GDR INSIGHT

HANDBOOK 2020

HANDBOOK
2020

Reproduced with permission from Law Business Research Ltd
This article was first published in November 2019
For further information please contact Natalie.Clarke@lbresearch.com

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

www.globaldatareview.com

To subscribe please contact subscriptions@globaldatareview.com

ISBN: 978-1-83862-235-0

Printed and distributed by Encompass Print Solutions
Tel: 0844 2480 112

CONTENTS

Privacy

Cybersecurity

Data in Practice

PREFACE

Global Data Review is delighted to publish this inaugural edition of the *GDR Insight Handbook*.

The handbook delivers specialist intelligence and research to our readers – general counsel, government agencies and private practitioners – who must navigate the world's increasingly complex framework of legislation that affects how businesses handle their data.

The book's comprehensive format provides in-depth analysis of the global developments in key areas of data law and their implications for multinational businesses. Experts from across Europe, the Americas and Asia consider the latest trends in privacy and cybersecurity. Attention is also given to new legislation in the United States that regulates the use of artificial intelligence, and strict data localisation rules emerging in jurisdictions such as China. The handbook provides practical guidance on the implications for companies wishing to buy or sell data sets, and the intersection of privacy, data and antitrust. A chapter is dedicated to assessing how companies should respond to the GDPR enforcement regime.

In preparing this report, Global Data Review has worked with leading data lawyers and consultancy experts from around the world and we are grateful for all their cooperation and insight.

The information listed is correct as at October 2019. Although every effort has been made to ensure that all the matters of concern to readers are covered, data law is a complex and fast-changing field of practice, and therefore specific legal advice should always be sought. Subscribers to Global Data Review will receive regular updates on any changes to relevant laws over the coming year.

We would like to thank all those who have worked on the research and production of this publication.

Global Data Review
London
October 2019

PART 2

Cybersecurity

UNITED STATES: CYBERSECURITY

Avi Gesser, Matthew J Bacal, Matthew A Kelly, Daniel F Forester, Clara Y Kim and Gianna C Walton
Davis Polk & Wardwell LLP

Overview of key laws

Regulation of cybersecurity in the United States is fragmented, with requirements varying based on the nature of a company's business, location or customer base. At the federal level, a complex web of agencies oversee a patchwork of cybersecurity rules and requirements for companies doing business in the United States. At the state level, all of the states have data breach notification laws and a slight majority of states also have affirmative cybersecurity and data security regulations, with a mix of enforcement bodies. Examples of such regulations are discussed below.

Federal Laws Related to Cybersecurity

Gramm-Leach-Bliley Act

Under the Gramm-Leach-Bliley Act (GLBA) (also known as the Financial Modernization Act of 1999), financial institutions must appropriately safeguard non-public personal information of consumers and customers, each as defined in the GLBA. Broker-dealers and investment advisers must establish written policies and procedures 'reasonably designed' to protect the security and confidentiality of customer information and safeguard against potential threats to such information, as well as to prevent unauthorised access to, or use of, such information.[1] The Federal Trade Commission (FTC), federal bank agencies and other regulatory authorities may enforce the GLBA depending upon the type of covered entity and the applicable rule.

Health Insurance Portability and Accountability Act

The Health Insurance Portability and Accountability Act (HIPAA) requires health plans, healthcare clearing houses and healthcare providers, as well as certain business associates of such covered entities, to use reasonable technical, administrative, and physical safeguards to

1 17 CFR section 248.30(a).

protect the security and confidentiality of protected health information.[2] Protected health information includes individually identifiable health information transmitted or maintained electronically or in any other form or medium.[3] Covered entities must establish written security policies and procedures, as well as perform regular risk analysis.[4] In addition, if a security breach has occurred that involves unsecured personal health information, the covered entity must notify the affected individuals, the Secretary of the Department of Health and Human Services (HHS), and the media if said breach involves more than 500 people in a certain jurisdiction, within a certain time frame.[5] HIPAA is enforced by the HHS Office for Civil Rights.

Federal Trade Commission

Section 5 of the Federal Trade Commission Act prohibits 'unfair and deceptive acts or practices' by entities with respect to, among other things, their treatment of consumers' personal information.[6] The FTC has brought enforcement actions under section 5 against companies for insufficiently protecting consumer personal data or falsely claiming adequate cybersecurity protections were in place. Additionally, the FTC has published various guidance containing best practices for safeguarding information as well as insight into its historical enforcement actions in the cybersecurity context.

