LEXOLOGY®
Getting The Deal Through

Cybersecurity

in USA

Table of contents

Contributors

USA

Benjamin A. Powell
benjamin.powell@wilmerhale.com
Wilmer Cutler Pickering Hale and Dorr LLP

Jason C. Chipman
jason.chipman@wilmerhale.com
Wilmer Cutler Pickering Hale and Dorr LLP

Leah Schloss
leah.schloss@wilmerhale.com
Wilmer Cutler Pickering Hale and Dorr LLP

Maury Riggan
maury.riggan@wilmerhale.com
Wilmer Cutler Pickering Hale and Dorr LLP

LEGAL FRAMEWORK

Legislation

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

The United States generally addresses cybersecurity through sector-specific statutes, regulations and private industry requirements.

At the federal level, numerous agencies impose cybersecurity standards through a variety of regulatory and enforcement mechanisms. For example, the Gramm–Leach–Bliley Act (GLBA) and the Health Insurance Portability and Accountability Act (HIPAA) (and implementing regulations and agency guidance) require entities in the financial services and health sectors, respectively, to employ technical, administrative and physical safeguards to protect customer information from unauthorised access or use. Several states have also implemented financial or health sector cybersecurity requirements. Perhaps most notably, the New York Department of Financial Services (NYDFS) has issued cybersecurity requirements for financial services companies licensed under New York law.

The Federal Information Security Management Act (and implementing guidance) establishes cybersecurity standards for federal government agencies and their contractors. The Federal Risk and Authorization Management Program (FedRAMP) is a government-wide programme that provides a standardised approach to security assessments, authorisation and continuous monitoring for companies providing cloud services to federal civilian agencies. Provisions of the Department of Defense (DOD) Defense Federal Acquisition Regulations Systems (DFARS) mandate the use of cybersecurity-related contract clauses in nearly all DOD contracts and subcontracts. The DFARS regulations include requirements with respect to security controls and cyber incident reporting. The Federal Acquisition Regulations (FAR) Council has also issued its own rule, which is intended to prescribe 'the most basic level' of safeguards for acquisitions by US federal executive agencies when a contractor's information systems may contain 'federal contract information'. The FAR rule requires contractors to implement a set of safeguards that are a subset of those required under the DFARS rule.

The Federal Trade Commission (FTC) is the main federal consumer protection agency responsible for enforcing the FTC Act's prohibition on 'unfair and deceptive acts or practices'. Using this authority, the FTC frequently enforces minimum security requirements with respect to entities collecting, maintaining or storing consumer's personal information. In June 2015, the FTC issued the 'Start with Security' guide, which identifies the FTC's lessons learned from over 50 data security enforcement actions brought by the FTC since 2001. The guide advises companies to incorporate a series of 10 lessons learned, ranging from authentication controls to network segmentations.

In mid-2018, a federal appellate court vacated an FTC order issued against a company for allegedly 'unreasonable' security practices in violation of the FTC Act. The court held that the FTC's order had failed to direct the company to cease committing any specific unfair acts or practices and instead imposed only the general requirement that it maintain a 'comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers'. While the court avoided the broader issue of whether the alleged security failings constituted 'unfair' business practices under the FTC Act, the decision raised questions about parts of the FTC's prior data security consent orders and may cause the FTC to shift its approach for future data security enforcement actions.

The Sarbanes–Oxley Act of 2002 (and implementing regulations) requires publicly traded companies to maintain a system of internal controls over financial reporting. Regulatory guidance states that '[m]anagement's evaluation of the risk of misstatement [of financial reports] should include consideration of the vulnerability of the entity to fraudulent activity . . . and whether any such exposure could result in a material misstatement of the financial statements.' To meet these requirements, companies are audited to determine the extent to which they maintain a series of IT 'general

controls' on systems designated as related to financial reporting. In early 2018, the Securities and Exchange Commission (SEC) approved an interpretive release updating guidance on public company disclosures and other obligations concerning cybersecurity matters. Much of the guidance is devoted to reiterating and expanding upon earlier staff guidance, which was issued to assist companies in assessing what disclosures might be required about cybersecurity risks or incidents. The new guidance further illustrates potential disclosures that companies should consider, stresses the importance of cybersecurity policies and procedures, and discusses the application of disclosure controls and procedures, insider trading prohibitions and selective disclosure prohibitions in the cybersecurity context. Recognising that the cybersecurity landscape continues to shift, the SEC's chair noted that the SEC 'will continue to evaluate developments in this area and consider feedback about whether any further guidance or rules are needed'.

