AMERICAN BANKRUPTCY INSTITUTE

2018 Winter Leadership Conference

Cybersecurity in 2019: How Protected Are You?

John G. Loughnane, Moderator
Nutter McClennen & Fish LLP; Boston

Cliff Dutton
Epiq; New York

David Fisher
Integra, Inc.; Denver

Rebecca Fruchtman
Bank of America Merrill Lynch; Chicago

Elizabeth B. Vandesteeg
Sugar Felsenthal Grais & Helsinger LLP; Chicago

CONCURRENT SESSION

2018

Cybersecurity 101

SFGH
Sugar Felsenthal Grais & Helsinger LLP

What types of information and data do all companies need to protect?

- Personally identifiable information (PII): information that can be linked to a specific individual
  - Includes name, birthdate, social security number, driver's license number, account numbers
- Non-personally identifiable information: cannot by itself be used to identify a specific individual
  - Aggregate data, zip code, area code, city, state, gender, age
- Gray area – "anomyzed data"
  - Non-PII that, when linked with other data, can effectively identify a person
  - Includes geolocation data, site history, and viewing patterns from IP addresses

What Data Must Be Protected?

- Personally Identifiable Information (PII)
  - Social Security number
  - Drivers license number
  - Credit/debit card numbers
  - Passport number
  - Bank Account Information
  - Date of Birth
  - Medical Information
  - Mother's maiden name
  - Biometric data (i.e., fingerprint)
  - E-mail/username in combination with password/security question & answer

What Data Must Be Protected?

- Payment Card Information (PCI)
  - Primary Account Number (PAN)
  - Cardholder Name
  - Expiration Date
  - Service Code (3 or 4 digit code)
  - PIN

What Data Must Be Protected?

- Business Information
  - Customer lists
  - Prospect lists
  - Trade secrets
  - Pricing information
  - Business plans and strategies
  - Employee lists

Why do we need to protect it?

- Data is a corporate asset
- Corporate data is at a higher risk of theft or misuse than ever before

Numerous Applicable Laws/Regulations

- Massachusetts Standards – 201 C.M.R. 17
- Gramm-Leach Bliley
- HIPAA
- Fair Credit Reporting Act (FCRA)

Top 10 Passwords Discovered in Data Breaches in 2016

1. 123456
2. password
3. 12345678
4. qwerty
5. 12345
6. 123456789
7. football
8. 1234
9. 1234567
10. baseball

Primary Types of Privacy Incidents

- Physical loss: Stolen or lost laptop, PDA, thumb drive, or other portable media containing PII or other sensitive data

- Mitigation
  - Encrypt
  - Prohibit/minimize/block saving PII on portable media
  - Records management

Primary Types of Privacy Incidents

- Hard copies: mis-mail, misplaced, stolen, or "disposal fail"

  - Mitigation
    - Handling policy and training
    - Disposal policy and training
    - Diligence/contracts with records management/disposal vendors

Primary Types of Privacy Incidents

- Unintended Disclosures
  - "computer glitch"
  - Incorrect permission settings
  - Misdirected email/fax

    - Mitigation
      - Regular systems and/or vulnerability testing
      - Encrypt or password-protect files
      - Outlook delay

Primary Types of Privacy Incidents

- Vendors: negligence, physical loss, database/server breach or stolen data at a vendor's location or server
  - Increases response costs about 20%

    - Mitigation
      - Vendor contract provisions
      - Appropriate review of vendors to confirm safeguards are in place

Primary Types of Privacy Incidents

- Stolen Data by Otherwise Authorized Users: rogue employee or other malicious insider with access downloads or sends personal or sensitive data to another unauthorized location for an improper purpose

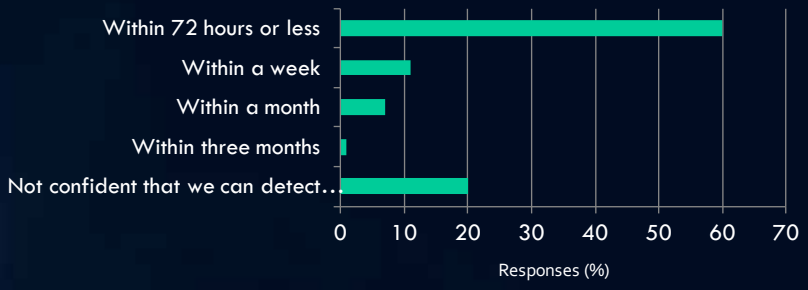
- Mitigation
  - Systems activity review – logging and periodic monitoring
  - Access reviews

