mandiant.com/resources/reports/m-trends-2022-insights-todays-top-cyber-trends-and-attacks(last accessed 11 April 2023)).

As data breaches and ransomware events increase in frequency and sophistication, boards of directors, management, employees, customers and regulators across the globe continue to increase 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 information technology (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 are likely to need to:

- conduct internal investigations;
- engage external specialists, including law firms, forensic investigators and public relations experts;
- implement crisis management or incident response 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 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 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 security controls and make informed strategic decisions to balance risk minimisation with operational needs.

---

4 See, e.g., 12 CFR Appendix B to Part 30, Section III.C (requiring national banks and federal savings associations in the United States 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, Article 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 (last accessed 11 April 2023)) (noting that financial institutions should '[e]stablish and maintain a cybersecurity strategy and framework tailored to specific cyber risks').

Although 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 publication 'Protecting Personal Information: A Guide for Business', '[e]ffective 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). Taking 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, financially motivated 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

5 US Federal Trade Commission (FTC), 'Protecting Personal Information: A Guide for Business' (October 2016), 2 (www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last accessed 11 April 2023)). Although 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 7) – its guidance is nonetheless helpful in identifying foundational security practices for the protection of sensitive information more broadly.

6 ibid., at 3–5.

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.

Although described in the context of cyber due diligence, the guidance provided in Chapter 4 for preparing for diligence and scoping of potential risk areas can be helpful for a company conducting its own internal risk assessment as well.

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;

---

7 FTC, 'Start with Security: A Guide for Business' (June 2015) (www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last accessed 11 April 2023)).

8 As at the end of 2020, the FTC has brought approximately 80 cases against companies that have engaged in unfair or deceptive practices involving inadequate protection of consumers' personal data, and more than 130 spam and spyware cases. 'FTC Report to Congress on Privacy and Security' (13 September 2021) (https://www.ftc.gov/system/files/documents/reports/ftc-report-congress-privacy-security/report_to_congress_on_privacy_and_data_security_2021.pdf (last accessed 11 April 2023)).

- 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 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] And while ransomware has been the most frequently observed type of cyberattack for at least the past three years, according to IBM's 2022 X-Force Threat Intelligence Index annual report, the top infection vectors in 2021 included phishing (41 per cent of incidents observed by X-Force) and vulnerability exploitation (34 per cent of incidents observed by X-Force).[13] An

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 (last accessed 11 April 2023)).

10 IBM Security, 'X-Force Threat Intelligence Index' (2019) (https://www.securindex.com/downloads/8b9f94c46a70c60b229b04609c07acff.pdf (last accessed 11 April 2023)).

11 Verizon, '2018 Payment Security Report' (https://www.verizon.com/business/resources/reports/payment-security/2018/ (last accessed 11 April 2023)).

12 id.

13 IBM Security, 'X-Force Threat Intelligence Index 2022' (https://www.ibm.com/downloads/cas/ADLMYLAZ (last accessed 11 April 2023)).

appropriate proactive security plan should include, among many other useful elements, cybersecurity awareness training and a method for identifying and patching known vulnerabilities.

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 such 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.