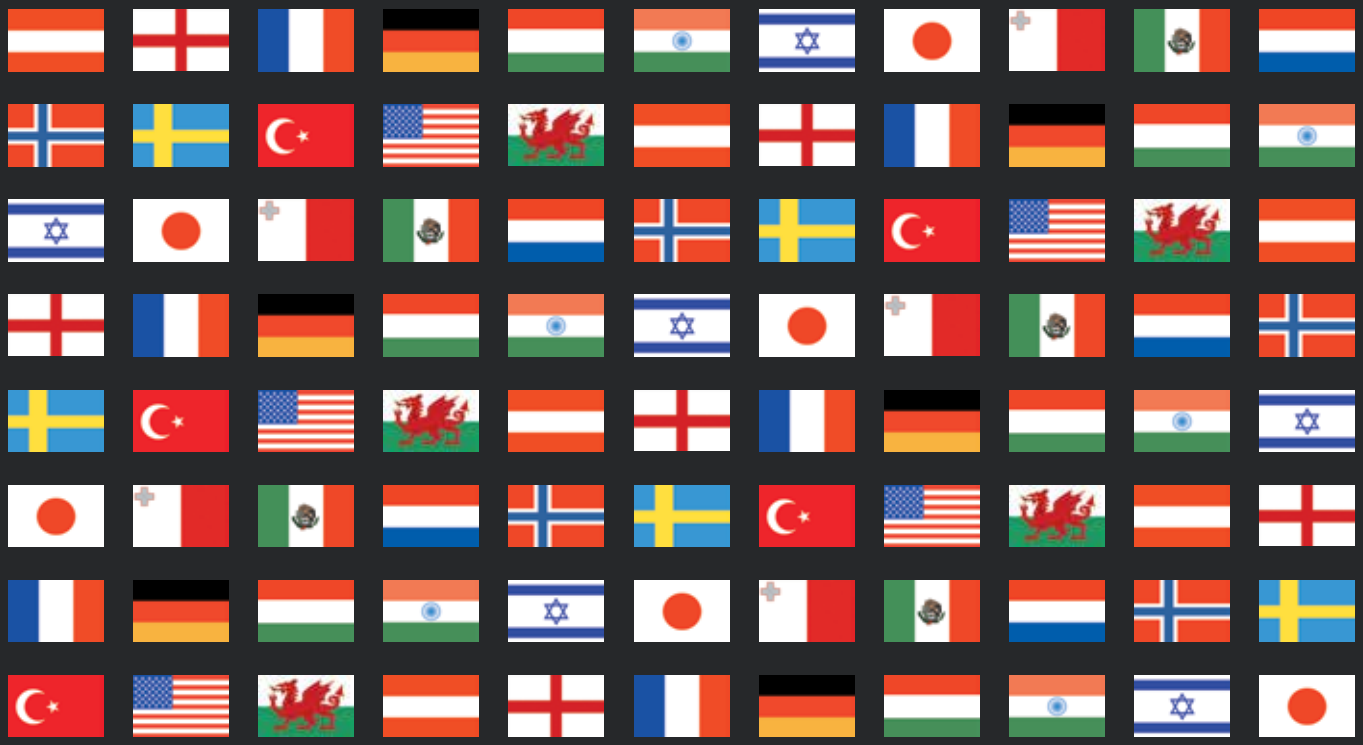
Cybersecurity

In 15 jurisdictions worldwide

Contributing editors
Benjamin A Powell and Jason C Chipman



2015

GETTING THE DEAL THROUGH

GETTING THE DEAL THROUGH

Cybersecurity 2015

Contributing editors

Benjamin A Powell and Jason C Chipman

Wilmer Cutler Pickering Hale and Dorr LLP

Publisher
Gideon Roberton
gideon.roberton@lbresearch.com

Subscriptions
Sophie Pallier
subscriptions@gettingthedealthrough.com

Business development managers
Alan Lee
alan.lee@lbresearch.com

Adam Sargent
adam.sargent@lbresearch.com

Dan White
dan.white@lbresearch.com

Law Business Research

THE QUEEN'S AWARDS FOR ENTERPRISE: 2012

Published by
Law Business Research Ltd
87 Lancaster Road
London, W11 1QQ, UK
Tel: +44 20 3708 4199
Fax: +44 20 7229 6910

First published 2015
First edition
ISSN 2056-7685

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

CONTENTS

United States

Benjamin A Powell, Jason C Chipman, Marik A String, Carla J Weiss and DeAnna Evans
Wilmer Cutler Pickering Hale and Dorr LLP

Legal framework

1 Summarise the main statutes and regulations that promote cybersecurity. Does your jurisdiction have dedicated cybersecurity laws?