Primary Types of Privacy Incidents

- Database/server breach: Unauthorized person accesses or hacks into a data server that stores personal or other sensitive data
  - Malware, hackers, phishing, ransomware

- Mitigation
  - Penetration testing, firewalls, intrusion detection, etc.
  - Systems activity review – logging and periodic monitoring
  - Training of employees

Companies are Still Too Optimistic About Ability to Detect an Attack



*Information from Tripwire Breach Detection Survey, http://www.tripwire.com/company/research/us-retail-survey/

Victims by the Numbers

Adapted from Mandiant's *MTrends Beyond the Breach: 2015 Threat Report*

Reputational Harm

- Consumer Study on Data Breach Notification
  - 62% said breach notification decreased trust and confidence in the organization
  - 15% would terminate their relationship with the notifying company (39% would consider terminating)
  - 94% believe reporting organization is solely to blame for breach
  - 72% thought organizations do a poor job communicating and handling a data breach

(Source: Ponemon Institute & Experian Data Breach Resolution)

What must companies do to protect it?

- Compliance with state, local, federal laws and regulations
- Contracts with third parties
- Privacy policies for website users
- Privacy audits
- Business may have more PII than it is thinking of

What is a Data Breach?

- Definition varies from state to state, but typically includes:
  - Unauthorized acquisition/access/use
  - Of Personally Identifiable Information (PII)
  - Unencrypted
  - Compromising the security, confidentiality or integrity of PII
  - Does not include good faith acquisition of PII

What is a Data Breach?
(That may trigger state notification laws)

- Unauthorized acquisition of PII that compromises the security, confidentiality or integrity of PII…
  - That results or could result in identity theft or fraud (OH)
  - Unless PII is not used or subject to further unauthorized disclosure (NE)
  - Unless no misuse of PII has occurred or is not reasonably likely to occur (NJ)
  - Unless no reasonable likelihood of harm to consumer whose PII was acquired has resulted or will result (CT)

What is a Data Breach? (That may trigger state notification laws)

- Unauthorized acquisition of PII that compromises the security, confidentiality or integrity of PII…
  - That has caused or is likely to cause loss or injury to resident (MI)
  - That causes or is reasonably likely to cause substantial economic loss to the individual (AZ)
  - Unless no reasonable likelihood of financial harm to consumer whose PII was acquired has resulted or will result (IA)

Why we should be careful with the word "breach"

- Using "breach" to describe a data-privacy related incident assumes the incident meets the definition of a security breach which triggers various notification requirements
- An "incident" does not always rise to the level of "breach" (i.e., encryption safe harbor)
- "Incident" is better received by the public than "breach"

Breach Notification Laws

- State laws differ with respect to:
  - Deadline for notifying (14, 30, 45 days; reasonable time)
  - Notification to Attorney General
  - Notification to other State agencies
  - Including Attorney General contact information
  - Substitute notice (email, website, media)
  - Specific facts of incident and type of PII compromised
  - Maintaining records of incident (for 3-5 years)
- Countries also differ with notice requirements

National Institute of Standards and Technology (NIST) Framework

- Identify: develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities
- Protect: develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services
- Detect: develop and implement the appropriate activities to identify the occurrence of a cybersecurity event
- Transfer: develop and implement appropriate insurance program that deals with cyber and privacy events
- Respond: develop and implement the appropriate activities to take action regarding a detected cybersecurity event
- Recover: develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event

Proactive Measures

- A Written Information Security Program (WISP): required by Massachusetts law, GLBA, and FTC Red Flags Rule
- Incident Response Plan: required by PCI DSS, GLBA, and HIPAA
- Carefully drafted Confidentiality Agreements for employees, vendors, and visitors
- Proper and ongoing training for employees on company's data security programs & cyber awareness
- Perform a data privacy review & risk assessment, including penetration testing
- Review your employee exit process