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. The Food and Drug Administration (FDA) has issued guidance on considerations for the post-market management of cybersecurity in medical devices. The guidance states that medical device cybersecurity is a shared responsibility among stakeholders, including healthcare facilities, patients, providers and manufacturers of medical devices. It recommends that companies address cybersecurity vulnerabilities during the design and development of medical devices, and also states that manufacturers should address cybersecurity vulnerabilities after medical devices have entered the market. In 2018, the FDA issued a draft revised version of the premarket guidance, as well as a cybersecurity 'playbook' for healthcare delivery organisations focused on promoting cybersecurity readiness.

There have also recently been numerous legislative proposals to regulate the security of certain sectors, including the automotive sector, data brokers, certain energy companies and internet of things manufacturers.

In addition to the sector-specific regulations described above, a handful of states have adopted general security requirements that apply to companies conducting business in their state, collecting personal information about residents or citizens of their states, or both. A primary example is the Massachusetts Standards for the Protection of Personal Information of Residents of the Commonwealth. These regulations require companies collecting personal information about Massachusetts residents to develop written information security programmes containing administrative, technical and physical safeguards. Other states have enacted narrower requirements, such as security requirements for particularly sensitive information (eg, payment card data, mental health information) and secure disposal requirements for electronic or paper media containing sensitive personal information.

In the criminal context, the Computer Fraud and Abuse Act (CFAA) outlaws intrusions into or interference with the security of a government computer network or other 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 prohibits 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 obtaining, altering or preventing authorised access to a wire or electronic communication while it is in electronic storage.

Beyond regulatory 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 establishes its own cybersecurity standards (the Payment Card Industry Data Security Standards (PCI-DSS)) that apply to merchants or vendors 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, President

Obama 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. Pursuant to this Executive Order, the National Institute of Standards and Technology (NIST) issued the voluntary Cybersecurity Framework, which provides a risk-based approach to cybersecurity and references various national and international standards. NIST's role in facilitating and supporting the development of the Framework was codified in the Cybersecurity Enhancement Act of 2014. President Trump's Executive Order 13800 – Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, requires federal agency heads to implement the NIST Cybersecurity Framework, further encouraging broad adoption of the voluntary risk-based standard.

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 healthcare sector are the most regulated sectors with regard to cybersecurity. Federal banking agencies promulgated several data security guidelines in 2000, including the Interagency Guidelines Establishing Information Security Standards. This guidance states that certain covered 'financial institutions' are required to implement comprehensive written information security programmes, including administrative, technical and physical safeguards 'appropriate to the size and complexity' of the financial institution and 'the nature and scope of its activities'. The financial regulators, through the Federal Financial Institutions Examination Council (FFIEC), have also issued a series of booklets as part of the IT Examination Handbook, covering issues ranging from information security to outsourcing technology services to management and governance. The Securities and Exchange Commission (SEC) has also issued guidance to public companies (as well as to the financial services institutions it regulates) and has articulated steps the SEC will take in the future to ensure cybersecurity preparedness in the securities sector. Some states have also issued cybersecurity requirements for financial institutions.

In the healthcare sector, under HIPAA, the Department of Health and Human Services (HHS) has adopted security standards to protect individually identifiable health information and has, in recent years, launched audits to assess compliance with HIPAA. Some states have also issued cybersecurity requirements for this sector.

Has your jurisdiction adopted any international standards related to cybersecurity?

The United States has not adopted any international cybersecurity standards into law. However, NIST's Cybersecurity Framework, created pursuant to Executive Order 13636, establishing voluntary standards applicable to critical infrastructure companies that incorporate many of these international benchmarks as examples of best practice to help US companies manage and reduce cybersecurity risks. NIST has continued to engage with industry stakeholders to update the framework.