Although the US has over 50 federal and state statutes implicating various aspects of the cybersecurity landscape, there are no comprehensive cybersecurity laws or regulations and there are no generally applicable cybersecurity standards. Instead, US law addresses cybersecurity through sector-specific regulations and requirements. For example, the Federal Information Security Management Act of 2002 established cybersecurity standards for federal government agencies and their contractors. Similarly, under the Gramm-Leach-Bliley Act (GLBA) and the Health Information Portability and Accountability Act, entities in the financial services and health sectors must protect customer information from unauthorised access or use. Some subject-matter specific cybersecurity standards focus narrowly on a single constituency or a single government agency. For example, the Veterans Affairs Information Security Enhancement Act, passed in 2006 as part of the Veterans Benefits, Health Care, and Information Technology Act, requires the Department of Veterans Affairs (VA) to implement agency-wide information security procedures to protect sensitive personal information held by the VA and VA information systems.

In the criminal context, the Computer Fraud and Abuse Act (CFAA) outlaws intrusions into or interference with the security of a government computer system or computers connected to the internet. In addition, several federal surveillance laws prohibit unauthorised eavesdropping on electronic communications, which can limit a variety of cybersecurity activities. For example, the Electronic Communications and Privacy Act (ECPA) prohibits unauthorised electronic eavesdropping. The Wiretap Act prevents the intentional interception, use, or disclosure of wire, oral, or electronic communication, unless an exception applies. The Stored Communications Act (SCA) precludes intentionally accessing, without authorisation, a facility through which an electronic communication service is provided and thereby obtains, alters or prevents authorised access to a wire or electronic communication while it is in electronic storage.

Beyond legal requirements mandating cybersecurity standards, many organisations are subject to voluntary standards, or are required by contract to comply with cybersecurity requirements. Of particular note, the payment card industry in the United States generally establishes its own cybersecurity standards that apply to merchants that process payment card data. The federal government has also focused substantially in recent years on the establishment of voluntary cybersecurity requirements, particularly for critical infrastructure entities, which are generally entities that provide vital services to a large part of the population. In 2013, the President of the United States issued Executive Order 13636, 'Improving Critical Infrastructure Cybersecurity' to establish a process for the government to create voluntary cybersecurity standards applicable to critical infrastructure entities.

2 Which sectors of the economy are most affected by cybersecurity laws and regulations in your jurisdiction?

In several respects, the financial services industry and the health-care sector are the most regulated sectors with regard to cybersecurity. Federal banking agencies promulgated data security guidelines in 2005 with the issuance of the 'Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice.' This guidance states that certain covered 'financial institutions have an affirmative duty to protect their customers' information against unauthorized access or use,' and that '[n]otifying customers of a security incident involving the unauthorized access or use of the customer's information [...] is a key part of that duty.' The Securities and Exchange Commission (SEC) has also issued guidance to public companies, and has articulated steps the SEC will take in the future to ensure cybersecurity preparedness in the securities sector. In the health-care sector, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires the Department of Health and Human Services (HHS) to adopt security standards to protect individually identifiable health information.

3 Has your jurisdiction adopted any international standards related to cybersecurity?

The US has not adopted any international cybersecurity standards into law. However, the National Institute of Standards and Technology has created a 'Cybersecurity Framework,' pursuant to Executive Order 13636, establishing voluntary standards applicable to critical infrastructure companies that incorporates many of these international benchmarks as examples of best practices to help US companies manage and reduce cybersecurity risks.

4 What are the obligations of responsible personnel and directors to keep informed about the adequacy of the organisation's protection of networks and data, and how may they be held responsible for inadequate cybersecurity?