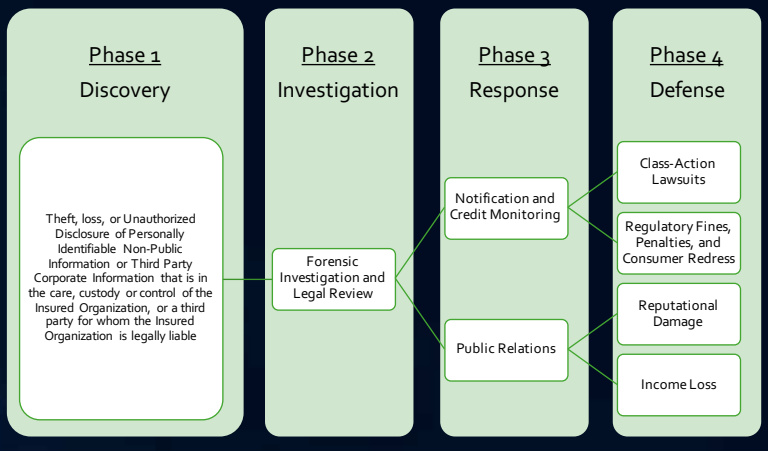
Who Should Be On Your Incident Response Team?

- Because the issue impacts almost every component of the organization, and failure to properly manage can result in both long and short term consequences, the team should include "C" level decision makers in the following areas:
  - Legal
  - IT
  - Risk management/insurance
  - HR
  - Marketing
  - Public relations
  - Compliance & internal audit
  - Physical security
  - Other executive, as appropriate
  - Third party response services (e.g., forensics, privacy counsel, notification)

Vendor Agreements

- Compliance with data privacy standards for the protection of PII, PHI, and/or PCI
- Return or destruction of PII, PHI, and/or PCI
- Use of subcontractors with access to PII, PHI, and/or PCI
- Notice of security and/or privacy incident within ____ hours
- Indemnification
- Cyber liability insurance

A Simplified View of a Data Breach Response Methodology



This chapter is from the upcoming American Bar Association Business Law Section book Guide for In-House Counsel: Practical Resource to Cutting-Edge Issues, to be published in early 2019.

Chapter 5

Cyber Security and Protecting Data Privacy

By Steven P. Seltzer, Esq., John G. Loughnane, Esq., and Susan N. Goodman, RN JD

Every day the national news includes a story about a company, application, or service that has suffered a data breach. It is a common occurrence, so companies must take steps to protect and respond to these events. Protection begins with understanding those laws and regulations affecting data privacy, and developing a privacy compliance program to minimize data security risks. This chapter will educate the reader on data privacy, cyber security, breach risk, breach mitigation, and the steps necessary to prepare for and respond to data security incidents and/or breaches.

Electronic transmission and storage of data has become a part of everyday life, both commercially and personally. Most individuals have certainly moved well beyond the mere carrying of a smart phone or swiping of a credit card and now drive vehicles that are full of electronic "syncing" options; track health and fitness information either through an app, a wearable, or both; and pay bills or transfer money through the assistance of an app. Digitization is equally as pervasive in business. Legal counsel representing clients in industries subject to data privacy laws and regulations are required to understand and stay informed on what has become an ever-evolving data privacy landscape. Data compromise has become an equally pervasive theme for many industries. Accordingly, cybersecurity and data breach awareness is clearly a priority issue for counsel, especially in-house counsel. With emphasis on in-house generalists, this chapter provides an overview of how to develop an effective data privacy program, address ongoing risks, and prepare for and mitigate security incidents. Both legal and general media outlets have reported many data breaches in recent years, making it unnecessary to rehash them. No business—whether large or small—is immune from the risk. Although massive breaches like the one reported by Equifax in 2017 gain big headlines, there are many more that escape publicity.

Not surprisingly, data privacy and cybersecurity laws and processes overlap. In fact, what is often thought of and discussed as cyber security inherently includes development of data privacy processes to minimize data security breaches. Effective data security programs require engagement and integration throughout various levels of the organization. The best IT/data security team cannot effectively keep any organization's data secure without the engagement of organizational leadership, end-user employees, compliance professionals, vendors, and, ultimately, the board of directors. Organizations often have competent teams covering each of these areas, yet fail to effectively integrate the communication, policies, training, and incident response responsibilities cross-functionally.

Further, although organizations must have robust sanction policies to deal with process-and-procedure violations, overly harsh or punitive approaches to security incidents/breaches may simply cause staff to refrain from reporting incident and/or breaches, fearing immediate termination. In response, some organizations have incorporated specific analytical frameworks for assessment of compliance concerns into organizational handbooks or conduct codes to improve expectation transparency and, hence, compliance engagement at the employee level.