Securities and Exchange Commission

Under the Securities Act of 1933 and the Securities Exchange Act of 1934, public companies are required to consider the materiality of cybersecurity to their operations and make any necessary cybersecurity disclosures in registration statements and reports. The Security and Exchange Commission (SEC)'s February 2018 Statement and Guidance on Public Companies Cybersecurity Disclosure provides insight into such requirements, stating that companies should report, among other things, material cyber incidents that have previously occurred, the 'probability' and 'magnitude' of potential cyber incidents, and whether the company has the capability to prevent or remediate cyber incidents.[7] Additionally, among other rules, Rule 201 of Regulation S-ID requires certain financial institutions and creditors to create and put in place written programmes to prevent identity theft, including policies and procedures targeting identity theft stemming from cybersecurity events,[8] and under section 13(b)(2)(B)

2 45 CFR sections 164.306, 308, 310, 312.

3 45 CFR section 160.103.

4 45 CFR section 164.308.

5 45 CFR sections 164.404, 406, 408.

6 15 USC section 45.

7 SEC Commission Statement and Guidance on Public Company Cybersecurity Disclosures, 83 Fed. Reg. 8166 (26 February 2018) (to be codified at 17 CFR Parts 229, 249), https://www.govinfo.gov/content/pkg/FR-2018-02-26/pdf/2018-03858.pdf.

8 17 CFR section 248.201.

of the Securities Exchange Act of 1934,[9] certain public companies must create and put in place internal accounting controls that reasonably protect the company from cybersecurity fraud. The SEC enforces such cybersecurity disclosure requirements through enforcement actions.

Other

Federal Information Security Modernization Act of 2014

The Federal Information Security Management Act of 2002 (FISMA), replaced by FISMA 2014, requires federal government agencies and contractors to create and put in place cybersecurity programmes.[10] In response to FISMA, the National Institute of Standards and Technology (NIST) of the United Statess Department of Commerce published guidance on minimum security requirements.

Cybersecurity Information Sharing Act of 2015

The Cybersecurity Information Sharing Act (CISA)'s objective is to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats. CISA allows companies to share information with federal law enforcement about cybersecurity attacks without waiving privilege.[11] Additionally, under CISA, private companies are permitted to monitor their own information systems, or the information systems of another entity with consent, for purposes of cybersecurity.[12]

State laws related to cybersecurity

In the absence of an overarching federal law governing cybersecurity in the United States, state governments regulate data and cybersecurity. All states have their own data breach notification laws, but not every state has data governance or cybersecurity requirements. The states also vary in their definitions of personally identifying information, but most cover some combination of first name or first initial with last name of an individual, in conjunction social security number, driver's licence number, financial number or medical information. Notification triggers vary by state and, in terms of the form of notification to individuals, most state statutes require that notices be made in writing and sent via US mail, including information on the estimated date of breach, a description of the personally identifiable information acquired by an unauthorised person as part of the breach, steps the company is taking to restore security and confidentiality of the information after the breach, and the company's contact information for more information.

9 15 USC section 78m.
10 44 USC section 3554.
11 6 USC section 1504.
12 6 USC section 1503.

Variation across state laws

Notification triggers

The states vary in terms of what exactly triggers a company's notification obligation. Although all states require notification at some point after a breach occurs once the company discovers or knows of the breach, the specific language used to describe the trigger for the notification varies. The language used includes notification upon 'discovery or notification' of a breach, when the company 'becomes aware' of the breach, 'knows' about the breach, 'knows or has reason to know' about the breach, or simply 'discovers' the breach. In the majority of states, notification obligations are triggered by some combination of the company's 'discovery or notification' of a breach ('discovering or being notified', 'discovery or notification', or 'discovers or is notified').

Risk of harm

In a majority of states, a determination of a breach alone does not trigger notification to affected individuals. Rather, most states further require companies to perform a 'risk of harm' analysis before determining whether notification of the breach is required. While the language of the statutes varies, a risk of harm provision generally provides that notification of a breach is not required if a covered entity or service provider determines after an investigation that the breach is not reasonably likely to cause harm or result in substantial economic loss to affected individuals.

Notification to entities

Some states require an additional notification to the state's attorney general, normally triggered when the breach affects more than a certain number of residents of that state. Many states require notification to the attorney general where more than 1,000 individuals are affected by the data breach, though the exact number varies. Some states also require notification to consumer reporting agencies in the event of a breach.

Although each state's breach notification triggers differ, the laws of California, Massachusetts, New York and Texas provide representative examples.

California

California's data breach notification statute does not include a risk of harm threshold. Instead, if a company has a reasonable belief that an unauthorised person has acquired California residents' personal information, then the company must provide notification to them in 'the most expedient time possible and without unreasonable delay'.[13] Personal information includes an individual's name in combination with a sensitive data element (such as a social security number or a driver's licence number), as well as a username or email address in

13 Cal Civ Code section 1798.82(a), (g).

combination with a password or security question and answer that would permit access to an online account.[14] If more than 500 California residents are affected by a breach, companies are also required to notify the California Attorney General.