All directors and officers (D&O) owe their companies the fiduciary duties of care, loyalty and good faith. Given the broad-based impact of cybersecurity threats and data breaches on business viability and reputation, D&Os can no longer expect their company's IT department to successfully manage these concerns in isolation. Instead, successful boards lead their organisations in addressing and incorporating cybersecurity concerns into all facets of business decision-making and processes.

US corporate directors are generally not required by law to have specific expertise in cybersecurity areas. D&Os are generally responsible for proactively monitoring, managing and educating themselves on risks to the company, including cybersecurity risks and trends. Boards that fail to account for cybersecurity risks to a business may leave their companies vulnerable to a variety of civil litigation claims for failure to adequately maintain cyber and data protections, and prevent unauthorised access to consumer personal and financial information. In light of the growing emphasis on managing cybersecurity concerns, an increasing number of companies in the United States hire outside experts to report to the board on cybersecurity issues on a regular basis. In addition, boards are increasingly examining board committees to ensure that there is appropriate board oversight of the company's data security and privacy procedures.

5 How does your jurisdiction define cybersecurity and cybercrime?

The US lacks consistent and clear definitions for cybersecurity and cybercrime. In general, cybercrime is defined by the CFAA as accessing a protected computer without authorisation or exceeding authorised access to such protected computer. A 'protected computer' includes computers used in interstate communication, such as computers connected to the internet. 'Cybersecurity' is generally not defined in law, although the US Department of Defense (DoD) and the General Services Administration

recently published recommendations calling for common cybersecurity definitions for federal acquisitions in order to increase efficiency and effectiveness in the public and private sector.

6 What are the minimum protective measures that organisations must implement to protect data and information technology systems from cyberthreats?

Industries vary with respect to the protective measures taken to thwart cyberthreats and data breaches. Both health-care and certain financial services industries have minimum requirements they are required to meet. However, these requirements are generally broad and do not include specific technical standards. For example, although HHS regulations identify a specific level of encryption that companies should use, companies are not required to use it. Instead, encrypting data provides a safe harbour for companies otherwise facing notice obligations in the event of a data security breach.

Merchants, payment processors, and other parties dealing in payment cards, such as credit cards, are required to comply with various technical requirements under the Payment Card Industry Data Security Standards, which are implemented via contract between parties and are not enacted into law. These standards include 12 categories of requirements that companies must meet with respect to the security of payment card information. Companies failing to comply risk fines from the payment card brands.

Apart from these mandatory standards, the National Institute of Standards and Technology's Cybersecurity Framework created in response to Executive Order 13636 catalogues best practices for identifying, protecting, detecting, responding to and recovering from cybersecurity incidents by creating adaptable benchmarks and recommendations. While these standards are explicitly not mandatory, some have suggested that widespread adoption of this Framework by companies may result in the Framework representing a new 'standard of care' for US businesses generally.

7 Does your jurisdiction have any laws or regulations that specifically address cyberthreats to intellectual property?

Both the Digital Millennium Copyright Act and the Computer Fraud and Abuse Act provide legislative safeguards against cyberthreats to US intellectual property rights, including threats arising from cyber intrusions.

In addition, the federal government has issued two strategies under President Obama to address cyberthreats to US trade secrets and intellectual property rights. The 'Strategy on Mitigating Theft of US Trade Secrets' aims to protect US trade secrets abroad, promote voluntary best practices, enhance domestic law enforcement and improve legislation. The 'Joint Strategic Plan on Intellectual Enforcement' focuses on improving transparency in intellectual property policy and rulemaking, ensuring interagency coordination and securing US rights abroad.

Several pieces of pending legislation seek to protect US intellectual property rights and trade secrets from foreign governments and allegedly government-sponsored entities involved in hacking US computers and networks.

8 Does your jurisdiction have any laws or regulations that specifically address cyberthreats to critical infrastructure or specific sectors?