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&Os) 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.

Regulators, particularly in the financial services sector, have made clear that they expect board and management involvement in data security. For example, for the financial sector, the Interagency Guidelines Establishing Information Security Standards provide that the board of directors or an appropriate committee of the board shall approve the entity's written information security programme and oversee the development, implementation and maintenance of the programme, including assigning specific responsibility for its implementation and reviewing reports from management. Similarly, the FFIEC IT Examination Handbook Management Booklet emphasises the importance of board oversight and management implementation of effective IT programmes, including IT security. The NYDFS cybersecurity requirements also mandate that a covered financial institution's cybersecurity policy be approved by a senior officer, the board of directors or a board committee; that the senior official overseeing the programme report at least annually to the board or equivalent governing body; and that the board or a senior official certify the entity's compliance with the regulatory requirements.

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 to 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. For public companies, the recently issued SEC guidance indicates that required securities disclosures about how a company's board administers its risk oversight function should include a discussion of the board's role in overseeing the management of cybersecurity risks where such risks are material to a company's business. As part of this disclosure, the Guidance encourages companies to include a discussion about how the board interacts with management on cybersecurity issues.

How does your jurisdiction define cybersecurity and cybercrime?

The United States 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. Protected computers include computers used in interstate communication, such as computers connected to the internet. Cybersecurity is generally not defined in law.

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 required to be taken to thwart cyberthreats and data breaches. Both healthcare and certain financial services entities 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. Under federal government contract clauses, the DOD and other federal agency contractors and subcontractors holding certain (broadly defined) categories of information (covered defence information and federal contract information, respectively) are required to comply with security requirements prescribed in NIST Special Publication 800-171, Protecting Controlled Unclassified Information in Nonfederal Information Systems and

Organizations (with only a subset required for non-DOD contractors). DOD contractors and subcontractors providing IT services or cloud services are required to comply with other security requirements specified in the contract or in DOD cloud security guidance. Contractors providing cloud services to civilian government agencies under FedRAMP are also required to comply with certain contractual security requirements.

Merchants, payment processors and other parties dealing in payment cards, such as credit cards, are required to comply with various technical requirements under the PCI-DSS, which are implemented via contracts 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, NIST's Cybersecurity Framework catalogues best practices for identifying, protecting, detecting, responding to and recovering from cybersecurity incidents by creating adaptable benchmarks and recommendations. Although 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.

Scope and jurisdiction

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

Both the Digital Millennium Copyright Act and the CFAA prohibit certain cyberthreats to US intellectual property rights, including threats arising from cyber intrusions. The Defend Trade Secrets Act authorises trade secret owners to file a civil action in federal court seeking relief for trade secret misappropriation. This Act is seen by many as an important tool for businesses to sue insider threats and other cyber thieves for intellectual property theft.

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 the 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 and FERC. They also require the characterisation of all cyber systems that influence the bulk-electric system as low, medium or high impact. In addition, these standards call for responsible entities to identify, assess and correct deficiencies in their cyber policies. In April 2018, FERC updated these standards to clarify the obligations of operators of 'low impact' bulk-electric systems and cyber systems with respect to protecting against access from external users or devices, and to articulate standards for protecting against threats from transient devices, such as thumb drives. Additionally, the Transportation Security Administration has statutory authority to promulgate regulations related to pipeline physical security and cybersecurity, though it has not yet exercised this authority to issue cybersecurity requirements. As discussed above, the financial, healthcare and government contracting sectors are subject to regulatory and contractual requirements to implement administrative, technical and physical safeguards to prevent or mitigate a cyberattack.

President Obama also issued Executive Order 13636 – Improving Critical Infrastructure Cybersecurity, which called for the enhancement of security measures to protect critical infrastructure. This Executive Order did not establish

mandatory standards but, instead, required the creation of voluntary standards for the protection of critical infrastructure entities. Pursuant to this Executive Order, NIST issued the voluntary Cybersecurity Framework, which provides a risk-based framework and identifies best practices for identifying, protecting, detecting, responding to and recovering from cybersecurity incidents. NIST published an updated Framework in mid-2018. The Cybersecurity Act of 2015 also includes several significant provisions designed to facilitate the sharing of cybersecurity threat data among the government and private sector companies.

