Chambers
Global Practice
Guides

Definitive global law guides offering
comparative analysis from top-ranked lawyers

Cybersecurity 2022

USA: Law & Practice
and
USA: Trends & Developments

Ed McNicholas, Fran Faircloth and Kevin Angle
Ropes & Gray LLP

practiceguides.chambers.com

USA

Law and Practice

Contributed by:
Ed McNicholas, Fran Faircloth and Kevin Angle
Ropes & Gray LLP see p.23

CONTENTS

1. BASIC NATIONAL REGIME

1.1 Laws

In the USA, cybersecurity is governed by a complex quilt of generally applicable federal laws, sector-specific federal laws, generally applicable state laws and sector-specific state laws, as well as common law norms that have evolved through court decisions. Generally applicable federal laws govern information sharing with the government and particular acts such as computer hacking or the unlawful interception of electronic communications, while other federal laws dictate specific rules that are applicable only to certain companies in critical infrastructure sectors such as healthcare and financial services.

States have a similar combination of general and sector-specific laws governing cybersecurity. California, for example, has adopted generally applicable information security requirements, along with sector-specific laws such as its own financial services privacy law, the California Financial Information Privacy Act (CalFIPA), and medical information privacy law, the California Confidentiality of Medical Information Act (CMIA).

Companies outside of critical infrastructure sectors are subject to generally applicable reasonable security and data breach notification statutes in state law. New York and Massachusetts, for example, have significant cybersecurity measures in place. These laws hinge on the types of personal information that should be protected. Such statutes generally eschew the broad definitions of personal data contained in the EU's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) in favour of definitions focused on key pieces of personal information, such as a first name and last name in combination with another identifier (eg, social security number or financial account number).

Even the CCPA, which generally applies a broad definition of personal information for its privacy provisions, employs this narrower definition of personal information in the section providing a private right of action for victims of a data breach that is "*a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information*". These state definitions of personal information have expanded over time, with states increasingly including categories such as medical information, biometric information, and username and password within their definitions of personal information subject to security requirements.

Additional details about some of the most significant US cybersecurity laws are provided below.

Federal Trade Commission (FTC) Act

The closest the USA comes to an overarching cybersecurity law is Section 5 of the Federal Trade Commission (FTC) Act, which prohibits unfair or deceptive acts or practices affecting commerce. The FTC has interpreted Section 5 as imposing a de facto reasonable security standard on organisations conducting business in the USA, but it focuses on people as consumers, not employees or in their personal lives. Section 5 also does not apply to most not-for-profit organisations or businesses overseen by some other federal regulators, such as most financial services and much of the healthcare sector.

The FTC may bring two types of actions when enforcing Section 5. First, it may bring an enforcement action against an act or practice that it deems "unfair", in violation of Section 5. Unfair practices are those that are likely to cause substantial injury to consumers, which the consumers cannot reasonably avoid and which are

not offset by benefits to consumers or competition – for example, a failure to encrypt credit card information. The FTC's other principal type of enforcement action under Section 5 is against deceptive statements to consumers – for example, the FTC may allege that a company's promises about security are deceptive where the FTC believes a business has failed to live up to those promises.

Penalties

The FTC Act does not include authority to impose monetary penalties in the first instance, and the Supreme Court recently confirmed in AMG Capital Management LLC v FTC that the FTC is not authorised to seek equitable monetary relief such as restitution or disgorgement in such cases. As a result, FTC settlements in cases alleging unfair or deceptive acts or practices in the area of cybersecurity typically involve extensive (often 20-year) monitoring and reporting requirements and other injunctive relief such as requirements that companies adopt particular security practices. Many of these requirements can themselves be quite onerous and costly.

Additionally, although monetary penalties are not included as initial relief under the FTC Act, once a company enters into a settlement with the FTC, the terms of the settlement may subject the company to future monetary penalties for alleged violations of the order, up to an impressive USD46,517 per violation (which, in the cybersecurity setting, could mean per person). In one notable example, Facebook entered into an FTC settlement in 2012, in which Facebook promised not to misrepresent certain privacy practices; in 2019, the FTC alleged that Facebook had violated that order, and Facebook ultimately entered into a USD5 billion settlement with the FTC.

Sector-Specific Federal Laws

Dozens of sector-specific laws apply to many organisations, including the following most widely applicable:

- the Health Insurance Portability and Accountability Act (HIPAA), which applies to Protected Health Information (PHI) processed by certain healthcare entities or their business associates;
- the Gramm-Leach-Bliley Act (GLBA), which imposes security requirements on certain financial institutions;
- the Communications Act of 1934, as amended, which imposes a duty on telecommunications carriers to protect the confidentiality of proprietary information of customers.

Penalties vary by statute. Civil penalties for unknowing HIPAA violations can range from USD100 to USD50,000 per violation, with the potential for criminal penalties as well.

Anti-Hacking Laws

Other key laws at the federal level include the Computer Fraud and Abuse Act (CFAA), which prohibits several computer crimes, including hacking. Depending on the violation alleged, the CFAA authorises criminal penalties of between one and 20 years of imprisonment, as well as a private cause of action. Significantly, the U.S. Supreme Court recently significantly undercut the application of the CFAA to insider threats.

The Economic Espionage Act is a potent criminal law tool for combatting foreign nation-state (and other) theft of trade secrets, including through hacking and other cybercrimes. Individuals knowingly committing an offence that will benefit a foreign government may be imprisoned for up to 15 years or fined up to USD5 million, and organisations committing violations may be subject to a fine of up to USD10 million or three times the value of the stolen trade

secret to the impacted organisation. The Defend Trade Secrets Act also provides a private right of action available to the victim of the trade secret theft along with a civil seizure remedy.

The Electronic Communications Privacy Act (ECPA) prohibits certain access to data in transit or when held by a stored communications provider or remote computing service, such as a cloud provider. Criminal penalties range up to five years' imprisonment, and a civil cause of action exists.

State Laws

Numerous state laws also impose cybersecurity obligations that protect the personal information of their residents. Every state has some form of unfair or deceptive acts or practices statute, with similar obligations to Section 5 of the FTC Act. Several states have also adopted statutes requiring reasonable security, with state laws in Massachusetts, Nevada and New York establishing more specific security requirements, such as encryption of any personal information transmitted over public networks or wirelessly.

All 50 states, Washington, DC and the US territories have also adopted laws requiring notification to individuals and, in some cases, regulators in the event of a data breach. Notably, however, these data breach notification laws – as well as the reasonable security laws described above – apply to a narrow subset of information, typically including a name in combination with another element such as a social security number or other government identifier, financial account or credit card number, or, increasingly, health or biometric information.

Penalties

Penalties for violations of state cybersecurity laws vary by state, with actual damages typically available along with, in some cases, statutory damages. The New York Stop Hacks and Improve Electronic Data Security (SHIELD) Act creates potentially significant statutory damages of up to USD5,000 per violation of the law's reasonable security requirement. Attorneys general typically interpret a "violation" to mean each impacted individual in an incident, and so such statutory damages can be potentially very substantial; however, regulators will typically settle for well below the theoretical maximum penalty. The California Consumer Privacy Act (CCPA) creates a private right of action with statutory damages of up to USD750 per consumer whose personal information is accessed without authorisation due to a failure by a business to maintain reasonable security procedures.

Courts

As a common law system, the US approach to cybersecurity also includes an important role for the federal and state judiciary in developing common law norms, such as negligence and trespass, and applying them to complex cybersecurity issues. For instance, whether a given set of security practices is reasonable will ultimately be adjudicated in the courts, using norms informed by the common law as well as the interpretation of the relevant statutes.

Industry Self-Regulation

Some significant aspects of the US cybersecurity regime are subject to industry self-regulation, most notably the Payment Card Industry's Data Security Standard (PCI-DSS), which dictates the protections required for payment cards in much more detail than any federal or state law.

NIST

The National Institute of Standards and Technology (NIST) is part of the Department of Commerce, which has developed a Cybersecurity Framework that, while nominally voluntary for the private sector, has inspired several regulatory models that dictate the particular manner in which the US government assesses the cyber-

security of itself, its contractors, and the subcontractors of its contractors, as well as those companies that are in various critical infrastructure sectors.

1.2 Regulators

Regulatory enforcement of cybersecurity is both general and sector-specific in the USA. Some principal regulators include the following.

Federal Trade Commission (FTC)

The FTC asserts the broadest authority among federal regulators over for-profit businesses not otherwise subject to another regulatory authority. As discussed in **1.1 Laws**, the FTC enforces its unfair and deceptive acts and practices jurisdiction, which it interprets as including unreasonable security practices resulting in substantial injury.