In-house counsel is particularly well-situated to pull together the various aspects necessary for the development and execution of an effective data privacy and cybersecurity program. Rule number one is to acknowledge that data privacy and cyber security is not just an IT issue. Whether discussing prevention efforts or dealing with a real or suspected breach, the legal department is front and center. Remember, it's not IT that will be talking to regulators or defending against threatened or actual litigation. However, it is still important for you, as in-house counsel, to know your IT partners well. You must meet regularly with your IT department and have at least a working understanding of their security efforts and processes. Your IT

department must know you well and feel comfortable calling you as soon as an issue (or even potential issue) arises. If you work inside a smaller company without a significant IT staff, maintaining a solid relationship with the IT vendor who services your computer systems would be helpful, allowing the vendor to come in on short notice without having to learn your business and systems from scratch.

You will also need support and serious buy-in at all levels of your organization—from employees to senior management, all the way up to the CEO. You might enlist support from the CEO by reminding him or her that in the event of a data breach, he or she is likely to be the star witness in any litigation or regulatory investigation (whether or not you have a public-relations spokesperson) and will want to demonstrate the company's robust breach prevention and readiness efforts. If you work in a public company, the board may also have responsibilities to stay informed and ask questions about the company's cybersecurity protection programs. Indeed, regulatory agencies such as the SEC and HHS are taking more interest in companies' cybersecurity risk management and governance, as well as disclosure of cybersecurity preventive programs and actual incidents, making board and C-level awareness imperative.

For example, in 2013 and 2014 an unauthorized third party stole credentials to over one billion Yahoo accounts, but disclosure of those incidents did not occur until December 2016.[1] The outcry that followed was tremendous and included the filing of 43 consumer federal and state class actions, a stockholder class action based on sections 10(b) and 20(a) of the Securities Exchange Act of 1934, four stockholder derivative actions, and investigations by the SEC, FTC, and the U.S. attorney and state attorneys general offices.[2]

Yahoo's 2016 10K noted the resignation of its general counsel as a "management change" adopted in response to the findings of Yahoo's data breach independent committee.[3]

The independent committee found "that (i) the 2014 Security Incident was not properly investigated, managed and communicated internally at the time, so that the Company was not adequately advised with respect to the legal and business risks associated with the incident and (ii) the Audit and Finance Committee and the full Board were inadequately informed of the full severity, risks, and potential impacts of the 2014 Security Incident."[4]

Uber experienced a cyber attack in 2014 compromising 50,000 names and driver's licenses of Uber drivers.[5] However, it was the handling of a 2016 breach that resulted in employment ramifications. In November 2017, Uber disclosed that hackers had stolen 57 million driver and rider accounts in the 2016 breach.[6] The disclosure indicated that two company employees, the chief security officer (who reportedly also held the title "deputy general counsel") and the security and law enforcement legal director, had complied with the hackers' ransom, paying $100,000 in exchange for the hackers' promise to delete the compromised data and keep the breach to themselves.[7] Uber did not report the breach in a timely fashion, resulting in adverse legal and media responses. The CSO was subsequently asked to resign, and the director was terminated.[8] These breach incidents make clear that in-house counsel all the way up to the general counsel can and will be held responsible for known data breaches when not investigated and managed properly.

Data breaches in the healthcare sector have also been large and well-publicized. Anthem Blue Cross Blue Shield represented the largest settlement for a breach of protected health information (PHI) under HIPAA with a settlement of $115 million.[9] Anthem was hacked in February 2015, during which the information of approximately 79 million insureds was compromised.[10] Anthem was aware of flaws in its cybersecurity system in 2013 and failed to proactively address them, allowing hackers to access extensive information, including names,

birthdates, Social Security numbers, addresses, and e-mail, employment, and income information.[11] As part of the settlement agreement, Anthem agreed to offer each affected person two years of credit monitoring and reimbursement for breach-related expenses.

Regardless of the size of your company, you should have—or may be required to have—an incident response plan ready to go. Notice it is not only a "breach" response plan, given that the company must react when a cyber or data situation occurs even before knowing whether it qualifies as a breach. You need trusted outside counsel on call, preferably someone who knows your business and is generally familiar with your IT department personnel (and/or IT vendor) and systems. You want to avoid the panic of having to find and retain counsel in the heat of a cybersecurity incident. This means investing time and expense to allow your outside counsel to meet with you and your IT colleagues to learn about your company's systems and technology processes, and ensuring your counsel has information security and/or cyber forensic vendors who can be called in quickly.