Massachusetts

Massachusetts's data breach notification statute does not include a risk of harm threshold. It requires notification as soon as practicable and without unreasonable delay once a company has reason to know that the personal information of a Massachusetts resident was acquired or used for an unauthorised purpose.[15] Personal information includes a resident's name in combination with a sensitive data element (such as a social security number or a driver's license number).[16] If notification is required to individuals, companies are also required to notify the Massachusetts Attorney General and the Director of Consumer Affairs and Business Regulation.[17]

New York

Until 2019, the New York breach notification law did not include a risk of harm threshold. Notification to individuals was required if identifying information, in combination with a sensitive data element (such as a social security number or a driver's license number), was acquired by someone without authorisation.[18] In these circumstances, notification was also required to the New York Attorney General.[19] The deadline for notification to individuals was in 'the most expedient time possible and without unreasonable delay'.[20]

These notification obligations were amended by the Stop Hacks and Improve Electronic Data Security (SHIELD) Act, which added a risk of harm threshold for notification.[21] The SHIELD Act expands the kinds of personal information that triggers a notification obligation to include identifying information in conjunction with account numbers usable to access financial accounts or biometric data, as well as a username or email address in combination with a password or security question and answer that would permit access to an online account.[22] It also provides that unauthorised access (ie, the mere viewing, rather than the

14 Cal Civ Code section 1798.82(h).
15 Mass Gen Laws Chapter 93H section 3(b).
16 Mass Gen Laws Chapter 93H section 1(a).
17 Mass Gen Laws Chapter 93H section 3(b).
18 NY Gen Bus Law section 899-aa(1), (2).
19 NY Gen Bus Law section 899-aa(8)(a).
20 NY Gen Bus Law section 899-aa(2).
21 Stop Hacks and Improve Electronic Data Security Act, S. 133 section 3(2)(a), Reg Sess (NY 2019), https://legislation.nysenate.gov/pdf/bills/2019/S133.
22 Stop Hacks and Improve Electronic Data Security Act, S. 133 section 3(1)(a), (b), Reg Sess (NY 2019), https://legislation.nysenate.gov/pdf/bills/2019/S133.

acquisition) of personal data triggers notification.[23] In addition, if the data breach incident involves over 500 New York residents, companies must notify the New York Attorney General within 10 days of such determination.[24]

Texas

Texas's data breach notification statute does not include a risk of harm threshold. Companies are required to notify state residents as quickly as possible when the company has a reasonable belief that there has been an unauthorised acquisition of computerised data that compromises the security, confidentiality or integrity of sensitive personal information.[25] Personal information includes an individual's name in combination with a sensitive data element (such as a social security number or driver's licence number), or information that identifies an individual and relates to the physical or mental health or condition of the individual.[26] There is no obligation to notify the Texas Attorney General or other state regulators under Texas law.

Recent amendments to the Texas breach notification law will take effect on 1 January 2020 and provide that notification must be provided no later than 60 days after a determination that a breach has occurred, and must also be provided to the Attorney General of Texas if the breach involves the personal data of 250 or more Texas residents.

Broadly applicable state laws

As noted above, every state has a data breach notification law, but not all have substantive cybersecurity requirements for the governance of data. Currently, 29 states have requirements for the security of data collected.[27] Most of these states require that companies maintain some variation of 'reasonable security measures' to secure personally identifying information.

Some states have more specific or robust requirements. For example, the Massachusetts statute governing security breaches specifically provides that the 'department of consumer affairs and business regulation shall adopt regulations relative to any person that owns or licenses personal information about a resident of the commonwealth.'[28] As such, anyone who owns or licenses personal information about a resident of Massachusetts is subject to 201 CMR 17.00, the Standards for the Protection of Personal Information of Residents of

23 Stop Hacks and Improve Electronic Data Security Act, S. 133 section 3(1)(c), Reg Sess (NY 2019), https://legislation.nysenate.gov/pdf/bills/2019/S133.

24 Stop Hacks and Improve Electronic Data Security Act, S. 133 section 3(2)(a), Reg Sess (NY 2019), https://legislation.nysenate.gov/pdf/bills/2019/S133.

25 Tex Bus and Com Code Ann section 521.053(a), (b).

26 Tex Bus and Com Code Ann section 521.002(a)(2).

27 Data Security Laws: State Government, Nat'l Conf of St Legs (22 February 2019) http://www.ncsl.org/research/telecommunications-and-information-technology/data-security-laws-state-government.aspx.

28 Mass Gen Laws. Chapter 93H section 2(a), https://malegislature.gov/laws/generallaws/parti/titlexv/chapter93h/section2.

the Commonwealth.[29] These standards designate the specific components of each entity's required comprehensive information security programme, computer system security and other requirements.

