Cybersecurity 2016

Contributing editors
Benjamin A Powell and Jason C Chipman
Wilmer Cutler Pickering Hale and Dorr LLP
## Global Overview

Benjamin A Powell, Jason C Chipman and Marik A String
Wilmer Cutler Pickering Hale and Dorr LLP

### Austria

Árpád Geréd
Maybach Görg Lenneis & Partner

### England & Wales

Michael Drury
BCL Burton Copeland

### France

Merav Griguer and Dominique de Combes de Nayves
Dunaud Clarenc Combes & Associés

### Germany

Svenja Arndt
ARNDT Rechtsanwaltsgesellschaft mbH

### India

Salman Waris
TechLegis, Advocates & Solicitors

### Japan

Masaya Hirano and Kazuyasu Shiraishi
TMI Associates

### Korea

Jin Hwan Kim, Brian Tae-Hyun Chung, Jennifer S Keh and Sung Min Kim
Kim & Chang

### Malta

Olga Finkel and Robert Zammit
WH Partners

### Mexico

Federico de Noriega Olea and Rodrigo Méndez Solís
Hogan Lovells BSTL, SC

### Norway

Christopher Sparre-Enger Clausen
Advokatfirmaet Thommessen AS

### Sweden

Jim Runsten and Ida Häggström
Synch Advokat AB

### Switzerland

Michael Isler and Jürg Schneider
Walder Wyss Ltd

### United Arab Emirates

Stuart Paterson, Benjamin Hopps and Nihar Lovell
Herbert Smith Freehills LLP

### United States

Benjamin A Powell, Jason C Chipman and Leah Schloss
Wilmer Cutler Pickering Hale and Dorr LLP
United States

Benjamin A Powell, Jason C Chipman and Leah Schloss
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?

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 Federal Information Security Management Act of 2002 (and implementing guidance) establishes cybersecurity standards for federal government agencies and their contractors. Similarly, 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 enacted state parallels to the GLBA and HIPAA requirement. 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.

In 2015, the Department of Defense (DoD) enacted a potentially significant interim rule (meaning that the rule is in effect but may be further refined when finalised) applicable to companies that do business with the US defence community. The new rule is a DoD regulation that establishes prescriptive cybersecurity requirements as part of the Defense Federal Acquisition Regulations Systems (DFARS), which mandates the use of cybersecurity-related contract clauses in all DoD contracts. These clauses are mandatory ‘flowdown’ terms to subcontractors at all tiers. The rule, which includes requirements with respect to security controls and cyber incident reporting, has been highly criticised by industry as being overly burdensome and in need of revision. The rule is currently in effect, but it was open to a public comment period, and may be changed through the standard regulatory process. In fact, DoD has already announced its intent to issue a new interim rule.

For companies handling consumer data, the Federal Trade Commission (FTC), the main federal consumer protection agency responsible for enforcing the prohibition on ‘unfair and deceptive acts or practices,’ frequently enforces minimum security requirements with respect to entities collecting, maintaining or storing personal information. In June 2015, the FTC issued ‘Start with Security’ guidance, which identifies the FTC’s lessons learned from 30+ data security enforcement actions brought by the FTC since 2001. This guidance advises companies to incorporate a series of 10 lessons learned, ranging from authentication controls to network segmentation.

For publicly-traded companies, the Sarbanes-Oxley Act of 2002 (SOX) and implementing regulations require publicly-traded companies to maintain a system of internal controls over financial reporting. Regulatory guidance has stated 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’ (ITGC) on systems designated as related to financial reporting.

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. There are also numerous pending legislative proposals to regulate the security of certain sectors, including the automotive sector, data brokers and certain energy companies.

A handful of states have also 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, etc) 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 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 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, the President 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 a voluntary ‘Cybersecurity Framework’, which provides a risk-based approach to cybersecurity, and references various national and international standards.
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 several data security guidelines in 2000, including the ‘Interagency Guidelines Establishing Information Security Standards’. These guidelines state that 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 institutions 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 a range of topics 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 the SEC will take in the future to ensure cybersecurity preparedness in the securities sector. In the health-care sector, under HIPAA, the Department of Health and Human Services (HHS) has adopted security standards to protect individually identifiable health information.

3 Has your jurisdiction adopted any international standards related to cybersecurity?
The United States has not adopted any international cybersecurity standards into law. However, NIST has created a ‘Cybersecurity Framework,’ 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.

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&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, the financial sector 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 issued an updated version of the Management Booklet of its IT Examination Handbook in November 2015, which emphasises the importance of board oversight and management implementation of effective IT programmes, including IT security.

5 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. A ‘protected computer’ includes computers used in interstate communication, such as computers connected to the internet. ‘Cybersecurity’ is generally not defined in law, although DoD and the General Services Administration published recommendations in 2014 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 required to be taken to data breaches and data breaches. Both health-care 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 the new DoD-mandated contract clauses, DoD contractors and subcontractors holding certain (broadly defined) categories of information (covered defence information) are required to comply with security requirements prescribed in NIST Special Publication 800-37, ‘Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations,’ while 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 cloud security requirements.

7 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.