Financial Services

The financial services sector is overseen by numerous regulators depending on the type of entity supervised and the financial product or service. These include the Commodity Futures Trading Commission (CFTC), the Consumer Financial Protection Bureau (CFPB) and the Federal Trade Commission (FTC). Self-regulatory agencies such as the Financial Industry Regulatory Authority (FINRA) and National Futures Association (NFA) have also issued rules applicable to cybersecurity.

The Securities and Exchange Commission (SEC) – and, specifically, its Office of Compliance Inspections and Examinations (OCIE), which has authority over certain registered advisers, broker-dealers and funds – has taken a leading role in promoting cybersecurity measures in the financial services sector. While the SEC has brought certain administrative enforcement actions, some of its most notable engagement has been through OCIE cybersecurity market conduct reviews (sometimes called "sweeps"). OCIE has listed cybersecurity as one of its top examination priorities since 2013, and has issued numerous guidance documents describing measures it views as elements of a robust cybersecurity programme. The SEC has proposed rules requiring regulated entities to adopt reasonably designed policies and procedures that include periodic risk assessments, access controls, monitoring, threat and vulnerability management, and incident response.

The FTC also recently updated its cybersecurity safeguards rule applicable to financial institutions such as private funds and mortgage brokers not subject to another functional regulator to require specific security controls and accountability measures.

Healthcare

The Department of Health and Human Services (HHS) – and, in particular, its Office of Civil Rights (OCR) – is responsible for enforcing HIPAA. OCR will investigate complaints and data security breaches with the potential to enforce both civil and, in some instances, criminal penalties. OCR is also tasked with conducting periodic audits of compliance by covered entities and their business associates.

State Regulators

At the state level, numerous regulators also come into play. State attorneys general play a leading role in enforcing cybersecurity laws across sectors, often joining together in multi-state groups to investigate companies experiencing data breaches. State departments of insurance oversee the cybersecurity of their regulated entities.

A particularly notable state regulator is the New York Department of Financial Services (NYDFS), which enforces a comprehensive regulation imposing specific cybersecurity requirements on its regulated entities (banks, credit unions and insurers, among others). Each state has a regula-

tory agency focused on insurance, similar to the NYDFS, and several states have now enacted a model law based on the NYDFS cybersecurity rules.

1.3 Administration and Enforcement Process

Specific investigative procedures vary by agency, and it is important to be aware of the rules and manner of practice before each regulator. Most regulators will typically begin with the issuance of a voluntary request for information or a mandatory Civil Investigative Demand (CID) or subpoena.

Often companies are allowed or encouraged to make presentations to the regulator to discuss the regulator's concerns and the company's practices; this often leads to informal resolutions. Where the agency determines that violations have occurred, it may pursue administrative remedies that can be, but rarely are, challenged in court.

1.4 Multilateral and Subnational Issues

The USA is a federal system, with subnational state and even local laws playing important roles in establishing cybersecurity requirements, as described more fully in **1.1 Laws**.

At the multinational level, the USA participates in efforts to co-ordinate responses to cybercrime. The USA ratified the Budapest Convention, the first cybercrime treaty, aimed at harmonising national laws on cybercrime and increasing transnational co-operation. The USA has also entered into Mutual Legal Assistance Treaties (MLATs) on a bilateral basis with other nations to facilitate co-operation, though some of the mechanisms contemplated by these treaties can be slow to implement.

Due to delays and difficulties associated with MLATs, among other things, the USA enacted the Clarifying Lawful Overseas Use of Data (CLOUD) Act. The CLOUD Act creates a mechanism for the executive branch to enter into treaties with foreign governments to expedite the cross-border flow of data in response to law enforcement requests for electronic data held by providers in foreign jurisdictions. The first CLOUD Act treaty was entered into between the USA and UK in 2019. The USA has also entered into an agreement with Australia under the CLOUD Act that is currently subject to review by legislatures in both countries. If approved, this treaty would make it easier for law enforcement in both countries to obtain evidence from entities in the other country.

Relations with the European Union have focused on the adequacy of US privacy laws, which led to a Safe Harbor and Privacy Shield agreement, both of which were invalidated by the Court of Justice of the European Union. The USA has also spearheaded the APEC Cross-Border Privacy Rules (CBPR) System, which is an effort to create a level international playing field by establishing internationally recognised standards.

1.5 Information Sharing Organisations and Government Cybersecurity Assistance

Since 2018, the Cybersecurity and Infrastructure Security Agency (CISA) has led efforts to co-ordinate the US government's approach to cybersecurity, as well as its outreach to private companies. CISA facilitates information sharing in multiple ways, including by sharing real-time machine-readable cyberthreat indicators and defensive measures.

The DHS (of which CISA is a component) has instituted a Cyber Information Sharing and Collaboration Program (CISCP), through which it shares unclassified threat intelligence information via public-private networks in the critical infrastructure sector. Additionally, the United

States Computer Emergency Readiness Team (US-CERT) provides national threat intelligence and works to assist critical infrastructure in responding to cybersecurity threats. DHS also operates an Automated Indicator Sharing (AIS) capability that shares real-time threat indicators and defensive measures.

Many private organisations participate in Information Sharing and Analysis Centers (ISACs) or Information Sharing and Analysis Organizations (ISAOs), which share threat intelligence, including from government sources. Financial services organisations may, for example, participate in the Financial Services Information Sharing and Analysis Center (FS-ISAC), a non-profit entity created by industry participants that also co-operates closely with the Department of Treasury. In total, 25 sector-specific ISACs are currently members of the National Council of ISACs, covering sectors ranging from the Automotive ISAC to the Elections Infrastructure ISAC.

The creation of these organisations was encouraged by the 1998 Presidential Decision Directive/NSC-63 on Critical Infrastructure Protection. Following up on the success of these efforts, a 2015 executive order further directed the Director of Homeland Security (DHS) to strongly encourage the development and formation of ISAOs.

The FBI and other elements of the intelligence community likewise share information with private sector companies through a variety of programmes such as the FBI's InfraGard private-sector partnership programme.

1.6 System Characteristics

The USA currently follows a largely sectoral/sub-national (state-based) model for enforcement, although some agencies have broad authorities. As noted, the FTC is the principle federal cybersecurity regulator, enforcing its unfair and deceptive acts and practices requirements pursuant to Section 5 of the FTC Act. Likewise, CISA and NIST provide guidance and assistance across the federal government and sectors of US industry, often using a voluntary, co-regulatory approach.

Other federal regulators operate on a sectoral enforcement basis, with agencies such as the SEC, in particular OCIE, reviewing cybersecurity compliance for regulated advisers and broker-dealers, and similarly, HHS, in particular OCR, providing oversight over healthcare entities.

Numerous state cybersecurity requirements are also in place. Data breach notification laws are now in place in all 50 US states, as well as in Washington, DC and three US territories. On top of those data breach laws, multiple states also have additional security requirements. Most of these states require some version of "reasonable" security, though some have more express requirements. Massachusetts was the earliest state to adopt specific security requirements by regulation, including the development of a written information security programme and encryption of all covered data on mobile devices and transmitted across public networks.

In recent years, New York has adopted more specific cybersecurity laws and regulations. The NYDFS adopted some of the strictest requirements for organisations under its supervision. These include data breach notification within 72 hours, penetration testing and multi-factor authentication. This law has spread throughout the insurance sector, which is subject primarily to state oversight. The New York SHIELD Act adds a reasonable security requirement along with specific measures that will satisfy that requirement, which may be interpreted by regulators or plaintiff's attorneys as the appropriate standard of security.

1.7 Key Developments

The year 2021 saw further significant developments in US cybersecurity law. The final report of the Cyberspace Solarium Commission has reflected a significant reconsideration and reformulation of US cybersecurity strategy, leading to several new approaches that are being proposed and enacted in a piecemeal fashion. Overall, the Commission calls for reforms to the US government cybersecurity structures, including efforts to shape international norms for cyberspace, to harden the US critical infrastructure so as to deny benefits to attacks, to inflict costs on attacks through offensive law enforcement and national security operations, to operationalise enhanced public-private co-operation, and to preserve a robust military capacity to use cyber-operations to protect national security. The Commission was led by a bipartisan congressional group and has considerable policy backing.