Some federal agencies in the United States have promulgated standards associated with protecting critical infrastructure entities from cyber intrusions. Of particular note, the Federal Energy Regulatory Commission (FERC) has established 'Critical Infrastructure Protection Reliability Standards' to address potential vulnerabilities in the bulk-electric system. These standards require certain electricity grid 'bulk-power' system asset owners and operators to document, report and provide compliance evidence on a variety of security controls to the North American Electric Reliability Corporation (NERC) and FERC. They also require the characterisation of all cyber systems that influence the bulk-electric system as either low, medium or high impact. In addition, these standards call for responsible entities to identify, assess and correct deficiencies in their cyber policies. Additionally, under the GLBA entities in the financial services sector must protect customer information from unauthorised access or use. And the Transportation Security Administration (TSA) has statutory authority to promulgate regulations related to pipeline physical security and cybersecurity. However, the TSA has yet to issue such regulations.

The President of the United States has also issued Executive Order 13636, 'Improving Critical Infrastructure Cybersecurity' that calls for the enhancement of security measures to protect critical infrastructure. This Executive Order does not establish mandatory standards but instead requires the creation of minimum voluntary standards for the protection of critical infrastructure entities. In so doing, it attempts to balance efficiency, safety, privacy, business confidentiality and civil liberties in the cybersecurity realm. A core component of the Executive Order is a requirement that NIST create a voluntary risk-based Cybersecurity Framework, in collaboration with both private and public sector stakeholders, to establish standards and best practices for organisations dealing with cybersecurity threats within the critical infrastructure arena.

9 Does your jurisdiction have any cybersecurity laws or regulations that specifically address privacy and civil liberties?

In the US, the ECPA and the Stored Communications Act's (SCA) work in tandem to prevent unauthorised government access to private electronic communications. The ECPA includes three titles. Title I outlaws unlawful interceptions of wire, oral and electronic communications. Title II contains the SCA, which regulates the disclosure of electronic communications in electronic storage with third-party internet service providers. Title III regulates the use of pen registers or trap and trace devices, which are devices that can acquire metadata, such as phone numbers. Many states have similar laws against government and private wiretapping, some of which are even more stringent than the federal laws.

The GLBA Privacy Requirements mandate that financial institutions give consumers privacy notices that explain the institution's information-sharing practices. Consumers also have the right to opt out and limit some of the information shared. Financial institutions must protect the information collected about individuals, except for information collected in business or commercial activities.

In the health-care sector, the HIPAA Privacy Rule protects all individually identifiable health information stored or transmitted by a covered entity or its business associate in any form or media. In particular, the HIPAA Privacy Rule regulates how covered entities use and disclose protected health information. It also creates limitations on the release of health records, establishes safeguards to protect the privacy of health information, creates accountability through civil and criminal penalties and enables patients to determine how their information is used and whether any disclosures have been made.

10 What are the principal cyberactivities that are criminalised by the law of your jurisdiction?

In general, a wide variety of criminal laws touch cybersecurity one way or another. For example, federal criminal statutes address the following activities, among others:

- computer hacking;
- identity theft;
- economic espionage;
- trade secret theft;
- breaking into computer systems and accessing, modifying, or deleting data;
- stealing confidential information;
- defacing internet websites; and
- flooding websites with high volumes of irrelevant internet traffic to make websites unavailable to actual customers.

11 How has your jurisdiction addressed information security challenges associated with cloud computing?

There is no overarching framework for regulation of cloud computing information security. As such, this is done on an ad hoc, sector-by-sector basis.

For example, HIPAA regulations require entities covered by HIPAA to execute a business associate agreement with their cloud providers. These agreements subject the cloud provider to many of the same privacy restrictions as the initial covered entity. Similarly, the GLBA regulations and Federal Financial Institutions Examination Council (FFIEC) guidance require financial services companies to exercise diligence over their third-party information technology providers, which includes cloud providers.

In addition, the Federal Risk and Authorization Management Program (FedRAMP) is a government-wide programme that incorporates cloud computing into the federal government's IT capabilities through the authorisation and use of certified cloud computer providers. It also provides a standardised approach to securing cloud products and services.

One of the goals of FedRAMP is to significantly decrease government costs, secure cloud networks, create consistent security standards and provide continuous monitoring.

12 How do your jurisdiction's cybersecurity laws affect foreign organisations doing business in your jurisdiction? Are the regulatory obligations the same for foreign organisations?