Now it is time to get into the details. This chapter consists of five parts. Part I provides a summary of various threat sources and attacks that routinely and persistently challenge organizations of all sizes. Part II sets forth a high-level summary of the legal framework governing data privacy and cybersecurity issues in the United States. Part III discusses essential elements of corporate resilience, including the need to foster an internal culture of security, the importance of an interdisciplinary approach, techniques for managing vendor relationships, considerations for corporate partnerships and acquisitions, and securing adequate and appropriate insurance to cover risks. Part IV focuses on designing, testing, and updating an incident response plan as required by various laws and as a matter of essential planning. This section will also address handling an actual breach situation. Finally, Part V presents a summary list of

recommendations for in-house counsel to consider when tackling data privacy and cybersecurity issues.

I. Threat Sources

The most likely source of a data breach comes from within your organization. You may find yourself dealing with an employee who simply made a mistake or fell victim to a scam, not to mention a disgruntled employee or former employee who intends to do harm. Indeed, there are big, bad foreign hackers out there, both state sponsored and part of organized crime, but an internal act is more likely the cause of a problem. One recent example is a purported class action filed against SunTrust Bank in which an employee accessed the personally identifiable information of approximately 1.5 million SunTrust customers with the intent to sell or transfer the information to criminals.[12] In addition to the breach itself, SunTrust allegedly erred in waiting over a month to inform its customers that their personally identifiable information had been compromised.

There are several schemes that hackers use to attack your data. "Spear phishing" is a favored mechanism for fraudulent actors. Basically, the wrongdoer sends an e-mail to certain employees purporting to be from either a senior executive or a known outside vendor asking for a wire transfer. By the time the false identity becomes known, the money is gone, having been wired to an account unaffiliated with the company. The wrongdoer uses publicly available information to figure out the correct e-mail address format and domain name, then develops a realistic-looking e-mail to send to those persons who are most likely have authority in the finance or accounting department to initiate wire transfers. For example, a Michigan-based tool company suffered an $800,000 loss when a fake e-mail pretending to be from a "Chinese supplier" fraudulently requested a wire transfer.[13] Another company suffered a multimillion-

dollar loss when an accounts payable employee processed a wire transfer that appeared to come from the company's president.[14] Note that the legal profession is not immune: a New Jersey law firm filed suit against Bank of America for alleged negligence in allowing a fraudulent account to receive funds wrongfully wired after the law firm's accounting department fell victim to an e-mail that appeared to have been sent by the firm's managing partner.[15]

Whether purporting to be from an internal source or an outside vendor, e-mails that appear to be from a known sender can easily cause an unsuspecting employee to wire a payment away from the company. This is especially problematic when a vendor's e-mail system is hacked. Then, the vendor's e-mail would actually be from a legitimate source but not for a legitimate purpose. A multifactor authorization process for any significant payment is therefore critical for any company, large or small.

"Phishing" is another common scheme to break into corporate electronic systems. Hackers will send blast e-mails into a company's employee roster, hoping that at least one person will click on an attachment disguised as something legitimate, thereby launching a virus and/or other malicious software. In October 2017, Seagate Technology settled a California federal class-action lawsuit filed after an employee fell for a phishing scheme involving a fake e-mail seeking detailed payroll data about company employees. The error was later alleged to have caused fraudulent acts against many of the company's current and former employees.[16]

"Ransomware" is another popular method for hackers. This method is used by criminal hackers to encrypt information, making it unusable without the encryption key. The wrongdoers will then demand "ransom" payments, usually in the form of cryptocurrency, to unlock systems or prevent further virus infection. This type of threat is especially aimed at industries that depend heavily on data. In May 2017, ransomware named WannaCry infected over 200,000 computers

in over 150 different countries. The infection spread through an exploit present on unpatched systems. Once WannaCry infected a computer on the victim's network, the ransomware would use a flaw in the software to spread from machine to machine, encrypting the files of each machine to which it gained access. The result was that the companies' machines became inoperable until the ransom of $300 per computer was paid. Of the companies affected, one of the most notable was the U.K. National Health Service, which was forced to turn away ambulances and cancel or delay certain treatments due to the attack. Similar facts led to a class-action complaint alleging that Allscripts Healthcare Solutions, a nationwide medical records software vendor in the United States, allowed a ransomware attack to cause life-threatening delays in medical care.[17]