President Trump's Executive Order 13800 – Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure ordered various designated agencies to report to the President on a number of issues relating to critical infrastructure cybersecurity to support these entities' risk management efforts. The reports mandated by the Order include reports on (i) whether federal policies and practices are sufficient to promote market transparency of cybersecurity risk management practices by critical infrastructure entities, particularly publicly traded entities; (ii) the potential scope and duration of a prolonged power outage associated with a significant cyber incident, the country's readiness to manage the consequences of such an incident, and any gaps or shortcomings in assets or capabilities; and (iii) cybersecurity risks facing the defence industrial base, including its supply chain, and US military platforms, systems, networks and capabilities, as well as recommendations for mitigating those risks. The Order also required designated agencies to identify authorities and capabilities to support critical infrastructure entities at greatest risk (as identified under a process established by Executive Order 13636) and solicit input from those entities as to whether and how these authorities and capabilities might be employed to support their cyber risk management efforts.

In May 2019, President Trump issued an executive order directing federal agencies to take a variety of steps to improve the quality of cybersecurity professionals who provide critical security functions for US government agencies.

Does your jurisdiction have any cybersecurity laws or regulations that specifically restrict sharing of cyberthreat information?

In the United States, information-sharing restrictions are generally focused on personal communications and personal information. For example, the ECPA, which includes the SCA, restricts sharing of, and government access to, certain private electronic communications. The ECPA includes three titles. Title I outlaws unlawful interceptions of wire, oral and electronic communications. Title II is the SCA, which restricts the disclosure of electronic communications held in electronic storage by third-party electronic communication and remote computing 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, including two-party consent requirements for wiretapping in some states.

Additionally, 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 information collected about individual consumers. Other statutes, such as the Right to Financial Privacy Act, restrict the sharing of certain financial information with the government, subject to several exceptions.

In the healthcare sector, the HIPAA Privacy Rule protects all individually identifiable health information stored or transmitted by a covered entity or its business associate in any 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 to third parties, creates accountability through civil and criminal penalties, and enables patients to determine how their information is used and whether any disclosures have been made.

The Cybersecurity Act of 2015, however, enacted several significant provisions designed to facilitate the sharing of cybersecurity threat data among the government and private sector companies. The Departments of Homeland Security (DHS) and Justice have issued guidance, as required by the Act, regarding the processes for sharing

information with the government in a manner covered by the Act's protections. The agencies have subsequently updated the guidance via a set of frequently asked questions.

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

In general, a wide variety of criminal laws touch on cybersecurity in 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.

Many state laws have also been amended over the past several years to enact similar criminal prohibitions associated with cyber intrusions. For example, in 2016, California amended its criminal laws to prohibit the use of 'ransomware', which is malware often designed to lock access to a computer until a ransom is paid. In late 2018, California enacted a law that went into effect on 1 July 2019 and that makes it illegal 'for any person to use a bot to communicate or interact with another person in California online, with the intent to mislead the other person about its artificial identity for the purpose of knowingly deceiving the person about the content of the communication to incentivise a purchase or sale of goods or services in a commercial transaction or to influence a vote in an election', unless the person discloses its use of the bot in a manner that is 'clear, conspicuous, and reasonably designed to inform persons with whom the bot communicates or interacts'.

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

There is no overarching framework for the regulation of cloud computing information security. However, companies in several economic sectors, particularly the health, financial and government contracting sectors, are subject to guidance or regulations applicable to cloud security. In general, requirements for cloud security focus on the same basic issue: cloud computing is a species of outsourcing, and a company moving data to the cloud remains responsible for the secure handling of that data.

For example, HIPAA regulations require entities covered by HIPAA to execute a business associate agreement with their service providers (including cloud providers) if their service providers are being provided access to personal health records. These agreements subject the service provider to many of the same privacy and security restrictions as the initial covered entity. Similarly, the GLBA regulations and FFIEC guidance require financial services companies to exercise diligence and oversight over their third-party information technology providers, which include cloud providers.