Foreign organisations that do business in the US are generally subject to state and federal laws to the same extent as US businesses operating in the same jurisdictions and collecting information about US individuals.

Best practice

13 Do the authorities recommend additional cybersecurity protections beyond what is mandated by law?

The National Institute of Standards and Technology (NIST) Cybersecurity Framework, issued in response to direction from Executive Order 13636, Improving Critical Infrastructure Cybersecurity, provides voluntary cybersecurity standards for protecting private sector computer networks owned or operated by critical infrastructure entities. NIST issued the first version of the Cybersecurity Framework in February 2014.

The Framework is divided into three parts: Framework Core, Implementation Tiers, and Framework Profile. The Framework Core is designed to identify key cybersecurity activities common across all critical infrastructure networks. These are activities that companies should address when creating programs to protect critical computer systems and that identify best practices for communicating risks throughout an organisation. Specifically, the Framework Core consists of five functions designed to provide company decision-makers with a strategic view of cybersecurity risk management: identify, protect, detect, respond and recover.

For each function, the Framework identifies existing technical standards, from NIST and other standards bodies, to serve as 'informative references' in support of the technical implementation of the functions.

The Implementation Tiers provide context on how an organisation views cybersecurity risk and the processes in place to manage that risk. The Tiers range from Partial (Tier 1) to Adaptive (Tier 4) and describe an increasing degree of rigour and sophistication in cybersecurity risk management practices based on the business needs of the organisation.

The Framework Profile is intended to help organisations 'establish a roadmap' for prioritisation of organisational efforts to reduce cybersecurity risks. Organisations are encouraged to focus on identifying and eliminating gaps between the 'Current Profile,' which identifies cybersecurity outcomes currently being achieved, and the 'Target Profile', which indicates the outcomes needed to achieve cybersecurity risk management goals.

14 How does the government incentivise organisations to improve their cybersecurity?

There have been numerous legislative proposals to develop incentives for organisations to improve their cybersecurity, including tying adoption of standards to incentives such as grants and streamlined regulation, or using tax credits, but so far these initiatives have not been passed and implemented.

15 Identify and outline the main industry standards and codes of practice promoting cybersecurity. Where can these be accessed?

The NIST Cybersecurity Framework is a recently developed standard for promoting cybersecurity. It can be accessed at www.nist.gov/cyberframework/. For financial institutions, the FFIEC issues an Information Security Handbook that outlines audit guidelines for reviewing financial institutions' security practices, effectively providing best practices to protect against security breaches. It can be accessed at http://ithandbook.ffiec.gov/it-booklets/information-security.aspx.

16 How do the government and private sector cooperate to develop cybersecurity standards and procedures?

The Department of Homeland Security (DHS), the Federal Bureau of Investigation, and the DoD all have established information sharing programs aimed at encouraging the private sector to share information about cyberthreats, such as indicators of compromise. Likewise, the NIST Framework is intended to be a voluntary, industry-led standard that applies to all critical infrastructure sectors. In developing the Framework, NIST issued a draft Framework, engaged with stakeholders at Cybersecurity Framework workshops, and solicited feedback and suggestions for the final Framework. NIST continues to update and improve the Framework as industry provides feedback on implementation.

17 Is insurance for cybersecurity breaches available in the jurisdiction and is such insurance common?

Insurance for cybersecurity breaches is available in the United States, and is becoming far more common for companies to have. The DHS has worked with public and private sector stakeholders to examine the current cybersecurity insurance market and develop solutions to advance its capacity to incentivise better cyber risk management.

Enforcement

18 Which regulatory authorities are primarily responsible for enforcing cybersecurity rules?

Enforcement of cybersecurity rules and standards falls to a variety of federal and state agencies. Various state attorneys general have initiated investigations of major data breaches and in some cases a group of US state attorneys generals have joined together to initiate multi-state investigations of data breaches. At the federal level, the US Secret Service (Electronic Crimes Task Forces and Cyber Intelligence Section), Federal Bureau of Investigation (FBI), and the DHS play leading roles in identifying and investigating cyber breaches. The SEC also requires disclosure of material cyber risks and incidents and has initiated several investigations relating to cyber incidents and information security. The Federal Trade Commission (FTC) has also investigated companies for failing to protect consumers' personal information and take reasonable cybersecurity steps. The FTC has reached over 50 settlements of enforcement actions related to the alleged failure of companies to take reasonable data security measures. The HHS also has authority to investigate data breaches involving medical patient information. The US Congress has also initiated its own investigations into prominent data breaches.