The New York SHIELD Act, for which the data security requirements will go into effect on 21 March 2020, imposes specific cybersecurity requirements upon entities in New York.[30] The act mandates that entities implement a data security programme that includes: the designation of one or more employees to coordinate the security programme for the entity; the identification of reasonably foreseeable internal and external risks; the training and management of employees in the security programme practices and procedures; the selection of service providers capable of maintaining appropriate safeguards and a requirement that these safeguards are delineated by contract; and regular testing and monitoring of the effectiveness of key controls, systems, and procedures; among many other specific security requirements.

And, while some states do not have specific cybersecurity requirements, other factors may encourage entities regulated under these laws to maintain strong cybersecurity measures. The California Consumer Privacy Act (CCPA), which will come into effect on 1 January 2020, is one prominent example. The CCPA does not delineate specific cybersecurity requirements beyond the general language included in many state laws, but the strength of an entity's cybersecurity measures could serve as a defence against the private right of action created under the CCPA for California consumers that have experienced a cyber breach of their personal information by an unauthorised person. A successful action requires that the withdrawal or disclosure be of unencrypted personal data and result from the company's violation of its duty to implement and maintain reasonable security procedures and practices.[31]

Industry-specific state laws

New York Department of Financial Services

Some states have specific cybersecurity requirements for certain industries. For example, in the state of New York, companies operating under licence, registration, charter, certificate, permit, accreditation, or similar authorisation under the Banking Law, the Insurance Law or the Financial Services Law, are subject to the New York Department of Financial Services (NYDFS) Regulation 23 NYCRR 500.[32] NYDFS requires that companies that are subject to this regulation comply with certain cybersecurity requirements, and requires that a senior officer or the board chairperson annually certify compliance with the regulations.

29 201 CMR 17.00: Standards for the Protection of Personal Information of Residents of the Commonwealth, https://www.mass.gov/files/documents/2017/10/02/201cmr17.pdf (last accessed 4 September 2019).

30 Stop Hacks and Improve Electronic Data Security Act, S. 133, Reg. Sess. (NY 2019), https://legislation.nysenate.gov/pdf/bills/2019/S133.

31 California Consumer Privacy Act of 2018, S. 1121, Chapter 735 (23 September 2018), https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB1121; section 1798.150(a)(1).

32 Cybersecurity Requirements for Financial Services Companies, NY Comp. Codes R. & Regs. Title 23, section 500, https://www.dfs.ny.gov/docs/legal/regulations/adoptions/dfsrf500txt.pdf.

Companies regulated under NYDFS must notify the Superintendent of Financial Services of any cybersecurity event that requires notice to be provided to any other government body, self-regulatory agency, or supervisory body; or created a reasonable likelihood of materially harming any part of the company's normal operation. Companies must submit this notice to the superintendent as promptly as possible, but in all cases within 72 hours of determination that a relevant cybersecurity event has occurred.[33]

The regulation also requires that companies implement and maintain a cybersecurity programme that is designed to protect each company's information systems, based on each company's risk assessment. The cybersecurity programme must be designed to perform certain core cybersecurity functions, which include identification and assessments of internal and external cybersecurity risks; use of defensive infrastructure to protect non-public information; detection of cybersecurity events; responding to detected cybersecurity events to mitigate any negative effects; recovering from cybersecurity events and restoring normal operations and services; and fulfilling applicable regulatory reporting obligations.[34]

The regulation also requires that companies maintain cybersecurity policies that are approved by a senior officer of the board of directors; that are based on the company's risk assessment; and that address information security, data governance and classification, asset inventory and device management, access controls and identity management, and business controls and identity management, among others.[35]

Companies are also required to have a written incident response plan that is designed to ensure prompt response to, and recovery from, any cybersecurity event that materially affects the confidentiality, integrity or availability of a company's information systems.[36]

Insurance laws

The National Association of Insurance Commissioners (NAIC) promulgated the Insurance Security Model Law (the Model Law),[37] which a number of states have used to model their own rules regarding data breach notification requirements for insurers. Under the Model Law, any cybersecurity event – defined as 'an event resulting in unauthorized access to, disruption or misuse of, an Information System or information stored on such Information System' – triggers a 72-hour notification requirement. In practice, this requires entities to conduct a prompt investigation upon discovery of a potential cybersecurity event. That investigation must include determining whether a cybersecurity event has occurred, assessing the nature and scope of the event, and identifying any non-public information that may have been involved. Many of the states that have adopted data breach notification laws specific to the insurance industry have used the Model Law as a template for their own regulations.