In addition, FedRAMP is a government-wide programme that incorporates cloud computing into federal government civilian agencies' IT capabilities through the authorisation and use of certified cloud computer providers. It also provides a standardised approach to securing cloud products and services. The DOD has issued its own cloud security requirements, as well as special mandatory contractual clauses for DOD cloud service providers.

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 United States are generally subject to state and federal laws to the same extent as US businesses that operate in the same jurisdictions and collect information about US individuals.

BEST PRACTICE

Increased protection

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

The NIST Cybersecurity Framework 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 and released an updated version in mid-2018.

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.

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; however, so far, these initiatives have not been passed or implemented.

The Cybersecurity Act of 2015 included several significant provisions designed to facilitate the sharing of cybersecurity threat data among the government and private sector companies. Among other things, the Act provided liability protection for private sector entities to:

- monitor their own information systems, the information systems of other entities (with authorisation) and information on those information systems;
- operate 'defensive measures' applied to entities' own information systems or the information systems of other

entities (with authorisation); and
- share and receive cyberthreat indicators or defensive measures from other entities, with no duty to warn or act based on information received.

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

- There are a number of cybersecurity standards applicable to specific industries. The following are of note.
- The NIST Cybersecurity Framework is a voluntary standard for promoting cybersecurity. It can be accessed at www.nist.gov/cyberframework.
- For financial institutions, the FFIEC has issued an Information Security Handbook, which is an audit guide 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.
- The PCI-DSS are standards applicable to merchants or vendors that process payment card data. Version 3.2 went into effect on 1 February 2018. Version 3.2.1, issued in May 2018, includes clarifying edits. Version 3.2.1 can be found at www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf.
- The DFARS contains a set of standards applicable to certain defence contractors and mandates the use of cybersecurity-related contract clauses in all DOD contracts. This rule, which includes requirements with respect to security controls and cyber incident reporting, has been highly criticised by industry as being overly burdensome. The rule can be found at 48 CFR subpart 204.73.

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

Guidance from NIST and other independent organisations generally recommend several key actions immediately after learning of a data security breach. Communication is of particular importance, both among company leadership and with key constituencies. Effective breach response often includes an incident response team made up of forensic experts and key personnel who can address legal, public relations, investor relations and SEC, insurance, IT, audit and customer concerns. Most breaches require a coordinated effort to gather the facts through forensic analysis. At the same time, company leaders may need to develop a strategy to respond to the incident. Outside experts often serve important roles in this regard. External counsel can help guide the response to a breach and can structure a forensic investigation in a manner that preserves legal privileges. Outside forensic experts may be necessary to bring special skills to the response and to ensure that company personnel have appropriate resources to address the situation. The FTC has also recently issued data breach response guidance that outlines suggested steps for securing operations, fixing vulnerabilities and notifying appropriate parties. The Department of Justice (DOJ) issued an updated version of its guidance on Best Practices for Victim Response and Reporting of Cyber Incidents, which includes a Cyber Incident Preparedness Checklist. This guidance updates the original version (issued in April 2015) to integrate changes in law, technology, organisational practices and the use of third parties in data management and incident response.

Information sharing

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

The Cybersecurity Act of 2015 includes several significant provisions designed to facilitate the sharing of cybersecurity threat data between the government and private sector companies.

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. The programme is aligned with the incident reporting requirements in the DFARS rule.

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: automotive; aviation; communications; defence industrial base; downstream natural gas; electricity; emergency management and response; financial services; health; healthcare supply chain; information technology; maritime; multistate; national defence; oil and natural gas; real estate; research and education; retail; surface transportation, public transportation and over-the-road bus; and water.

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.

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

The DHS, the Federal Bureau of Investigation (FBI) and DOD have all established information-sharing programmes 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, and it engaged in a similar process of stakeholder engagement and draft publications prior to publishing an update to the Framework in mid-2018. Additionally, the Cybersecurity Act of 2015 enacted several significant provisions designed to facilitate the sharing of cybersecurity threat data among the government and private sector companies.