These efforts have arrived at a propitious time given the significant increase in cyber-attacks. In particular, the notable uptick in ransomware has continued, with recent examples including the March 2021 attack on CNA Financial Corp. (which reportedly paid a USD40 million ransom to regain access to its systems) and the May 2021 attack on Colonial Pipeline. Numerous cities and hospitals were also impacted. Pandemic-related cybersecurity challenges also persisted, such as the increase of phishing scams targeting remote workers. Supply-chain issues came to the fore, and the Log4j vulnerability required rapid responses across industry and government. In light of the ubiquity of cybersecurity threats, it is not surprising that the Biden administration, state and federal regulators, and state legislatures took significant actions to address these risks. Some key highlights are as follows.

Federal Breach Notification

Breach notification requirements for organisations in certain critical infrastructure sectors were added to the consolidated appropriations bill in March 2022. The law will require organisations in certain critical infrastructure sectors to report substantial cybersecurity incidents to the Department of Homeland Security within 72 hours after discovering the incident has occurred, and payments of ransomware within 24 hours. Organisations will also be required to preserve evidence related to the incident. The law will provide protections from disclosure of information contained in reports filed with the Department, including against their use in regulatory proceedings, unless the information is produced in response to a subpoena. Additional details regarding the timing and content of the notice required, as well as the organisations required to comply, will await further rulemaking, which will also establish the date that the notification requirement will become effective.

Following a swath of cyberattacks from nation-states and others, the Biden administration issued Executive Order 14028 (E.O. 14028). The Order had five key objectives:

- increasing information sharing;
- bolstering cybersecurity requirements for agencies and vendors;
- establishing a cybersafety review board;
- setting a standard incident response protocol for federal agencies; and
- prioritising early detection and remediation of cybersecurity risks.

The Order will require, among other things, updates to the Federal Acquisition Regulation (FAR) and Defense Federal Acquisition Regulation Supplement (DFAR) to promote information sharing including a requirement that federal contracts report cybersecurity incidents that could affect a federal agency. Incident and vulnerability response playbooks applicable to federal agencies and required by the order were published by CISA in November 2021.

Department of Justice

The Department of Justice saw its primary anti-hacking statute, the Computer Fraud and Abuse Act narrowed by a Supreme Court decision that significantly undercut the application of the statute to insider threat cases.

The Department, however, proposed a new use of an old statute, the False Claims Act, by asserting that the anti-fraud provision could be invoked against government contractors that falsely certify their cybersecurity status in connection with a government contract or fail to report a significant data breach. The False Claims Act rewards qui tam whistle-blowers the right to bring an action on behalf of the federal government, with potentially a significant share of any recovered funds, and it has proved to be a potent threat to many government contractors in other contexts.

Federal Trade Commission

The FTC continued to assert its regulatory oversight authority; however, a key arrow in the FTC's quiver, its ability to seek equitable monetary remedies such as restitution, was removed by the U.S. Supreme Court's decisions in AMG Capital Management LLC v FTC. Potentially in part due to that development, the FTC announced in December that it was considering initiating a rulemaking that would address "lax security practices". The contours of any such rule were not disclosed and, in any event, will require a lengthy administrative process before being implemented. Adopting a specific rule, though, would provide the FTC with a new vehicle to seek monetary remedies for alleged unfair or deceptive cybersecurity acts or practices.

One area where the FTC has certainly provided greater clarity is with respect to the safeguarding requirements applicable to certain regulated financial institutions. Under the FTC's revised safeguards rule, covered institutions such as private funds and mortgage brokers are required to implement specific security controls such as multi-factor authentication and encryption and to adopt accountability measures.

The FTC is also drawing attention to its Health Breach Notification Rule, which requires a vendor of personal health records that is not an HIPAA-covered entity or business associate to notify affected individuals, the FTC, and in some cases the media of a breach affecting such records. In a policy statement issued in September, the FTC stated that the rule applies to developers of health applications and connected devices.

State Data Protection Laws

States continue to take the lead in adopting more comprehensive privacy and data security requirements in the USA. In 2021, Virginia and Colorado joined California in adopting comprehensive data protection laws, the Virginia Consumer Data Protection Act (VCDPA) and the Colorado Privacy Act (CPA). Both laws go into operation in 2023 and expand on the privacy rights available to individuals and the accountability requirements applicable to businesses, including requirements to conduct data protection assessments with respect to processing activities that create a heightened risk to individuals. The California Privacy Rights Act will also go into operation in 2023 and, among numerous privacy requirements, authorises regulations requiring businesses whose processing of personal information presents a significant risk to the privacy and security of an individual's personal information to perform a cybersecurity audit on an annual basis.

1.8 Significant Pending Changes, Hot Topics and Issues

Executive Initiatives

With progress on a comprehensive federal data protection law likely (though not certain) to stall in Congress in light of the upcoming mid-

term elections, much of the momentum behind cybersecurity change in 2022 will come at the executive level. The Biden administration has already proven to be active in this space, issuing E.O. 14028 and challenging Russia's perceived support for ransomware groups. Given the importance of cybersecurity as a national security issue, that activity is almost certain to continue. Pending initiatives include bolstering federal contracting requirements, responding to supply-chain threats, and moving toward a Zero Trust Architecture.

Passwords

As threat actors develop robust capabilities to crack passwords, organisations are increasingly requiring ever-more complex passwords, rotated frequently. Even with such requirements, passwords are frequently compromised through phishing and other techniques, as the growth of business email compromises demonstrates. Without multi-factor authentication and other controls, passwords can provide minimal protection against even unsophisticated cyber-attacks. Many organisations, accordingly, are likely to move toward adoption of multi-factor authentication, or even abandon standard passwords in favour of other means of authentication such as biometric factors (eg, fingerprints or voice recognition).

State Laws

Even if no federal data protection law is passed, we are likely to see additional efforts at the state level to adopt stricter data protection laws. Bills are currently pending in such diverse states as Alaska, Hawaii, Oklahoma and Washington state. Legislators in some states have proposed novel approaches to data protection. In Massachusetts, for example, legislators have introduced legislation that would impose fiduciary duties on data controllers.

2. KEY LAWS AND REGULATORS AT NATIONAL AND SUBNATIONAL LEVELS

2.1 Key Laws

Please see **1.1 Laws**.

2.2 Regulators

Please see **1.2 Regulators**.

2.3 Over-Arching Cybersecurity Agency

The Cybersecurity and Infrastructure Security Agency (CISA) is the closest body to a single overarching cybersecurity agency in the USA, although authority remains scattered across several agencies. Frequently, the FBI will intermediate civilian, intelligence community and national security interest with respect to complex breaches. For a discussion of regulatory enforcement agencies, please see **1.2 Regulators**. DHS has been tasked with co-ordinating cybersecurity threat intelligence sharing, as described more fully in **1.5 Information Sharing Organisations and Government Cybersecurity Assistance**.

2.4 Data Protection Authorities or Privacy Regulators

The USA does not currently have a Data Protection Authority in the EU sense, although the FTC has some aspects of one. Please see **2.2 Regulators**.

2.5 Financial or Other Sectoral Regulators

Multiple financial services and other sectoral regulators exist. Please see **2.2 Regulators**.

2.6 Other Relevant Regulators and Agencies

Please see **1.2 Regulators**.

3. KEY FRAMEWORKS

3.1 De Jure or De Facto Standards

In general, cybersecurity frameworks such as NIST and ISO 27001 are consulted by US organisations and considered authoritative (or, at a minimum, persuasive) in benchmarking cybersecurity controls. The Federal Financial Institutions Examination Council (FFIEC) adapts the NIST framework to financial services, while the Cybersecurity Maturity Model Certification (CMMC) provides a standard for the defence-industrial base, which is consistent with the NIST framework. Ohio's Data Breach Act expressly provides an affirmative defence based on adherence to such frameworks, as well as, among others, to the Payment Card Industry Cybersecurity Standards (PCI-DSS).

Other relevant controls include the 20 Critical Security Controls (CSCs) issued by the Center for Internet Security (CIS), which the California Attorney General's 2016 California Data Reach Report defines as the minimum standard for reasonable security. The controls include identifying the hardware and software connected to a network, implementing secure configurations, limiting administrator privileges, assessing and patching vulnerabilities, securing critical assets, putting in place key defensive measures, blocking vulnerable access points, monitoring accounts and network audit logs as well as training, testing and planning.

3.2 Consensus or Commonly Applied Framework

NIST is a common framework applied in the USA, and variants of NIST are becoming essentially mandatory in the financial services and defence sectors. Nonetheless, some organisations, particularly those with more of an international presence, frequently certify to ISO 27001. As noted in **3.1 De Jure or De Facto Standards**, other frameworks may provide an affirmative defence under Ohio law, and the California Attorney General's office has specifically referred to the CISA's CSCs.