Ransomware is a serious cyber threat, not only because of the attempts to extort money, but also because it attempts to render confidential trade secrets or other confidential corporate information unusable. It also stops business operations and impacts the revenue stream. Whether to pay a ransom to criminals can be a difficult decision for corporations. Although a modest payment to regain control of company assets is tempting, companies must consider how it will play in the press and the signal it could send to other hackers.

A company that uses consumer credit cards in any aspect of its business is a prime target for hackers. Financial and communications companies are frequent targets, as are retail stores and online businesses. Highly publicized breaches over the past several years have included Home Depot, Neiman-Marcus, Target, and Uber, to name a few. Healthcare companies, including hospitals and insurers, are another favorite target because they have confidential medical information and Social Security numbers on file. However, the important point to keep in mind is that it is not only large national chains and large regional hospitals that fall victim to

hackers. Small local businesses and hospitals, which also use and collect credit-card information or patient medical information, are also at risk. This is because it is assumed, usually correctly, that these smaller businesses have less-sophisticated cybersecurity protections (not to mention that these smaller companies often serve as vendors to large companies and may be a gateway to hacking into them). If you think your small business operates under the radar of computer hackers, think again.

II. Legal Framework

The legal framework for cyber security in the United States is often described as patchwork in nature. There is no one unifying law applicable to all businesses in all circumstances. Instead, companies are subject to a variety of federal and state laws and regulations depending on their industry and location. For example, certain federal statutes are industry-specific, setting forth obligations and prohibitions for participants in various sectors such as healthcare or the financial sector.

In addition to various federal and state statutes, cyber security is regulated through enforcement actions by a myriad of governmental agencies. The Federal Trade Commission (FTC) actively uses its enforcement power to curb "unfair or deceptive trade practices." Other pertinent federal governmental agencies include the Consumer Financial Protection Bureau, the Department of Education, the Department of Health and Human Services, the Federal Communications Commission, and the Securities and Exchange Commission. At the state level, state attorneys general play an active role as a counterpart to the FTC regarding consumer data, especially through the imposition of notification obligations in the event of a data breach impacting consumer data.

The patchwork is also made up of privately negotiated agreements between companies, vendors, and customers, setting forth obligations and responsibilities for cybersecurity issues. Companies are subject to tort-based claims, often in the form of class actions, for alleged violations of duties arising from breaches. Finally, companies in the United States with international operations (including conducting business online intended to reach people outside the United States) must be mindful of applicable foreign laws.

A detailed discussion of all laws applicable to cyber security and privacy is beyond the scope of this chapter. Instead, this chapter aims to provide a summary of some of the most critical laws in order to provide in-house counsel a sense of the legal framework and guiding principles. Set forth below is a discussion of: (1) industry-specific cybersecurity requirements in healthcare and financial services as examples of two, highly regulated industries; (2) a discussion of federal enforcement through the FTC and other agencies as well as state enforcement through state attorneys general; and (3) cross-border issues. Contract issues are discussed in Part III-C, *infra*.

A. Sampling of Industry-Specific Requirements

In-house counsel must have intimate familiarity with industry-specific data privacy and cybersecurity legislation applicable to their own company. Set forth below is a sampling of some of the most important legislation in the highly regulated areas of healthcare and financial services. The purpose of this discussion is to assist in-house counsel with a basic understanding of how such issues are treated in heavily regulated industries, given that these practices serve as examples of how the law has developed to deal with these issues.