Insurance

Is insurance for cybersecurity breaches available in your 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, particularly in the wake of judicial opinions finding that general insurance policies do not cover cybersecurity breaches. The breadth of cybersecurity threats and liability risks covered by insurance offerings varies. For example, some policies cover only more traditional cyberattacks, while others cover attacks such as fraudulently induced wire transfers. Similarly, some policies focus their coverage on the costs of notifying individuals and defending litigation in the wake of a breach, with insurance companies now often offering separate endorsements to cover regulatory and payment card brand fines, ransomware payments, and other emerging areas of costs in the wake of a breach. 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

Regulation

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 state attorneys general have joined together to initiate multistate investigations of data breaches. At the federal level, the US Secret Service (Electronic Crimes Task Forces and Cyber Intelligence Section), the FBI and the DHS play leading roles in identifying and investigating cyber breaches. In February 2018, the DOJ announced the creation of a Cyber-Digital Task Force, which issued a report describing the ways that the DOJ is combatting the global cyberthreat and how federal law enforcement can more effectively accomplish its mission in this vital and evolving area. The SEC requires disclosure of material cyber risks and incidents and has initiated several investigations (and is beginning to bring enforcement actions) relating to cyber incidents and information security. Recently, this has included an increased focus on potential insider trading before an incident is publicly announced). The FTC has also investigated companies for failing to protect consumers' personal information and to take reasonable cybersecurity steps. The FTC has reached over 50 settlements of enforcement actions related to companies' alleged failure to implement reasonable data security measures. The HHS also has the authority to investigate data breaches involving medical information, and the US Congress has initiated its own investigations into prominent data breaches.

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

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

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. These 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. As described in 'Legislation', however, in 2018 a federal appellate court called these types of orders into question. Individual state attorneys general have also initiated investigations and 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, and both the SEC and the HHS have entered into settlement agreements (including both injunctive relief and monetary penalties) with entities in the sectors they regulate respectively. The private sector has responded through the creation of best practices and contractual requirements in business-to-business agreements, while NIST released a cybersecurity framework for private industry.

What regulatory notification obligations do businesses have following a cybersecurity breach? Must data subjects be notified?

In the wake of a data breach, notification obligations can be triggered if specially defined categories of information have been accessed or acquired. All 50 US states have a data breach notice law that may demand notice to consumers or data subjects, or notice to regulators (eg, state attorneys general or consumer protection authorities). Additionally, certain organisations may have notice obligations to federal regulators. For example, defence contractors may owe notice to the Defense Criminal Investigation Service, universities may owe notice obligations to the US Department of Education and health organisations may owe notice to the Department of Health and Human Services. Likewise, breaches may trigger private sector contractual notice obligations as well.

Penalties

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 arise from 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.

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.

How can parties seek private redress for unauthorised cyberactivity 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, all 50 states and a number of US territories have data breach notice laws, many of which contain express individual rights of action. Under these statutory authorities, along with common law causes of action, consumers have brought class actions in response to data breaches involving sensitive personal information. US federal courts, however, are split on the nature of the harm required to give consumers standing to sue following a data breach, which is generally focused around whether it is sufficient to have only a risk of future identity theft or fraudulent credit card charges for which consumers are ultimately not responsible for paying.

THREAT DETECTION AND REPORTING

Policies and procedures

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 and state laws, regulations and mandatory standards that pertain to securing

privately owned IT systems and data in the United States' critical infrastructure sectors, resulting in a patchwork of regulatory requirements that organisations must follow.

For instance, organisations performing contracts requiring a security clearance from the US government are generally 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. Other federal contractors and subcontractors at all tiers are also required to comply with various security requirements under the DFARS and FAR rules.

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 that 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.

A primary example of a state law requiring companies to develop policies and procedures to protect data and systems from cyberthreat is the Massachusetts Standards for the Protection of Personal Information of Residents of the Commonwealth, which requires companies collecting personal information of Massachusetts residents to develop written information security programmes containing administrative, technical and physical safeguards that protect personal information.