3.3 Legal Requirements

Data security laws in the USA generally refer to some version of reasonable security, which to some degree is informed by common law norms of negligence. Various agencies, interpreting dozens of statutes, articulate specific requirements for particular sectors or states; often the result is a complex tangle of legal requirements that must be synthesised for interstate, cross-sector and international computer systems. At the federal level, for example, the FTC interprets its "unfairness" authority to require that regulated entities put in place appropriate security procedures. The HIPAA security rule imposes general requirements, including ensuring the confidentiality, integrity and availability of electronic PHI, identifying reasonably anticipated threats, and ensuring compliance from employees and other members of the organisation's workforce.

Some states and sectoral-specific laws have more detailed requirements, as detailed below.

- The NYDFS requires specific security controls from its regulated entities. These include appointment of a chief information security officer (or similar position), vulnerability assessments and penetration testing, audit trails, multi-factor authentication, training, encryption of non-public personal information, and implementation of an incident response plan, including reporting to NYDFS within 72 hours of a notifiable security breach.
- Massachusetts regulations require implementation of a written comprehensive information security programme and other controls, including risk assessments, annual reviews of the scope of security measures, monitoring and access restrictions, and controls for ven-

dors potentially accessing covered personal information.
- Other state laws, including in Nevada, require more specific standards. New York's SHIELD Act, while not specifically requiring particular measures, lists security controls that would create a "reasonable" security programme.

3.4 Key Multinational Relationships

Please see **1.4 Multilateral and Subnational Issues**.

4. KEY AFFIRMATIVE SECURITY REQUIREMENTS

4.1 Personal Data

Affirmative security requirements vary by sector and state, based on dozens of different laws. Please see **1.1 Laws** and **3.3 Legal Requirements**.

4.2 Material Business Data and Material Non-public Information

As discussed in **9.2 Public Disclosure**, public companies are required to disclose material cybersecurity incidents. This includes not only the theft of personal data but also other business data, to the extent access to or theft of such data would be material to the company.

Additionally, while most security statutes and data breach notification laws in the USA relate to personal information, the NYDFS regulation also applies to business information that would cause a material business impact to the covered organisation if subject to public disclosure. This provision is reflected in the model cybersecurity insurance law enacted in a growing number of other states as well.

4.3 Critical Infrastructure, Networks, Systems

CISA, created by the Cybersecurity and Infrastructure Security Agency Act, is the federal agency responsible for critical infrastructure protection. Other federal guidance has been issued respecting particular sectors, including the chemical, electrical and transportation sectors.

4.4 Denial of Service Attacks

Hackers responsible for denial-of-service attacks may be subject to criminal enforcement under US laws, including the CFAA. Businesses whose endpoints may be used by hackers to propagate these attacks may be subject to various security requirements; however, no victim (either the subject of the attack or a business whose systems were compromised to effect such an attack) has thus far been subject to enforcement action.

4.5 Internet of Things (IoT), Software, Supply Chain, Other Data or Systems

Internet of Things (IoT)

The California Internet of Things (IoT) Law, SB 327, became effective on 1 January 2020 and requires the manufacturer of a connected device to include reasonable security features that are appropriate to the nature and function of the device and the information it collects. The law provides that, for devices that authenticate outside of a local area network, it is a reasonable security feature if either any pre-programmed password is unique to each device or if a new means of authentication is generated before access is granted to the device for the first time.

Pursuant to the federal IoT Cybersecurity Improvement Act of 2020, the director of NIST will develop, in consultation with private industry, cybersecurity guidelines for all IoT devices used in government contracts.

Supply Chain

Recent security incidents, including breaches impacting Kaseya's remote monitoring and management tool and Microsoft Exchange, have re-emphasised the threat of supply-chain attacks. E.O. 14028 attempts to address this risk by requiring NIST to issue guidance identifying practices that enhance the security of the software supply chain. The guidance is to include procedures for providing a purchaser a Software Bill of Materials (SBOM) for each product. CISA also has within its mandate addressing supply-chain risk, and, in the defence sector, DFAR clause 239.730 authorises the Department of Defense (DoD) to manage supply-chain risk. The DoD may opt against using sources that do not meet its standards for managing supply-chain risk.

Other Data or Systems

Please see **1.1 Laws** and **1.2 Regulators**.

5. DATA BREACH REPORTING AND NOTIFICATION

5.1 Definition of Data Security Incident, Breach or Cybersecurity Event

All 50 US states, Washington, DC and three US territories have some form of breach notification law; no one standard exists for breach notification in the USA. In general, a security incident is potentially reportable if there is acquisition of personal information (specifically, see **5.2 Data Elements Covered**). In some states, access to personal information alone, without proof that the personal information was taken by an unauthorised actor, is sufficient to potentially trigger notification. Good faith but unauthorised access to or acquisition of personal data by an employee generally does not trigger notification.

Some federal sector-specific laws also require notification for certain security incidents and may sometimes override state rules. HIPAA, for example, may require notification in the event of a security incident impacting PHI and generally does not pre-empt state breach notification laws, although some states waive application of their data breach laws where HIPAA applies.

In March 2022, Congress passed the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA). CIRCIA will require organisations in certain critical infrastructure sectors to provide notice to the Department of Homeland Security in the event of a substantial cybersecurity incident, which could include ransomware and other attacks that do not directly involve data theft. Such organisations would also be required to provide notice within 24 hours of making a ransomware payment. Key details regarding notification will need to be addressed through agency rulemaking. The notification requirements will go into effect on dates prescribed in a final rule issued by the Director of CISA.

5.2 Data Elements Covered

The data elements covered by US state breach notification laws vary by state. Some states, such as Pennsylvania, focus principally on government or financial identifiers, potentially requiring notice where the first name (or first initial) and last name are compromised along with data elements such as social security number, driver's licence number, or financial account information together with the required security code that would allow access to a financial account. Increasingly, state breach notification laws are covering additional information, such as health or medical information, biometric information, as well as username and password combinations.

HIPAA covers PHI, which is health information processed by HIPAA-covered entities or their business associates, and includes individually

identifiable health information such as demographic data, medical histories, test results, insurance information and other similar information used to identify a patient or healthcare provider. Health information processed by vendors of personal health records not subject to HIPAA is captured by the FTC's Health Breach Notification Rule.

CIRCIA notification requirements will not turn on specific data elements, but instead the occurrence of a "substantial cyber incident," which will be defined through rulemaking but could include incidents such as denial of service attacks, ransomware, or exploits that do not necessarily involve the theft of personal or other sensitive data.

5.3 Systems Covered

Most US data breach notification statutes are agnostic as to the type of system potentially impacted, but instead turn on the type of data – whether it is in electronic or paper form and includes the elements described in **5.2 Data Elements Covered** about a resident of the state. Again, there are state-by-state variations. For example, 11 states potentially require notification in the event that paper, not just electronic, records are compromised.

HIPAA applies only to the systems of covered entities and their business associates.

5.4 Security Requirements for Medical Devices

The US Food and Drug Administration (FDA) is the primary regulator for medical devices, and works with federal government agencies, members of the private sector, device manufacturers and others to protect the security of medical devices.

The FDA has issued guidance on security requirements for medical devices and issues cybersafety communications if it identifies vulnerabilities that could pose risks to existing products. Device manufacturers are required to follow federal quality system regulations (QSRs), which include the obligation to address cybersecurity risks, and also to report to the FDA when their device may have caused or contributed to death or serious injury, or may have malfunctioned in a way that could cause death or serious injury in the future.

5.5 Security Requirements for Industrial Control Systems (and SCADA)

CISA has issued best practices for industrial control system cybersecurity, but it is focused primarily on critical infrastructure. In addition, sector-specific regulators for the various industries that depend on SCADA systems have set requirements for those particular industries. For example, the chemical industry, nuclear industry, and electrical industry each have separate cybersecurity rules promulgated by separate regulators.

5.6 Security Requirements for IoT

Please see **4.5 Internet of Things (IoT), Software, Supply Chain, Other Data or Systems**.

5.7 Requirements for Secure Software Development

Sector-specific and state laws and regulations address requirements for secure software development. Among the specific safeguards applicable to financial institutions subject to the FTC's safeguards rule and the NYDFS regulation is the requirement to adopt secure development practices. NIST has issued a Secure Software Development Framework as required by E.O. 14028.