33 NY Comp Codes R & Regs Title 23, section 500.17.
34 NY Comp Codes R & Regs Title 23, section 500.02.
35 NY Comp Codes R & Regs Title 23, section 500.03.
36 NY Comp Codes R & Regs Title 23, section 500.16.
37 Insurance Data Security Model Law (2017), https://www.naic.org/store/free/MDL-668.pdf.

Other industries

Vermont Data Broker Act

Some states have specific cybersecurity requirements for other sectors as well. Vermont, for instance, has regulations specific to data brokers. Data brokers are businesses or units of a business that knowingly collect and sell or license to third parties brokered personal information of a consumer with whom the business does not have a direct relationship.[38]

The law requires data brokers to register with Vermont's secretary of state, establish an information security programme that meets enumerated criteria, and provide consumers the ability to opt out of data collection. The law also requires data brokers to report certain information annually, including 'the number of data broker security breaches that data broker has experienced during the prior year, and if known, the total number of consumers affected by the breaches'. The law defines a data broker security breach as an 'unauthorized acquisition or a reasonable belief of an unauthorized acquisition of more than one element of brokered personal information', by an unauthorised person, where the data is not encrypted, redacted, or rendered unreadable or unusable by some other method.

Colorado Securities Act

Another state with industry-specific cybersecurity requirements is Colorado, where broker-dealers are required to establish and maintain written procedures 'reasonably designed' to ensure the cybersecurity of 'Confidential Personal Information'.[39] The regulation further provides that, to the extent possible, the cybersecurity procedures should provide for an annual assessment that covers: the potential risks and vulnerabilities to the confidentiality, integrity, and availability of personal information; the use of secure email for email containing personal information, including use of encryption and digital signatures; authentication practices for employee access to electronic communications, databases and media; procedures for authenticating client instructions received via electronic communication; and disclosure to clients of the risks for using electronic communications.[40]

Obligations for protecting IT systems and data from cyberthreats

As indicated at the outset of this chapter, the United States does not have a comprehensive regulatory regime prescribing minimum physical, administrative and technical protections that companies must take to defend their IT systems and data from cyberthreats. Instead, the

38 Data Brokers, Vt Sec'y of State, https://www.sec.state.vt.us/corporationsbusiness-services/data-brokers.aspx (last accessed 4 September 2019).

39 'Confidential Personal Information' is defined as first name or first initial and last name in combination with any one or more of the following: social security number; driver's licence number; account number or credit or debit card number, in combination with any required security or access code; individual's digitised or other electronic signature; or user name, unique identifier or electronic mail address in combination with a password or access code. Securities Laws & Rules, Colo Dep't of Reg Agencies, https://www.colorado.gov/pacific/dora/securities-law-rules.

40 Securities Laws & Rules, Colo Dep't of Reg Agencies, https://www.colorado.gov/pacific/dora/securities-law-rules.

cyber defence obligations of any individual company will typically be the combined product of a range of private contractual duties and regulatory responsibilities, including those established by the kinds of rules and regulations described above.

Still, despite the number and variety of sources, reasonableness remains the most common benchmark for cybersecurity governance and compliance in the United States. Indeed, with rare exceptions, the substantial majority of US companies are – at a minimum – subject to some form of statute, rule or regulation requiring them to demonstrate 'reasonableness' in at least some aspects of the design and implementation of their cybersecurity and information security defences.

Reasonableness remains something of an elusive standard, however – one that is generally understood to permit varying levels of protection based on the unique circumstances, capabilities and risk profiles of a particular company. Expectations as to what constitute reasonable protections also evolve over time – responding to changes in threat profiles, technological innovation, and customer concerns.

US companies wishing to limit legal risk will, therefore, often be required to look to cybersecurity frameworks, published best practices, industry standards, available regulatory guidance, as well as the outcomes of prior enforcement actions to gauge their own efforts. Perhaps counterintuitively, regimes based on reasonableness may also end up inheriting and reinforcing rules-based regimes that may not otherwise apply to a particular company's activities and operations. One prominent example of a rules-based regime that may significantly impact expectations as to reasonableness is the NYDFS cybersecurity rules, which are described further above.

Looking across various US regulations, one can identify a degree of coalescence around certain elements of security programmes that are likely to be considered 'reasonable'. These elements include:

- encryption of personal, financial, sensitive or otherwise valuable information;
- multifactor authentication for login and remote access;
- restricted access controls with minimum necessary user privileges (ie, granting employees access only to those files, functions, networks and applications that are actually necessary to achieve their business goals);
- employee training (eg, on phishing, social engineering and information security hygiene).
- vendor management and oversight;
- patch management and software update procedures;
- testing and vulnerability assessments;
- network monitoring for unauthorised activity by internal users and/or from external sources; and
- carefully crafted policies and procedures related to data security, use of technology, incident response, and data management.