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 low, medium or high impact. In addition, these standards call for responsible entities to identify, assess and correct deficiencies in their cyber policies. Additionally, the Transportation Security Administration (TSA) 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. And, as discussed above, the financial, health care and government contracting sectors are subject to regulatory or contractual requirements to implement administrative, technical and physical safeguards to prevent or mitigate a cybersecurity attack.

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. Pursuant to this Executive Order, NIST issued a voluntary ‘Cybersecurity Framework’, which provides a risk-based framework and identifies best practices for identifying, protecting, detecting, responding to and recovering from cybersecurity incidents. The Cybersecurity Act of 2015, which was enacted in December 2015, includes several significant provisions designed to facilitate the sharing of cybersecurity threat data among the government and private sector companies, and marks the end of a multi-year effort to find a compromise between industry demands for liability protection for cybersecurity information-sharing and privacy concerns regarding government access to such information.

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

In the United States, ECPA, which includes the SCA, restricts sharing of, and government access to, certain private electronic communications. ECPA includes three titles. Title I outlawed 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 some states with two-party consent requirements for wiretaping.

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. 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 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 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 HIPAA Privacy Rule applies to health maintenance organisations (HMOs), nursing homes, hospitals, doctors’ offices, and other health-care providers.

The HIPAA Privacy Rule requires all health-care providers, health plans, and health-care clearinghouses to notify individuals in the event of a breach of unsecured protected health information. A breach occurs when protected health information is acquired by unauthorised individuals. The HIPAA Privacy Rule also requires all health-care providers, health plans, and health-care clearinghouses to report a breach to the government and to affected individuals, if the breach involved identifiable health information.

The HIPAA Privacy Rule also requires all health-care providers, health plans, and health-care clearinghouses to report a breach to the government and to affected individuals, if the breach involved identifiable health information.

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. 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. DoD has issued its own cloud security requirements, as well as special mandatory contractual clauses for DoD cloud service providers.

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 United States 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 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 activities include:

- Identify and protect assets that are critical to your business operation;
- Detect threats and vulnerabilities to those assets;
- Respond to incidents when they occur;
- Recover from incidents to normal operations.

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 or implemented.

The Cybersecurity Act of 2015, which was enacted in December 2015, includes several significant provisions designed to facilitate the sharing of cybersecurity threat data among the government and private sector companies at the end of a multi-year effort to find a compromise between industry demands for liability protection for cybersecurity information-sharing and privacy concerns regarding government access to such information. Among other things, the Act provides liability protection for private sector entities to:

- monitor their own information systems, the information systems of another entity (with authorisation), and information on those information systems;
- operate 'defensive measures' applied to an entity’s own information systems or the information systems of another entity (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.

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

There are several cybersecurity standards applicable to specific industries. Of note are:

- the NIST Cybersecurity Framework, which establishes voluntary standards applicable to promoting cybersecurity. It can be accessed at www.nist.gov/cyberframework/;
- for financial institutions, the FFIEC has issued 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://www.ffiec.gov/tti-booklets/information-security.aspx; and
- the PCI-DSS establish standards applicable to merchants or vendors that process payment card data. The current version of these standards (version 3.1, adopted in April 2015) can be found at wwwpci-securetystandards.org/documents/PCI-DSS_v3.1.pdf; and
- a recently enacted set of standards applicable to certain defence contractors was established in late 2015 through amendments to the DFARS, which mandates the use of cybersecurity-related contract clauses for all DoD contracts. This new rule, which includes requirements with respect to security controls and cyber incident reporting, has been highly criticised by industry as being overly burdensome and in need of revision. The rule is currently in effect, but it was open to a public comment period, and may be changed through the standard regulatory process. A copy of the rule can be found at www.gpo.gov/fdsys/pkg/FR-2015-10-02/pdf/2015-24296.pdf.

16. 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 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.

17. 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, which was enacted in December 2015, includes several significant provisions designed to facilitate the sharing of cybersecurity threat data among the government and private sector companies, and marks the end of a multi-year effort to find a compromise between industry demands for liability protection for cybersecurity information-sharing and privacy concerns regarding government access to such information.

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 rule establishing this programme was recently modified to conform with the newly issued DFARS rule (though, as with the DFARS rule, these changes were subject to comment and may be revised through the normal regulatory process).

Several industries have developed information sharing and analysis centres (ISACs) designed to share intelligence on cyber incidents, thereby 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. US law firms and the automotive industry have also recently announced the establishment of industry ISACs.

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

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

DHS, the Federal Bureau of Investigation (FBI), and 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 it provides feedback on implementation. Additionally, the Cybersecurity Act of 2015, which was enacted in December 2015, includes several significant provisions designed to facilitate the sharing of cybersecurity threat data among the government and private sector companies, and marks the end of a multi-year effort to find a compromise between industry demands for liability protection for cybersecurity information-sharing and privacy concerns regarding government access to such information.

19. 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, particularly in the wake of judicial opinions finding that general insurance policies do not cover cybersecurity breaches. 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

20 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), FBI and 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 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. 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.

21 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.

22 What are the most common enforcement issues and how have the 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 program 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 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. The private sector has responded through the creation of best practices, and NIST released a cybersecurity framework for private industry in early 2014.

23 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.

24 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.

25 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, 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.
personally identifiable information that affect individuals in the state. Many of these states also require additional 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.

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. 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 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. 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 notification be made without undue delay and in the most expedient time possible, though some states include specific time frames.

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

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.