5.8 Reporting Triggers

Reporting to individuals under US state breach notification laws turns on the unauthorised acquisition of – or in some cases, access to – certain data elements, as summarised in **5.1**

Definition of Data Security Incident, Breach or Cybersecurity Event and **5.2 Data Elements Covered**. Timing of notices varies by state and sector, with Colorado, Florida and Maine requiring notice within 30 days of discovery of the notifiable event, while the NYDFS requires notice in 72 hours and one banking agency (the FDIC) recently proposed a 24-hour notice requirement.

Reporting triggers to state regulators, typically the state attorneys general, vary widely by state, with some states requiring notice to attorneys general in the event that even one state resident's personal information is compromised, while others are triggered only when the number of individuals passes a certain threshold (California, for example, requires notification only if 500 or more of its residents are receiving notice), and some states (such as Michigan and Pennsylvania) do not require notice to regulators at all. As with individuals, the timing of notification varies by state, with many states requiring notification to regulators at or before the date notices are sent to individuals.

Some states require notification to credit reporting agencies (CRAs) in the event that a specified number of their residents are notified. For example, New York requires reporting to the big three CRAs – Equifax, Experian and TransUnion – in the event that 5,000 or more New York residents are to be notified. Increasingly, customer contracts will also include notification requirements, sometimes with time periods as short as 24–48 hours, or "immediately".

Under HIPAA, notification to OCR is required within 60 days of the end of the calendar year in which a breach is discovered for breaches involving PHI of fewer than 500 individuals and without unreasonable delay in matters involving more than that number (and in no event more than 60 days).

5.9 "Risk of Harm" Thresholds or Standards

Consideration of the risk of harm to individuals is the majority rule in the USA and is allowed in at least 30 of 50 US states, as well as under HIPAA, before notification is required.

When relying on risk of harm to assert that notice is not required, reporting of the rationale for the determination is required to the Attorney General under Florida and Vermont law, and record-keeping is required in several other states.

6. ABILITY TO MONITOR NETWORKS FOR CYBERSECURITY

6.1 Cybersecurity Defensive Measures

The Cybersecurity Information Sharing Act (the CISA) and ECPA permit companies to monitor network traffic for information security purposes and to adapt certain defensive measures. The CISA also provides liability protection for organisations conducting such monitoring or deploying such defensive measures on their systems in compliance with the Act. Defensive measures may not destroy, provide unauthorised access to, or otherwise harm information systems that do not belong to the private entity deploying the measures or another entity that has consented to the deployment of such measures.

Email monitoring is generally permissible where an employer has provided notice to and obtained the consent of its employees for such monitoring. Consent is considered valid even if the employee must consent or lose their job. Absent notice and consent, employees may assert tort law claims alleging that the employer violated their reasonable expectation of privacy in the emails, although such claims may be pre-empted by the CISA.

6.2 Intersection of Cybersecurity and Privacy or Data Protection

Privacy laws such as the CCPA have the potential to impact a business's ability to protect the security, integrity and confidentiality of its data and systems. For example, hackers may seek to fraudulently use certain data subject rights to gain access to personal information that could subsequently be used for phishing or other illegal purposes. That risk emphasises the need for organisations responding to such requests to have in place robust procedures for verifying the identity of individuals seeking to avail themselves of privacy rights.

With that said, the CCPA, and regulations adopted by the California Attorney General, take into account some cybersecurity risks. For example, under the CCPA, service providers are generally not allowed to use the personal information of California residents for purposes other than providing specified services to a business. Regulations issued by the California Attorney General, however, make an exception for uses to detect data security incidents or protect against illegal activities.

7. CYBERTHREAT INFORMATION SHARING ARRANGEMENTS

7.1 Required or Authorised Sharing of Cybersecurity Information

Certain federal agencies are required to disclose non-confidential threat intelligence information with the private sector. For examples of such disclosure obligations, please see **1.5 Information Sharing Organisations and Government Cybersecurity Assistance**.

Private organisations are generally not required to disclose threat intelligence information with regulators. However, companies may be required to provide access to other information to facilitate government cybersecurity investigations. For example, the Communications Assistance for Law Enforcement Act (CALEA) requires certain telecommunications organisations to create mechanisms for law enforcement to conduct certain approved surveillance activities. ECPA likewise anticipates certain lawful government requests for access to electronic communications. Additionally, E.O. 14028 requires the development of contract language applicable to federal contractors to ensure sharing of information related to potential cybersecurity incidents with their contracting agency.

7.2 Voluntary Information Sharing Opportunities

For examples of voluntary information sharing organisations, please see **1.5 Information Sharing Organisations and Government Cybersecurity Assistance**. The CISA also creates pathways for information sharing, including by exempting threat intelligence information from disclosure under the Freedom of Information Act (FOIA). E.O. 14028 has tasked the Office of Management and Budget (OMB) to develop Federal Acquisition Regulation (FAR) and the DFAR contract requirements that facilitate information sharing by federal contractors.

8. SIGNIFICANT CYBERSECURITY AND DATA BREACH REGULATORY ENFORCEMENT AND LITIGATION

8.1 Regulatory Enforcement or Litigation

The FTC and state attorneys general are some of the primary cybersecurity enforcers in the USA. The FTC in particular has played a key enforcement role, bringing hundreds of privacy and

security cases. Some key recent FTC enforcement action includes its USD5 billion 2019 settlement with Facebook that, among other things, required the social media giant to implement a comprehensive data security programme. In November 2020, the FTC settled an action with Zoom alleging deceptive statements regarding its security features, including that meeting recordings were encrypted when they could, in fact, remain unencrypted for up to 60 days before being transferred to a secure server.

State attorneys general also continue to play significant roles in enforcement. Among other recent settlements, state attorneys general – working together in a multi-state investigation and enforcement involving 43 state attorneys general – settled with Anthem for USD39.5 million over a 2014 data breach involving the records of approximately 80 million individuals, and entered a USD17.4 million settlement with Home Depot over that company's well-publicised 2014 payment card breach.

8.2 Significant Audits, Investigations or Penalties

Please refer to **8.1 Regulatory Enforcement or Litigation**.

8.3 Applicable Legal Standards

Regulators

As has been noted, regulators – including the FTC, other federal regulators, and state attorneys general – may seek to enforce unfair or deceptive acts and practices statutes, typically requiring a showing that a company made a false or misleading statement (potentially including through omissions) about its cybersecurity practices, or some general unfairness related to the same. Some other statutes enforced by regulators may include data breach notification statutes requiring notice within specified time frames, or security statutes generally requiring some form of reasonable security, though in the case of some statutes or regulations (eg, some rules applicable to financial institutions or state requirements in Massachusetts and New York) more specific security measures are required.

Private Plaintiffs

Private plaintiffs may pursue numerous theories in litigation related to the unauthorised access or access of personal information, including the following.

Contract

This requires proof either of an express contractual promise or an "implied contract" to protect personal information. The latter theory receives mixed treatment in the courts, with some courts finding that transactions do not carry with them promises to protect certain information, including payment card information, while others find a duty to protect certain sensitive information.

Tort/negligence

Private plaintiffs frequently allege that a breached organisation was negligent in failing to protect their personal information. To establish this allegation, plaintiffs must prove that the organisation had such a duty, and failure to do so is often a basis for dismissal. Some recent decisions have nonetheless found duties to protect certain sensitive information. For example, the Pennsylvania Supreme Court held in Dittman v UPMC that employers had a duty to protect their employees' sensitive personal information in some circumstances, while a trial court in Wisconsin has found the opposite in Reetz v Advocate Aurora Health.

Consumer protection statutes

As with regulators, private plaintiffs may sometimes bring claims alleging unfair or deceptive acts or practices. "Unlawfulness" may be an additional theory under such actions, requiring proof not of any false statement or general

unfairness, but instead the violation of a particular law.

Securities laws

Public companies (and their directors and officers) experiencing a data breach may also face allegations under various securities laws. These include derivative actions under which shareholders will assert that the directors and officers of a corporation breached their fiduciary duties by committing gross mismanagement, wasting corporate assets, or failing to adequately oversee corporate operations. These claims may often be dismissed, however, because plaintiffs must first establish either that they asked the board of directors to bring such a suit and the board wrongfully disagreed or found that it would be futile to make such a request.

Standing

One common defence to data breach lawsuits brought by private plaintiffs is that the plaintiffs lack "standing" – ie, that the suit is not properly presented before the court. In US federal courts, standing requires proof of, among other things, injury in fact, meaning the assertion of a cognisable injury to the plaintiffs. That injury must be sufficiently concrete; in other words, it must actually exist. The U.S. Supreme Court has held that a real risk of harm may satisfy that standard in some situations.