There is, however, no comprehensive checklist or test, the completion of which would demonstrate the adequacy of corporate cybersecurity defences or insulate a company from legal risk. The list of elements above may be over- or under-inclusive when considering reasonableness in a particular corporate environment.

To this end – as the FTC and other government agencies have highlighted – a company's best evidence of having met its obligations for protection of IT systems and data may not be adoption of any particular protections or implementation of any particular technologies. Instead, a company's best evidence of reasonableness may be the records of the process undertaken. In this regard, the NIST Cybersecurity Framework endorsed by the FTC may serve as a helpful reference. The framework identifies five 'concurrent and continuous functions' – identify, protect, detect, respond and recover – that, according to the FTC, 'provide a strategic view of the life cycle of an organization's management of cybersecurity risk'. That is, they provide the outlines of a process through which a company can conduct and create a record of effective risk assessment and mitigation.

Legal considerations in preparing for and responding to cyber incidents

Minimising the legal, operational and other risks that stem from a cyber event begins with careful preparation and planning prior to the occurrence of the incident, followed by level-headed, efficient and accountable execution of incident response plans. Indeed, the planning that occurs before a cyber incident is as important to effective management and mitigation of risk as the execution of the response itself. Waiting until a cyber incident occurs to decide what steps must be taken can lead to bungled responses and significant increases in risk of civil liability and regulatory intervention. Careful consideration of issues likely to arise in the event of a cyber incident can eliminate or mitigate legal risk, as well as many of the other potentially adverse consequences of the event.

A critical output of these thoughtful preparation efforts should be a written incident response plan (IRP), which will guide the company's response when an incident occurs and which can prevent decision makers from making ill-considered choices under potentially stressful circumstances. Development and maintenance of an effective IRP is not only best practice, it is often a hallmark of a reasonable cybersecurity programme and may be required by certain regulatory regimes.[41]

While there is no prescribed format to which such materials must adhere, an IRP should set out the company's expected procedures for identifying, responding to and remediating an incident. It should provide pragmatic instructions, with a balance between real-time flexibility and the institutional need for internal accountability and consistency of approach. Because a company's response to an incident may be judged (by the press, the public and by regulators) in part by its adherence to its IRP, it is important that the IRP sets out a framework that is achievable and that has buy-in from the various stakeholders who may be involved in the actual incident response process.

41 Cybersecurity Requirements for Financial Services Companies, NY Comp. Codes R & Regs Title 23, section 500.16.

Once written, the IRP should be practiced, tested and refined through regular periodic review, tabletop exercises, and mock incident scenarios. These exercises will reveal the company's ability to navigate an incident before it happens and allow executives to hone their emergency policies, procedures and decision-making.

One of the most difficult aspects of incident response planning, with significant potential for legal liability, is determining when a particular cyber event may trigger statutory or contractual notification obligations, including requirements to notify the company's customers, regulators, insurers, auditors and vendors, as well as the market. There are now breach notification regimes in each of the 50 US states, as well as federal, international, and industry-specific notification regulations. These various regimes differ in their notification triggers, content requirements and deadlines. Companies should not wait for an actual incident to begin the process of figuring out their potential notification obligations, especially because a failure to comply can lead to regulatory and civil liability, reputational harm and the perception among regulators, the press and the public that the company's overall management of the incident was lacking.

Upon the detection of a potential incident, the response process described in the IRP should serve as the guide for action. To the extent that deviations from the written plan are necessary, rationales for those changes should be well supported and documented to avoid ex post claims of policy or procedure violations. Responsible persons should work to confirm and understand the nature of the incident – including whether the event involves an on-premise breach, past or ongoing compromise of systems or exposure of data. Based on this information, and as contemplated by the IRP, the company may elect to engage outside professionals, including outside counsel, a security or forensics consultant, or a communications or crisis management firm, as needed. Any public commentary or disclosures related to the incident should be carefully considered to maintain business secrets, and avoid possible issues related to selective disclosure.

While the company works to remediate and recover from the incident, it should keep in mind any potential data breach notification obligations that may be implicated (including contractual notice requirements), and ensure that they are satisfied. This is a critical component of effective management of the firm's legal risks in the wake of a breach, as perceptions of late notification can have a significant impact on the public and regulatory assessments of a firm's overall incident response efforts.