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. Organisations within certain critical infrastructure sectors may be subject to sector-specific rules. For example, the DFARS rule requires companies to report cyber incidents affecting 'covered defence information' to the DOD, and to maintain forensic evidence (including forensic images and packet captures) for 90 days in the event the DOD decides to conduct a further review and requests that evidence. Additionally, companies subject to the PCI-DSS are required to maintain certain log and other forensic data for a period of time to facilitate forensic review and audit. Further, although companies subject to HIPAA are required to report breaches to the HHS, breaches affecting under 500 individuals only need to be reported collectively in an annual report rather than in the immediate wake of the incident.

Because cybersecurity breaches may require disclosure and result in litigation or regulatory enforcement, 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), including issuing hold notices as appropriate.

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, competitive conditions or financial controls.

Defence contractors with 'covered defence information' on their systems that experience a cybersecurity breach must

report the breach to DoD.

Organisations covered by HIPAA are required to notify the Secretary of HHS following a breach of unsecured protected health information.

Financial institutions subject to the NYDFS cybersecurity requirements must report certain incidents to the NYDFS.

All US states, the District of Columbia and many US territories have also enacted state data breach notice laws, 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. These laws also require notice to individuals and, at times, the media, consumer credit reporting agencies, or both, of certain breaches that result in the loss of personally identifying information.

Time frames

What is the timeline for reporting to the authorities?

Public companies may disclose material breaches to the SEC through a Form 8-K, which is the 'current report' companies must file with the SEC to announce major events that shareholders should know about. Depending on timing, these breaches may instead be reported in typical quarterly or annual securities filings.

For breaches that affect covered defence information, reports must be sent to the DOD (via: https://dibnet.dod.mil/portal/intranet/) 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. 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 unreasonable 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 that notification be made without undue delay and in the most expedient time possible, though some states include specific time frames (typically 30 or 45 days).

Financial institutions subject to the NYDFS cybersecurity requirements must report cyber incidents to the NYDFS within 72 hours of determining that the incident either (i) requires notice to be provided to any government body, self-regulatory agency or any other supervisory body or (ii) has a reasonable likelihood of materially harming any material part of the entity's normal operations.

Companies may also report breaches to law enforcement agencies, an action that the FTC has stated will be regarded favourably when considering whether to bring an enforcement action against a company.

Reporting

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 the 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.

UPDATE AND TRENDS

Update and trends

What are the principal challenges to developing cybersecurity regulations? How can companies help shape a favourable regulatory environment? How do you anticipate cybersecurity laws and policies will change over the next year in your jurisdiction?

Various members of Congress and congressional committees have tried to enact uniform nationwide data breach notification requirements and minimum data security standards. These endeavours, however, have continued to be unsuccessful, in part because of remaining tensions between business interests and state regulators and in part because of other legislative priorities that have taken precedent. With a split Congress in 2020, the chances of a broad data security bill passing both the Republican-controlled Senate and the Democrat-controlled House of Representatives in the year ahead seems increasingly unlikely. At the same time, several US states have introduced proposals modelled on the California Consumer Protection Act, a law that includes a variety of data security mandates for consumer information maintained by covered businesses. The lack of national data security standards has become a heightened issue following a recent federal appellate court decision that raised questions about the FTC's prior data security enforcement practices. Additionally, while state attorneys general had historically been investigating data breaches in collective, multistate investigations, many state regulators have lost patience with the slow pace of these joint investigations and have begun investigating companies' data security and breach response individually. This shift has required companies to respond to even more regulators in the wake of a breach.

In light of the ongoing lack of generally-applicable requirements, we anticipate that sector-specific regulators will continue to exercise their regulatory authority to expand cybersecurity requirements and bring enforcement actions. In the coming year, we anticipate that the federal procurement bodies will issue new cybersecurity regulations for all federal government contractors, building on the rules currently applicable to defence contractors. In light of newly issued public company guidance, we also anticipate increased investigation and enforcement activity from the SEC around cybersecurity disclosure, governance and trading issues.

LAW STATED DATE

Correct On

Give the date on which the information above is accurate.

1 January 2020