Since most individuals whose personal information is potentially accessed will suffer no such injury, however, plaintiffs have historically struggled to meet the requirements for standing. However, some more recent cases have begun to reverse that trend, and US courts are currently divided on the question.

8.4 Significant Private Litigation

Private litigation is a significant threat related to cybersecurity incidents in the USA, often relying on the causes of action described in **8.3 Applicable Legal Standards**. Some significant litigations include the following.

Equifax, one of the big three US credit reporting agencies, experienced a data breach impacting the records of approximately 150 million US individuals in 2017. Equifax faced both regulatory enforcement and private litigation. The agency settled these claims in a settlement of up to USD700 million. Separately, a class action alleging fraudulent statements in Equifax's public securities filings settled for USD149 million.

Yahoo! finalised its settlement in the consumer class action In re Yahoo! Inc. Customer Data Sec. Breach Litig. in August 2020. The settlement resolved the claims of approximately 194 million class members, requiring Yahoo! to pay USD117 million. The settlement covered several alleged data breaches occurring between 2013 and 2016. Separately, in 2019, the former directors and officers of Yahoo! agreed to a USD29 million settlement in a derivative action alleging that they had breached their fiduciary duties by failing to adequately protect customer data. The SEC also obtained a USD35 million penalty.

Anthem, Inc, settled a consumer class action relating to the alleged theft of some financial and medical records of up to 80 million individuals announced in 2015 for USD115 million. The company settled separately with regulators, including a settlement with HHS for USD16 million.

8.5 Class Actions

Class action lawsuits are a common feature of US cybersecurity litigation. In addition to some of the defences described in **8.3 Applicable Legal Standards**, including standing, a class action may be defeated where plaintiffs fail to prove all of the elements required for certification by the court. Among other things, certification of a class seeking monetary damages requires

proof that common questions of law and fact predominate, which can be difficult to prove where most class members will experience limited to no harm, with only a small number experiencing identity theft or other potential actual injury.

9. DUE DILIGENCE

9.1 Processes and Issues

Cybersecurity is an increasingly critical part of transactional diligence. Such diligence will assess cybersecurity risks applicable to the target as well as the administrative, technical and physical controls adopted to mitigate those risks. An initial step is to understand the categories and significance of the data the target collects and how they use and share such information. Personal data is always a focus, but other types of sensitive data such as confidential information, trade secrets and other business-critical data should not be forgotten. Diligence should also ascertain where such data is collected geographically to understand the particular obligations that may apply.

At the same time, equal weight is placed on the governance structures that are present (or absent) as an indicator of whether the company operationalises its policy commitments.

After conducting an initial assessment of the potential risks associated with the data a target collects and processes, diligence should be conducted on the security controls that are in place. Such diligence may include review of applicable policies and procedures implemented by a target, its governance structure, past data security incidents, audits or other past penetration tests, certifications, or other documented adherence to data security frameworks such as ISO 27001 or NIST.

The company's understanding and management of its third-party vendor cybersecurity exposures should also be a key aspect of cybersecurity diligence. A company that has substantial controls over the confidentiality, integrity and availability of data within its own network, but fails to analyse and address supply-chain and vendor risk, can present significant cybersecurity risk.

Depending on the risks associated with the data processing activities, the size of and other associated factors related to the transaction, a more detailed review may be appropriate, including a deeper dive by cybersecurity practitioners, typically directed by counsel, or even vulnerability scanning or penetration testing. Such forensic reviews are necessarily more intrusive and can be conducted pre-closing or post-closing, taking into account the level of risk.

9.2 Public Disclosure

Public companies are required to notify investors of material risks to their business. Guidance issued by the SEC in 2018, reinforced by public statements including a January 2022 speech by Chairman Gensler, specifically states that such material risks may include cybersecurity risks. Additionally, the SEC guidance notes the importance of timely disclosure regarding material breach incidents. Even where an incident is not considered material, a company should avoid disclosures implying that the company "may" experience breach incidents only in the future when it has already experienced non-material incidents in the past. Such past incidents, including any payment of ransom in response to a ransomware attack, should also inform the language of any risk factors contained in company disclosures as well as the presence of appropriate insurance protections.

10. INSURANCE AND OTHER CYBERSECURITY ISSUES

10.1 Further Considerations regarding Cybersecurity Regulation

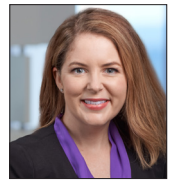
With significant business risks related to cybersecurity such as business interruptions caused by ransomware as well as regulatory and litigation risk, particularly in light of the active USA class action bar, many businesses in the USA turn to cyber insurance to reduce their potential exposures. Given the explosion of ransomware attacks and other cyberthreats, though, cyber insurers are adjusting their practices, in many cases raising their premiums and conducting more rigorous evaluations of a company's cybersecurity posture prior to binding a policy.

Cybersecurity is also now a national security issue for the USA, as noted throughout this chapter. Chris Inglis, a former Deputy Director of the National Security Agency, was confirmed as the first National Cyber Director, sometimes called the "cyber czar" in July 2021, which may well lead to enhanced federal co-ordination and focus on cybersecurity issues.

Ropes & Gray LLP is a leader in advising clients facing the rapidly evolving advances in technology that are increasing the value of data as an asset and raising the risks of cybersecurity threats and privacy. Its team of more than 50 attorneys across three continents provides services that fall into interrelated areas: the regulatory investigations and litigation team assists clients in responding to federal and state regulatory investigations and civil litigation arising from cybersecurity incidents and the collection, use and protection of consumer information; the corporate and transactional team guides clients on innovative deals where data is the primary asset, as well as data issues with respect to their acquisitions of companies across various sectors; the compliance and counselling team assists clients developing privacy and cybersecurity compliance programmes that support their global operations.

AUTHORS

Ed McNicholas is a partner and US leader of Ropes & Gray's data, privacy and cybersecurity group. Clients come to Ed with complex data, privacy and cybersecurity challenges, frequently during a major security incident that could materially impact the company. Ed also advises clients on the full range of federal, state and foreign privacy and data security requirements and has significant experience with investigations and class action litigation related to cybersecurity incidents. He is the lead editor of the "PLI Cybersecurity" treatise and a professorial lecturer in law at the George Washington University School of Law.



Fran Faircloth is a partner in Ropes & Gray's data, privacy and cybersecurity practice. She represents clients handling complex data, privacy and cybersecurity matters across a range of industries. Recently, Fran has advised clients on issues of data protection, cyber-attacks and contact-tracing technologies following the COVID-19 outbreak. Fran assists clients in privacy and cybersecurity-related class action litigation and enforcement actions by the FTC, state Attorneys General, the SEC and other government agencies. She also advises on difficult data privacy, cybersecurity and information law questions involving data breaches, ransomware, online brand protection, social media, e-commerce and internet governance.

Kevin Angle is counsel in Ropes & Gray's data, privacy and cybersecurity group. He represents a broad range of companies on privacy and cybersecurity matters, guiding clients through the existing patchwork of US federal and state laws as well as the EU's General Data Protection Regulation (GDPR) and other international laws. In that context, Kevin advises clients instituting comprehensive privacy and cybersecurity compliance programmes and on privacy and cybersecurity matters arising in corporate transactions. He also assists clients in responding to data-breach incidents, helping clients assess their legal obligations following a breach and respond to regulatory authorities.

Ropes & Gray LLP

2099 Pennsylvania Avenue NW
Washington, DC 20006
USA

Tel: +1 202 508 4779
Fax: +1 202 383 8349
Email: edward.mcnicholas@ropesgray.com
Web: www.ropesgray.com

Trends and Developments

Contributed by:
Ed McNicholas, Fran Faircloth and Kevin Angle
Ropes & Gray LLP see p.31

Introduction

Cybersecurity concerns increasingly pervade all sectors of the US economy – from nation-state threats impacting US national security, all the way down to commodity phishing scams and revenge porn affecting individuals. As a result, US policymakers at the federal, state and even local level are increasingly focused on enhancing cybersecurity defences.

The Biden administration has made cybersecurity a top priority, deploying many of the tools available to the federal government – from law enforcement to diplomacy – to deter cyber-aggression, update standards applicable to federal agencies, and encourage or even require information-sharing by agencies, federal contractors and others. Meanwhile, business leaders, up to and including corporate boards, are likewise making cybersecurity a key priority, consistently ranking cybersecurity as one of their top concerns.