The most well-known healthcare privacy law is commonly referenced as HIPAA, which stands for the Health Insurance Portability and Accountability Act of 1996.[18] In fact, much of

what makes up the final privacy and security rules were driven by the addition of the HITECH Act, implemented as part of the American Recovery and Reinvestment Act of 2009.[19] HITECH stands for Health Information Technology for Economic and Clinical Health Act. HITECH incentivized the adoption of electronic health record (EHR) technology by providing access to government subsidy dollars to offset the technology capital investment costs associated with the adoption of EHR through a tiered attestation process related to meeting certain adoption milestones. HITECH also legislatively mandated the Office of the National Coordinator for Health Information Technology (ONC).[20]

HIPAA/HITECH (hereinafter HIPAA) applies to health plans, healthcare clearinghouses, and certain healthcare providers that transmit data electronically within the bounds of the Transaction Rule.[21] The law also applies to "business associates"—entities providing services to a covered entity involving receipt, creation, transmission, or maintenance of PHI.[22] Under HIPAA, covered entities and business associates must request and disclose only the minimum amount of PHI of a patient needed to complete a transaction. Further, covered entities and business associates are responsible for implementing data security procedures, protocols, and policies to safeguard PHI at administrative, technical, physical, and organizational levels.[23] In the event of a breach, HIPAA requires notification to individuals whose PHI has been affected. Larger breaches, defined as involving more than 500 individuals, also require prominent media outlet notification.[24]

HIPAA operates to protect PHI, which is information that relates to an individual's past, present, or future physical or mental health or condition; the provision of healthcare to the individual; and the past, present, or future payment for the provision of healthcare to the

individual, as well as information that identifies the individual or that can be reasonably believed to be used to identify the individual.[25]

Two fundamental aspects of HIPAA are known as the Privacy Rule and the Security Rule.[26] The Privacy Rule seeks to protect PHI while allowing for the exchange of information necessary for healthcare. This rule requires covered entities to implement safeguards to protect PHI from inappropriate disclosure and to establish conditions for the use of information without patient authorization. Importantly, the rule establishes the rights of patients to their PHI, such as the right to examine, the right to obtain a copy, and the right to request corrections.

The Security Rule seeks to protect PHI while enabling covered entities to improve patient care. Under the Security Rule, a covered entity must maintain reasonable and appropriate administrative, technical, and physical safeguards for protecting PHI, including ensuring the confidentiality, integrity, and availability of all patient data; protecting against reasonably anticipated security threats and impermissible uses or disclosures; and ensuring workforce compliance.

As the opioid crisis has risen to the headlines in recent months, counsel should be reminded of another important data privacy law relevant to patient information related to substance use disorder, education, prevention, training, treatment, rehabilitation, or research. Records associated with these activities are protected at a higher level than that of HIPAA under 42 C.F.R. pt. 2. (hereinafter Part 2)[27] Organizations subject to these regulations require additional processes to ensure that patient information is not disclosed inappropriately. Part 2 requires a higher level of patient consent for disclosure of information and prohibits free redisclosure of information as is common under HIPAA.

In the financial services industry, the Gramm-Leach-Bliley Act (GLBA), enacted in 1999, applies to financial institutions, including banks, securities firms, insurance companies, and mortgage lenders. The law may also apply to credit counseling services, financial advisors, collection agencies, and credit-card issuing firms, along with other entities that provide or support financial services, as discussed below. GLBA regulates the collection, use, and disclosure by a financial institution of nonpublic personal information from consumers in connection with financial products or services.

As required under GLBA, the FTC issued regulations requiring specified financial institutions to implement measures to secure customer information. The "Safeguards Rule" applies to businesses that are "significantly engaged" in providing financial products or services. This broad definition captures a wide range of businesses. Entities that come into possession of customer information from other financial institutions, such as credit reporting agencies, are also required to comply.

Companies subject to the Safeguards Rule must develop a written information security plan that describes their program to protect customer information. The plan must designate a responsible employee to supervise security, identify and assess risks to customer information, and evaluate the effectiveness of existing safeguards for controlling these risks. The designated employee must also design, implement, monitor, and test a security program, among other steps. Any firm that is subject to GLBA must have a detailed understanding of how the industry-specific law impacts its business and must develop processes designed to ensure compliance.

Another federal statute relevant to the financial services industry is the Fair Credit Reporting Act (FCRA),[28] which applies to consumer reporting agencies and regulates the use and disclosure of consumer reports and credit-card account numbers.

A more recent regulation affecting the financial services industry came from the New York State Department of Financial Services (DFS), which issued cybersecurity regulations that are seen as the new standard for risk control and prescriptive rules in the industry.[29] The DFS regulations set forth detailed requirements that covered companies must follow in terms of establishing cybersecurity policies and programs, risk assessment, testing, data security, incident response plans, and more.