19 Describe the authorities' powers to monitor compliance, conduct investigations and prosecute infringements.

US federal and state authorities have wide-ranging authorities to monitor compliance, conduct investigations and prosecute infringements under numerous state and federal statutes. This includes the authority to demand documents and testimony, pursuant to legal process, and other information relating to cybersecurity incidents.

20 What are the most common enforcement issues and how have regulators and the private sector addressed them?

The most common enforcement actions are based on allegations of insufficient cybersecurity practices and failure to disclose breaches involving consumer information. The FTC has an active enforcement programme examining companies that allegedly did not take reasonable steps to protect consumer information. The FTC frequently seeks long-term consent agreements with companies that impose cybersecurity obligations. Such obligations may run for decades and require companies at their own expense to take certain security steps and have outside independent audits of the companies' compliance with the consent agreement. Individual state attorneys general have also initiated investigations obtained settlements relating to the loss of consumer data. The SEC has sent a variety of letters to corporations requesting information on past cyber incidents. The private sector has responded through the creation of best practices, and the NIST released a preliminary cybersecurity framework for private industry in early 2014.

21 What penalties may be imposed for failure to comply with regulations aimed at preventing cybersecurity breaches?

The most common penalties for failing to comply with cybersecurity-related regulations are related to the entry into consent orders with the federal or state government, class action lawsuits, civil penalties, and payment card industry compliance fees (designed to ensure that credit card information is securely maintained). Other potential penalties include cease and desist orders, criminal penalties, limitations on activities, functions, and operations, registration revocations, and termination of insurance.

22 What penalties may be imposed for failure to comply with the rules on reporting threats and breaches?

Penalties that may be imposed for failure to comply with the rules on reporting threats and breaches include civil enforcement penalties and monetary judgments through litigation.

23 What challenges and appeals can parties make against non-compliance rulings?

For class action litigation, parties can appeal through the normal appeals process for that jurisdiction (often in state courts). For federal enforcement actions, parties can challenge rulings in federal courts.

24 What are the possible sanctions for cybercrimes?

The Computer Fraud and Abuse Act provides for fines or imprisonment for up to 20 years. The Department of Justice may also criminally prosecute egregious violations of the Health Insurance Portability and Accountability Act, and the Economic Espionage Act also contains certain criminal penalties for trade secret theft.

25 How can parties seek private redress for unauthorised cyber activity or failure to adequately protect systems and data?

Depending on the facts of a specific situation, parties may seek private redress under a variety of causes of action, including approximately 34 separate tort claims, 15 contract claims, and other claims based on state and federal statutes. In particular, numerous state data breach notice laws contain individual rights of action, and consumers have brought class actions in response to data breaches involving sensitive personal information.

Threat detection and reporting

26 What policies or procedures must organisations have in place to protect data or information technology systems from cyberthreats?

There are currently no policies or procedures that all organisations must have in place to protect against cyberthreats. However, there are numerous federal laws, regulations, and mandatory standards that pertain to securing privately owned IT systems and data in our nation's critical infrastructure sectors, resulting in a patchwork of regulatory requirements organisations must follow.

For instance, organisations performing contracts requiring a security clearance from the US government generally are covered by the National Industrial Security Program and are obligated to follow the National Industrial Security Program Operating Manual (NISPOM). The NISPOM includes a wide range of information system security requirements, including identification and authentication management, passwords and scanning for malicious code.

Following Executive Order 13556, the government is standardising the way that the federal executive branch protects Controlled Unclassified Information, which includes the upcoming issuance of new Federal Acquisition Regulations provisions to require government contractors to protect information by such means as passwords and other access controls, encryption, and threat monitoring.

Covered entities under HIPAA must implement technical policies that allow only authorised persons to access electronic protected health information and have measures that guard against unauthorised access to electronic protected health information when it is transmitted over an electronic network.