Despite these measures, the advance of cybersecurity laws continues to trail the development of new threats, as the US continues to adhere to a largely voluntary, sector-based system, as opposed to mandating baseline technical and organisational measures through clear statutory or regulatory action.

Security Threats: 2021 and Beyond

The focus on cybersecurity is driven by the explosion of attacks affecting individuals and organisations across the USA. Incidents such as the Colonial Pipelines ransomware attack – in which hackers (and the public's reactionary purchases of gasoline) managed to disrupt fuel supply across the US east coast – grab headlines, but many incidents that do not garner such public attention still have a profound impact on their victims, whether government, businesses or individuals. Some notable threats include the following.

Ransomware

Ransomware continues to dominate the US threat landscape, with ransomware payments in 2021 nearly doubling in value from 2020, according to one metric. The problem was so pervasive that it was declared a "direct threat" to the US economy by the US Treasury Department. Ransomware payments themselves account for only a small part of ransomware's impact on US businesses. Costs also include remediation, lost business and other reputational harms. In many cases, ransomware threat actors will now also attempt to steal data (or claim to have done so). As a result, organisations experiencing an attack must analyse their obligations under the panoply of US breach notification laws, whose precise requirements vary from state to state and depend on the type of data potentially impacted.

Businesses affected by ransomware must also make key decisions promptly after an attack, such as when and how to restore systems and, of course, whether or not to pay the ransom. Those decisions are complicated by US regulatory requirements prohibiting payments that violate the US sanctions regime. In September 2021, the US Department of the Treasury's Office of Foreign Assets Control (OFAC) issued an Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments, making the point that businesses will potentially be subject to strict liability for payments in violation of that regime (although we note that no known

enforcement has actually taken place). The US Securities Exchange Commission has also suggested that the fact that a company has paid a ransom in the past may be a material consideration for investors, requiring disclosure by public companies in their securities filings.

Business email compromise

Business email compromise remains one of the most persistent and effective cyber-attacks impacting organisations. In 2020 alone, the US Federal Bureau of Investigations (FBI) estimates there were USD1.8 billion in losses associated with business email compromise events reported to its Internet Crime Complaint Center (IC3). Such attacks are often associated with wire fraud, but organisations experiencing a compromise must also assess the risk that sensitive data was accessed, often leading to breach notifications to individuals, regulators or other third parties. Risks associated with these attacks reinforce the need for best practices in email management – that is, ensuring that multi-factor authentication is in place, sensitive data is not sent or stored without encryption, and that mailboxes are periodically cleaned out.

Supply chain attacks/risk

The year 2021 began with businesses still reeling from a supply-chain attack linked to the Russian government, and closed with them scrambling to assess and remediate the Log4j vulnerability associated with widely utilised software code. Supply-chain risk is here to stay, requiring businesses and government to take note. If they have not done so already, US businesses should put in place procedures for assessing their supply chain: how will a software solution or vendor affect the overall risk profile of the organisation, and what steps are required to mitigate such risk? As described further below, the federal government is taking action to help businesses review an SBOM (software bill of materials), and adopt other specific solutions, but the effective implementation of those measures is still some way off. In the meantime, businesses are left on their own to conduct diligence and ensure that adequate contractual protections are in place.

Insider threats

Sophisticated intellectual property and financial theft continues to be facilitated by complex schemes involving rogue insiders. The losses arising from such schemes are often significant and point to the need to monitor traffic leaving a business's perimeter, constantly monitor employee activity – consistent with applicable requirements regarding transparency and consent – tightly limit administrator access, and segment network access to limit the reach of potential insider threats. The Cybersecurity Information Sharing Act permits companies to monitor certain network traffic for cybersecurity purposes and to implement defensive measures on their systems.

Federal Initiatives

To combat the numerous threats to the security, integrity and availability of IT systems and data, the US federal government has launched a host of initiatives. These range from diplomatic efforts to agency guidance, and include new uses of existing laws to enforce cybersecurity standards. In one effort to enhance cybersecurity at government contractors, for example, the Department of Justice recently announced its intent to use the federal False Claims Act (FCA) to pursue cybersecurity-related fraud, noting also the FCA's qui tam whistle-blower provisions that allow company insiders with knowledge of wrongdoing to initiate suits alleging FCA non-compliance on the government's behalf. Some other notable developments at the federal level are described below.

Executive Order 14028

Early this year, the Biden administration issued Executive Order 14028 (E.O. 14028), which fol-

lows the pattern of Executive Orders from President Obama and President Trump in relying on the federal government's purchasing power and ability to impose terms on its contractors and the vendors of government contractors – which, no doubt, covers a substantial percentage of US companies. E.O. 14028 aims to:

- improve information-sharing by federal contractors by removing contractual terms potentially restricting such sharing and requiring disclosures of security incidents to agencies potentially affected by them;
- increase cybersecurity requirements for agencies and vendors that contract with them, including through the implementation of zero trust principals;
- establish a cyber-safety review board with participants from both government and the private sector that would be convened following a cybersecurity incident (similar to the National Transportation Safety Board, NTSB, which does so following an airline accident or significant accident in other modes of transportation);
- setting a standard incident response protocol for federal agencies through the release of incident response playbooks, which were published by CISA in November; and
- prioritising early detection and remediation of cybersecurity risks.

Some of these initiatives are self-implementing, but many require further agency action, with developments expected in the coming year. To address software supply chain vulnerabilities, for example, E.O. 14028 tasks the National Institute of Standards and Technology (NIST) with developing a secure software development framework, which was released in February 2022. Likewise, NIST is taking comments on proposals related to internet of things (IoT) security and a Software Bill of Materials (SBOM). Many of the standards expected to be developed are directly applicable only to federal agencies or contractors, but contractors will often need to require similar terms of their vendors, and so a significant sector of the private sector may well be impacted by these efforts, either contractually or through establishment of industry "best practices" going forward.

Cybersecurity and Infrastructure Security Agency (CISA) and federal breach notification

While the FBI continues to serve a key role in mediating between national security, the intelligence community and civilian cybersecurity, CISA appears to be attempting to assert its role in "quarterbacking" (ie, co-ordinating) cybersecurity, both at the agency and executive branch level and for critical infrastructure industries. By critical infrastructure, CISA means not only "brick-and-mortar" infrastructure, but also other key industries such as financial services and healthcare. CISA has developed, and is expecting to continue developing, tools to promote information-sharing, both within government and with the private sector.

Breach notification: CISA

To that end, in March 2022, Congress passed a new security breach notification law, the Cyber Incident Reporting for Critical Infrastructure Act of 2022, requiring certain organisations in critical infrastructure sectors to report substantial cyber incidents and ransomware payments to the Department of Homeland Security within 72 and 24 hours respectively. The requirement will become effective on a date to be determined through federal agency rulemaking, as will many of the details of the notification requirement.

The Director of CISA is required to issue rules delineating, among other things, which organisations are required to submit incident reports, when and how to do so, and what information to include. The reports will include, at a minimum, if available:

- a description of the function of the affected information systems or devices;
- a description of any unauthorised access;
- the estimated date range of the incident; and
- the incident's impact on the operations of the covered organisation.

The law will provide protections for information submitted in such breach reports. Regulators would be prohibited from using the information in regulatory enforcement actions, and the information would receive protections against certain disclosures under the Freedom of Information of Information Act and through civil discovery. Disclosure would also be deemed not to waive the attorney-client privilege, to the extent applicable. The scope and validity of many of these protections could nevertheless be challenged by enterprising plaintiffs' attorneys, and so disclosure would not be without some risk. Many of these protections would also not apply to the extent an organisation submitted information in response to a subpoena authorised by the law, rather than through voluntary compliance.

Even without new laws, some federal agencies appear poised to more strictly enforce existing breach notification requirements. The Federal Trade Commission's (FTC's) Health Breach Notification Rule was first issued in 2009. Recently, though, it has gained renewed attention. In 2020, the FTC sought public comment on the rule; in September of last year, it issued a policy statement asserting that the makers of health apps, connected devices and other similar products are "vendors of personal health records" mandated to comply with the rule requiring notice to affected individuals, the FTC and, in some cases, the media in certain breaches involving health information and entities not subject to HIPAA. Only recently, the FTC followed up with a set of FAQs. Expect guidance is to be followed by action: the rule carries stiff potential penalties for violations of up to USD43,792 per violation.