Finally, because company personnel who become aware of undisclosed cyber events may be in possession of material non-public information, cyber incidents may lead to heightened risk of insider trading. As highlighted by the SEC's February 2018 Statement and Guidance on Public Company Cybersecurity Disclosures,[42] companies should take steps to limit such risks in the course of executing the firm's incident response process. This can be accomplished not only by limiting dissemination of non-public information regarding the incident, but also

42 SEC Commission Statement and Guidance on Public Company Cybersecurity Disclosures, 83 Fed Reg 8166 (26 February 2018) (to be codified at 17 CFR Parts 229, 249), https://www.govinfo.gov/content/pkg/FR-2018-02-26/pdf/2018-03858.pdf.

potentially by the implementation of trading blackout restrictions or preclearance procedures for key stakeholders that are likely to become aware of material non-public cyber events. It may also be helpful – depending on the nature of the incident and the analysis needed to assess potential risks – to keep a record of parties who are brought 'in the tent' in the course of the response efforts.

Responsibilities of directors

As a general matter, directors should be informed about the types of data and information most important to their company, and the potential legal and business consequences of a compromise or loss with respect to such data the company faces. As part of the board's responsibility for oversight of the company's operations and systems, directors should be informed of the company's cybersecurity-related risks, the steps that the company has taken to address such risks (including company security policies and procedures and internal controls), and the company's plans and protocols for responding to cyber incidents. In the event of a material security breach or other incident, the board should be informed of significant developments. Boards also should consider guidance from the SEC in determining whether cybersecurity public disclosure is appropriate (as discussed above).

In addition to staying informed with respect to cybersecurity issues facing the company, board members may take affirmative action as part of their oversight authority. In board meetings, directors should ensure that sufficient time is devoted to discussing cybersecurity issues and enough data is provided with respect to such issues. Depending on the type of company, the board should consider whether any board members should have IT or cybersecurity expertise. Additionally, the board might consider either creating a cybersecurity committee or formalising cybersecurity as a responsibility of another board committee, such as the audit committee. In connection with enforcement actions, there is a growing trend toward requiring board of director certifications with respect to improved cybersecurity practices, which heightens the importance of these issues to directors serving on boards.

Private redress

Given uneven enforcement under a patchwork of regulation, a major risk that companies operating in the United States face is the threat of cyber-related civil litigation. While state attorney generals, federal regulators and other public actors can also impose penalties or otherwise hold companies accountable, companies also face significant legal risk from private actors as well.

Plaintiffs have been successful in using general consumer protection laws that generally prohibit unfair and deceptive business practices in bringing claims against companies after a breach. Section 5(a) of the FRC Act prohibits 'unfair or deceptive acts or practices in or affecting commerce'.[43] Many states have laws with similar language, and some actions have been successfully brought by alleging that failure to take proper measures to protect data

43 15 USC section 45(a)(4)(A).

could constitute an 'unfair act' under these types of statutes. Some plaintiffs have succeeded in bringing claims against companies for data breach based on simple negligence theory, arguing that companies have breached an independent legal duty of care to take reasonable measures to safeguard plaintiffs' information.

Some state statutes explicitly allow for private right of action following a cyber breach. For instance, the California Consumer Privacy Act (CCPA), when it goes into effect on 1 January 2020, will create a private right of action for California consumers against companies that have experienced a cyber breach, if their personal information has been taken by an unauthorised person resulting from the company's violation of its duty to implement and maintain reasonable security procedures and practices. Plaintiffs in CCPA cyber breach cases will likely not be required to prove harm because the law provides for statutory damages at a minimum of US$100 and a maximum of US$750 per consumer per incident. In many cases, the only viable defence to such an action will be that the company upheld its 'duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information'.[44] Proving that a company had reasonable cybersecurity measures can be difficult and costly, particularly because the CCPA does not spell out specific cybersecurity requirements.

The CCPA does provide another defence to cyber breach class actions, but it is not likely to be of much assistance to companies in most cases. Before bringing action for statutory damages, the consumer is required to provide the company with 30 days' written notice identifying the specific provision that has been violated. If the company cures the noticed violation and provides the consumer with an express written statement stating that the violations have been cured and no further violations will occur, then the consumer can no longer bring action.[45] This cure may be unavailable in many situations, such as when, for example, hackers have already taken the consumer's personal data and sold it on the dark web.

44 CCPA, section 1798.150(a)(1).

45 CCPA, section 1798.150(b).

Avi Gesser
Davis Polk & Wardwell LLP

Mr Gesser is a partner in Davis Polk's litigation department. He represents clients in a wide range of cybersecurity issues, enforcement and investigation matters, and complex commercial litigation.

As a principal member of Davis Polk's cybersecurity and data privacy practice, Mr Gesser has substantial experience advising clients on compliance with various cybersecurity regulations, enhancing cybersecurity policies, procedures, training and governance, cloud migration, and data minimisation, as well as cybersecurity risk disclosures and due diligence. He advises clients who have experienced data breaches and ransom-related cyber incidents, and has conducted internal investigations relating to cybersecurity events, such as phishing and spoofing attacks, and represented companies in related civil litigations and regulatory investigations. Mr Gesser was recently retained by a global financial services firm in connection with a sophisticated attack on their computer system, as well as several international financial institutions on complying with the New York Department of Financial Services cyber regulations. He is also a frequent commentator on cybersecurity issues and the primary author of the Davis Polk Cyber Blog.