Under the GLBA, financial institutions are required to identify and control risks to customer information and customer information systems and to properly dispose of customer information. Appropriate measures the institutions must take include access controls on customer information systems and monitoring systems and procedures to detect actual and attempted attacks on or intrusions into customer information systems.

27 Describe any rules requiring organisations to keep records of cyberthreats or attacks.

Currently there are no broad rules requiring all organisations to keep records of cyberthreats or attacks. For organisations within certain critical infrastructure sectors, there may be agency-specific rules organisations are obligated to follow. Additionally, companies subject to the Payment Card Industry Data Security Standards are required to maintain certain log and other forensic data for a period of time to facilitate forensic review and audit.

Because cybersecurity breaches may require disclosure and result in litigation and/or regulatory enforcement, however, organisations should be aware that they may be required to provide forensic evidence and information about any such attacks. Organisations should maintain records accordingly (consistent with standard preservation practices).

Update and trends

Given the uneven patchwork of cybersecurity laws and regulations at both the state and federal levels, pressure has been growing in the United States for the establishment of more uniform and clear cybersecurity standards. But a consensus on how to craft such standards has proven elusive, with some political leaders advocating for more government-imposed regulations and others pushing for industry-driven solutions to cybersecurity challenges. Several legislative proposals are under consideration to bolster protections for critical infrastructure, increase information sharing and cyber protection standards, clarify data breach notification requirements, and enhance penalties for cybercrimes. Even without legislation, federal agencies are likely to increase enforcement actions under existing authorities. Firms with insufficient cybersecurity practices will also continue to be exposed to an array of private rights of action by consumers whose personal data has been compromised. Where cybersecurity reforms have occurred in the past several years, they have generally proceeded in close consultation with private industry. Indeed, Executive Order 13636 focuses on 'voluntary' adherence by private industry to a common set of cybersecurity standards, and generally depends on industry cooperation to succeed. A proactive approach by firms, including development of comprehensive cybersecurity policies with plans for reacting to cyber breaches, will help ensure that private industry plays a leading role in shaping reforms to the cybersecurity legal landscape.

28 Describe any rules requiring organisations to report cybersecurity breaches to regulatory authorities.

Numerous federal and state regulations require organisations to report cybersecurity breaches to regulatory authorities.

Public companies may be required to disclose through public filings with the SEC material breaches that affect the company's products, services, relationships with customers or suppliers, or competitive conditions.

'Cleared defence contractors' (ie, those who have been granted clearance by the DoD to access, receive, or store classified information) and contractors with 'unclassified controlled technical information' on their systems that experience a cybersecurity breach must report the breach to the DoD.

Organisations covered by HIPAA are required to notify the Secretary of Health and Human Service following a breach of unsecured protected health information.

Most states also have enacted state data breach notice legislation, many of which require organisations to notify state attorneys general and other state regulatory agencies of security breaches involving sensitive personally identifiable information that affect individuals in the state. Many of these states also require additional notice to individuals and, at times, the media, of certain breaches that result in the loss of personally identifying information.

29 What is the timeline for reporting to the authorities?

Public companies may disclose material breaches to the SEC through a Form 8-K, the 'current report' companies must file with the SEC to announce major events that shareholders should know about.

For breaches that affect UCTI, reports must be sent to the DoD via http://dibnet.dod.mil/ within 72 hours of discovery of any cyber incident and must include specific, detailed data about the nature of the intrusion and any government projects possibly implicated. Regulations regarding reporting requirements for cleared defence contractors have not yet been promulgated, but the statute requires 'rapid reporting' of breaches.

For breaches related to unsecured protected health information that affect 500 or more individuals, HIPAA-covered organisations are required to notify the Secretary of HHS without reasonable delay, and in any case no later than 60 days after a breach. For breaches that affect fewer than 500

individuals, the Secretary may be notified of such breaches on an annual basis.

For notification to states regarding breaches affecting individuals in that state, most state laws require notification be made without undue delay and in the most expedient time possible, though some states include specific time frames.

30 Describe any rules requiring organisations to report threats or breaches to others in the industry, to customers or to the general public.