Federal banking regulators, meanwhile, have also recently updated their notification rule to require that certain "banking organisations" notify their primary federal regulator of a notifiable security incident within 36 hours of their determination that the incident has occurred. Just recently, the SEC announced a proposed rule that would establish new cybersecurity standards applicable to regulated entities and require reporting of "significant" cybersecurity breaches affecting a registered investment adviser or the adviser's fund or private fund clients.

FTC cybersecurity rulemaking?

While CISA plays a key co-ordinating role, it currently does not function as a federal cybersecurity regulator – that role is assumed by various agencies, depending on the industry sector in question. The Federal Trade Commission, though, has long assumed the leading role in enforcing cybersecurity standards. Traditionally, it does so by enforcing the general prohibition under Section 5 of the FTC Act against unfair and deceptive acts and practices, which the FTC interprets to require reasonable security measures. However, this past year, the US Supreme Court removed a key arrow from the FTC's enforcement quiver in AMG Capital Management LLC v FTC, in which the Court held that the FTC may not seek equitable relief in the form of disgorgement or restitution – the FTC's traditional path to pursuing monetary relief – without first issuing a specific rule. Absent such rules, the FTC may still pursue injunctive remedies (ie, requirements that a business violating Section 5 live up to certain promises or change behaviour), but it cannot assess a fine.

Perhaps as a result, the FTC is now considering rulemaking to "curb lax security practices"; doing so would allow it to seek monetary redress on behalf of consumers. A federal cybersecurity rule could also help to better define the minimum cybersecurity standards companies must

meet. The contours of any such rule are yet to be determined – the FTC has not even issued a draft. The FTC is likely to hold workshops, informal hearings and grant other opportunities to comment on their proposals. Expect further developments in the year to come.

Financial institutions

Federal financial regulators also appear poised to update decades-old cybersecurity rules. The Securities Exchange Commission (SEC) has long been active in the cybersecurity space. Its Office of Compliance Inspections and Examinations (OCIE) has included cybersecurity in its annual examination priorities and compliance sweeps since 2015, and has issued guidance related to its findings. The SEC's core cybersecurity rule, though, Regulation S-P, which is applicable to broker-dealers, investment companies, and investment advisers, has not changed since the early 2000s.

In a recent speech, the SEC's Chairman Gensler suggested that the time has come to expand on the rule, and in early February the SEC issued a proposed rule that would amend its disclosure regime and push advisers to consider their cybersecurity risks, including considerations of multi-factor authentication and least privilege/zero trust concepts. In his speech, Chairman Gensler also noted other SEC rules relevant to cybersecurity that he considers due for an update, such as Regulation SCI, applicable to stock exchanges, clearing houses, alternative trading systems and other large registrants, and so further developments in the area of financial services cybersecurity are possible.

The FTC also recently updated its own safeguards rule applicable to certain financial institutions not subject to SEC oversight (or regulation by another federal functional regulator). Coming into full effect in December 2022, the update includes specific security controls such as multifactor authentication, along with various governance and accountability measures.

Evolving State Laws

States are often referred to as the laboratories of democracy in the USA, and that is certainly true when it comes to privacy and cybersecurity regulation. While efforts to adopt comprehensive data protection legislation have stalled at the federal level, states – including California, Colorado and Virginia – have adopted robust privacy laws. State bills are also under consideration in numerous other states with such diverse political climates as Florida, Indiana, Massachusetts, New York and Oklahoma. Some of these bills include novel privacy concepts such as the creation of data fiduciaries. Some key state law cybersecurity developments are as follows.

CCPA litigation

One key feature of the California Consumer Privacy Act (CCPA), which went into operation in 2020, is its private right of action available in the event of data breaches impacting specified categories of personal information that were caused by failures to adopt reasonable security procedures. Critically, this right of action carries statutory damages of up to USD750 per person – a strong incentive for enterprising plaintiffs' attorneys. While the predicted tsunami of CCPA breach litigation has not yet come to pass, plaintiffs' attorneys have filed numerous claims. Courts have also begun to address some of the CCPA's ambiguities. In one recent decision, for example, a federal judge rejected the argument of the defendant, Blackbaud, that it was acting as a "service provider" in storing its customers' information and not as a "business" directly subject to the CCPA's security requirement. In doing so, the court relied in large part on Blackbaud's decision to register as a "data broker" under California law.

Heading into 2023, one important change brought about by the California Privacy Rights Act (CPRA), which expands on the CCPA's privacy protections, is its clarification that the implementation of new security or data breach notice procedures will not "cure" a data breach.

Data protection assessments

New US state privacy laws also seem to be adopting and adapting the European concept of data protection assessments. Both the Virginia Consumer Data Protection Act (VCDPA) and Colorado Privacy Act (CPA) incorporate the requirement in relation to the processing of sensitive data, and the CPRA authorises regulations requiring businesses whose data processing presents significant risk to consumers' privacy or security to conduct a cybersecurity audit.

Data fiduciaries

Legislators in US states have also begun to incorporate concepts imported from traditional fiduciary duties within privacy legislation. The CPA describes some of its privacy principles such as data minimisation as "duties", and includes the traditional "duty of care" – in this case, framed as the duty to provide reasonable security. Going one step further, a proposed bill in New York and an earlier draft of a bill in Massachusetts (which could be resurrected, at least in part) would create duties of care, loyalty and confidentiality with respect to personal data. How those concepts would play out in the context of data protection would need to be tested in practice.

Conclusion

With many bills pending and new proposals under consideration, it remains to be seen where US state data protection legislation will head. Businesses should be mindful, though, of the evolving nature of state laws and the need to stay abreast of new requirements. Congress also remains active in addressing cybersecurity risks, as highlighted by the recent, rapid passage (at the time of publication of this article) of the Cyber Incident Reporting for Critical Infrastructure Act, at least partly in response to the recent conflict in Ukraine. Federal regulators and standards organisations will continue to respond to developments as they occur.

Ropes & Gray LLP is a leader in advising clients facing the rapidly evolving advances in technology that are increasing the value of data as an asset and raising the risks of cybersecurity threats and privacy. Its team of more than 50 attorneys across three continents provides services that fall into interrelated areas: the regulatory investigations and litigation team assists clients in responding to federal and state regulatory investigations and civil litigation arising from cybersecurity incidents and the collection, use and protection of consumer information; the corporate and transactional team guides clients on innovative deals where data is the primary asset, as well as data issues with respect to their acquisitions of companies across various sectors; the compliance and counselling team assists clients developing privacy and cybersecurity compliance programmes that support their global operations.

AUTHORS

Ed McNicholas is a partner and US leader of Ropes & Gray's data, privacy and cybersecurity group. Clients come to Ed with complex data, privacy and cybersecurity challenges, frequently during a major security incident that could materially impact the company. Ed also advises clients on the full range of federal, state and foreign privacy and data security requirements and has significant experience with investigations and class action litigation related to cybersecurity incidents. He is the lead editor of the "PLI Cybersecurity" treatise and a professorial lecturer in law at the George Washington University School of Law.

Fran Faircloth is a partner in Ropes & Gray's data, privacy and cybersecurity practice. She represents clients handling complex data, privacy and cybersecurity matters across a range of industries. Recently, Fran has advised clients on issues of data protection, cyber-attacks and contact-tracing technologies following the COVID-19 outbreak. Fran assists clients in privacy and cybersecurity-related class action litigation and enforcement actions by the FTC, state Attorneys General, the SEC and other government agencies. She also advises on difficult data privacy, cybersecurity and information law questions involving data breaches, ransomware, online brand protection, social media, e-commerce and internet governance.

Kevin Angle is counsel in Ropes & Gray's data, privacy and cybersecurity group. He represents a broad range of companies on privacy and cybersecurity matters, guiding clients through the existing patchwork of US federal and state laws as well as the EU's General Data Protection Regulation (GDPR) and other international laws. In that context, Kevin advises clients instituting comprehensive privacy and cybersecurity compliance programmes and on privacy and cybersecurity matters arising in corporate transactions. He also assists clients in responding to data-breach incidents, helping clients assess their legal obligations following a breach and respond to regulatory authorities.

Ropes & Gray LLP

2099 Pennsylvania Avenue NW
Washington, DC 20006
USA

Tel: +1 202 508 4779
Fax: +1 202 383 8349
Email: edward.mcnicholas@ropesgray.com
Web: www.ropesgray.com

Chambers Guides to the Legal Profession

Chambers Directories are research-based, assessing law firms and individuals through thousands of interviews with clients and lawyers. The guides are objective and independent.

practiceguides.chambers.com