Matthew J Bacal
Davis Polk & Wardwell LLP

Mr Bacal is counsel in Davis Polk's corporate department, practicing in the intellectual property and technology transactions group. He advises clients on intellectual property, technology, media and privacy-related issues arising from corporate and commercial transactions, such as mergers and acquisitions, licensing, development and outsourcing/services arrangements, joint ventures and collaborations, financings, restructurings and capital markets offerings.

He has a particular focus on negotiating and drafting strategic licensing, development, supply, outsourcing, services, and other commercial arrangements relating to media and sports rights, content distribution, branding, sponsorship, fashion, software and other technology. Mr Bacal also regularly counsels clients on questions of copyright, internet and data privacy law.

In his pro bono practice, Mr Bacal has provided intellectual property advice and counselling for a variety of organisations, including UNICEF, Equality Now, Probono.net, CatchLight, and Volunteer Lawyers for the Arts.

Matthew A Kelly
Davis Polk & Wardwell LLP

Mr Kelly is an associate in Davis Polk's litigation department, where he has represented clients in a variety of regulatory, white-collar, and civil litigation matters, including investigations by government agencies and self-regulatory organisations, internal investigations, shareholder derivative suits, and complex commercial and contractual disputes. A member of Davis Polk's cybersecurity and data privacy practice, Mr Kelly often advises clients on matters that present significant technological or data-driven challenges, including issues related to statistical modelling, machine learning, data governance, data privacy and cybersecurity. Mr Kelly's work has also included advising clients on remediation and enhancement of internal compliance programmes, as well as on strategic use of technology to minimise legal risk and increase efficiencies in connection with litigation and compliance matters. He is a frequent speaker and writer on matters related to data privacy and cybersecurity and is a contributor to the Davis Polk Cyber Blog.

Daniel F Forester
Davis Polk & Wardwell LLP

Mr Forester is an associate in Davis Polk's corporate department, practising in the intellectual property and technology transactions group. He advises clients on intellectual property and technology issues arising from corporate and commercial transactions, such as mergers and acquisitions, data or intellectual property licensing, development and commercialisation arrangements, joint ventures and collaborations, financings, restructurings and capital market offerings. He is also a member of the cybersecurity and data privacy group and advises clients on cybersecurity, personal data, technology and data initiatives, development of privacy and data security policies and in connection with larger strategic transactions. He writes frequently on data privacy and cybersecurity matters and is a contributor to the Davis Polk Cyber Blog.

Clara Y Kim
Davis Polk & Wardwell LLP

Ms Kim is an associate in Davis Polk's litigation department.

Gianna C Walton
Davis Polk & Wardwell LLP

Ms Walton is an associate in Davis Polk's corporate department, practicing in the intellectual property and technology transactions group.

Davis Polk

Davis Polk & Wardwell LLP (including its associated entities) is an elite global law firm with world-class practices across the board. Industry-leading companies and global financial institutions know they can rely on Davis Polk for their most challenging legal and business matters. The firm's top-flight capabilities are grounded in a distinguished history of 170 years, and its global, forward-looking focus is supported by 10 offices strategically located in the world's key financial centres and political capitals. Approximately 1,000 lawyers collaborate seamlessly across practice groups and geographies to provide clients with exceptional service, sophisticated advice and creative, practical solutions.

450 Lexington Avenue
New York, NY
10017
United States
Tel: +1 212 450 4000
Fax: +1 212 701 5800

www.davispolk.com

Avi Gesser
avi.gesser@davispolk.com

Matthew J Bacal
matthew.bacal@davispolk.com

Matthew A Kelly
matthew.kelly@davispolk.com

Daniel F Forester
daniel.forester@davispolk.com

Clara Y Kim
clara.kim@davispolk.com

Gianna C Walton
gianna.walton@davispolk.com

The GDR Insight Handbook delivers specialist intelligence and research to our readers – general counsel, government agencies and private practitioners – who must navigate the world's increasingly complex framework of data legislation. In preparing this report, Global Data Review has worked with leading data lawyers and consultancy experts from around the world.

The book's comprehensive format provides in-depth analysis of the developments in key areas of data law. Experts from across Europe, the Americas and Asia consider the latest trends in privacy and cybersecurity, providing practical guidance on the implications for companies wishing to buy or sell data sets, and the intersection of privacy, data and antitrust.

Visit globaldatareview.com
Follow @GDR_alerts on Twitter
Find us on LinkedIn

an LBR business

ISBN 978-1-83862-235-0