Most states require organisations to report security breaches involving personally identifiable information to individuals whose information was affected. Each state has its own rules, but typical requirements include that the notification be made in writing in the most expedient time possible. At the federal level, HIPAA and the GLBA require covered entities to report breaches of sensitive health or financial information, respectively. Many state data breach laws include an exception for entities complying with these federal obligations.

31 Describe practices and procedures for voluntary sharing of information about cyberthreats in your jurisdiction. Are there any legal or policy incentives?

The Defense Industrial Base (DIB) Voluntary Cyber Security and Information Assurance programme is a voluntary cybersecurity information-sharing programme between DoD and eligible DIB companies. Companies in the programme receive certain threat information in return for sharing information regarding network intrusions that could compromise critical DoD programmes and missions.

Several industries have developed information sharing and analysis centres (ISACs) designed to share intelligence on cyber incidents, threats, vulnerabilities, and associated responses present throughout the industries. The National Council of ISACs recognises the following centres: aviation, defence industrial base, emergency services, electric sector, financial services, information technology, maritime security, multi-state, communications, national health, nuclear, oil and gas, public transit, real estate, research and education, supply chain, surface transportation, and water. In the wake of the recent increase in retail breaches, a new retail ISAC has also been established.

Organisations may also choose to voluntarily share information with federal and state law enforcement and the DHS to aid in the investigation and prosecution of criminal cybersecurity attacks.

32 Are there generally recommended best practices and procedures for responding to breaches?

In responding to breaches, retaining data security experts and forensic specialists can guard against compromises or figure out the causes of a particular incident to restore a system's integrity, as well as help remediate and identify need for additional controls. Experienced outside counsel can help preserve privileges, conduct internal investigations, and determine obligations and counsel company through the state and federal disclosure process.

WILMERHALE®

Benjamin A Powell **benjamin.powell@wilmerhale.com**
Jason C Chipman **jason.chipman@wilmerhale.com**
Marik A String **marik.string@wilmerhale.com**
Carla J Weiss **carla.weiss@wilmerhale.com**
DeAnna Evans **deanna.evans@wilmerhale.com**

1875 Pennsylvania Ave, NW
Washington, DC 20006
United States

Tel: +1 202 663 6000
Fax: +1 202 663 6363
www.wilmerhale.com

Getting the Deal Through

Acquisition Finance
Advertising & Marketing
Air Transport
Anti-Corruption Regulation
Anti-Money Laundering
Arbitration
Asset Recovery
Aviation Finance & Leasing
Banking Regulation
Cartel Regulation
Climate Regulation
Construction
Copyright
Corporate Governance
Corporate Immigration
Cybersecurity
Data Protection & Privacy
Debt Capital Markets
Dispute Resolution
Domains & Domain Names
Dominance
e-Commerce
Electricity Regulation
Enforcement of Foreign Judgments
Environment
Foreign Investment Review
Franchise
Gas Regulation
Government Investigations
Insurance & Reinsurance
Insurance Litigation
Intellectual Property & Antitrust
Investment Treaty Arbitration
Islamic Finance & Markets
Labour & Employment
Licensing
Life Sciences
Mediation
Merger Control
Mergers & Acquisitions
Mining
Oil Regulation
Outsourcing
Patents
Pensions & Retirement Plans
Pharmaceutical Antitrust
Private Antitrust Litigation
Private Client
Private Equity
Product Liability
Product Recall
Project Finance
Public-Private Partnerships
Public Procurement
Real Estate
Restructuring & Insolvency
Right of Publicity
Securities Finance
Ship Finance
Shipbuilding
Shipping
State Aid
Tax Controversy
Tax on Inbound Investment
Telecoms & Media
Trade & Customs
Trademarks
Transfer Pricing
Vertical Agreements

Also available digitally

Online

www.gettingthedealthrough.com

iPad app

Available on iTunes

Law Business Research

Cybersecurity
ISSN 2056-7685

THE QUEEN'S AWARDS FOR ENTERPRISE: 2012

LACCA
LATIN AMERICAN CORPORATE COUNSEL ASSOCIATION

Official Partner of the Latin American Corporate Counsel Association

ABA Section of International Law
Your Gateway to International Practice

Strategic Research Sponsor of the ABA Section of International Law