Other federal laws imposing cybersecurity obligations on the use of personal data within certain industries include the Children's Online Privacy Protection Act,[30] the Family Educational Rights and Privacy Act, the Electronic Communications Privacy Act,[31] the Communications Act, and the Computer Fraud and Abuse Act.

B. Enforcement

Every business must be aware of the authority of various governmental entities to exercise enforcement powers to shape standards of corporate behavior in the areas of data security. For example, the Federal Trade Commission Act prohibits unfair or deceptive commercial practices in interstate commerce.[32] The FTC's interpretation of the act allows it to bring enforcement actions against companies for failure to comply with posted privacy policies, changing policies without adequate notice, and/or failing to safeguard personal information. Any dispute about the power of the FTC to act in the area of cyber security was resolved by the Third Circuit's decision in *FTC v. Wyndham Worldwide Corp.*,[33] where the court rebuffed a challenge to the FTC's powers. The Eleventh Circuit, however, in a widely anticipated ruling involving the since-defunct company LabMD, threw out an FTC order directing LabMD to overhaul its data security program. The appeals court in *LabMD* found that a lack of specifics on how the cybersecurity

changes should be implemented caused the order to fail, but the court deferred to the FTC on the broader question about the scope of its data security authority.[34]

The FTC labels company behavior as "deceptive" when false representations are made to customers through publicly posted policies or announcements. In addition, the FTC considers company behavior to be "unfair" when the company is engaged in practices deemed unreasonable under the circumstances. These labels have been used by the FTC to bring lawsuits against companies for such acts as failing to properly inform consumers of the types of data the company was collecting, and for using consumer information in a manner that was not previously disclosed.[35] Further, the representations made to consumers at the time of collection continue to exist even when data is acquired as the result of a merger.[36] The typical result of a FTC enforcement action is a negotiated consent agreement.

All companies should be aware of the power of the FTC (and other applicable regulatory bodies) to bring actions to challenge and shape corporate behavior regarding cyber security even after the *LabMD* decision. Unfortunately, no concise one-size-fits-all document allows for easy comfort on this issue. Instead, in-house counsel should generally be aware of the FTC's enforcement actions (and the types of complaints brought and consent orders previously entered into) as well as the FTC's outreach efforts through the issuance of public guidelines and recommendations (all of which are available on the FTC website at www.ftc.gov).

The SEC has also stepped up its enforcement role through its *Commission Statement and Guidance on Public Company Cybersecurity Disclosures*, issued on February 21, 2018. These enhanced guidelines require public companies to disclose details about board of directors' oversight of cyber security, overall corporate risk management, and any risks or incidents that are material. Failure to disclose is a risk for public companies to avoid.

The Office of Civil Rights (OCR) is the organization tasked with investigating and resolving HIPAA violations on behalf of HHS. Over the last three years, settlement figures posted by OCR have ranged from tens of thousands of dollars to tens of millions, as seen in the *Anthem* case. All "large" breaches are posted by HHS on a public breach portal.[37] Counsel should also be aware that other civil monetary penalty obligations could be assessed by HHS consistent with the authority granted under section 1128A of the Social Security Act.

States, of course, enforce their own laws and regulations. State attorneys general have broad enforcement powers, and some are rather activist. State regulators may also have powers to enforce their regulations, such as the New York Superintendent's power to enforce the DFS regulations.

C. Cross-Border Issues

The General Data Protection Regulation (GDPR), promulgated by the European Union and effective as of May 25, 2018, governs the processing and free movement of personal data, recognizing the fundamental rights and freedoms of persons with respect to their personal information. The GDPR applies to data "controllers" and "processors" established in the European Union, regardless of where processing takes place. Importantly, the GDPR also applies to controllers and processors outside the European Union when they are engaged in activities such as offering goods or services in the EU or monitoring a data subject's EU behavior.

The GDPR's reach is broad and may be fairly viewed as stressing privacy more than data protection. The complexity of the regulation has spawned a legal practice specialty in and of itself. Therefore, in order for in-house counsel to determine the extent to which the GDPR (or other foreign laws) impose obligations given the nature of information held or shared by the company, consulting outside counsel with expertise is advisable. Even if determined not to be

applicable, in-house counsel will benefit from a working knowledge of the GDPR and other foreign laws, as the thought process behind the enactment of this legislation represents a clear trend for the future.

In certain situations, the GDPR requires a company to undertake a privacy impact assessment, which is an analysis of where data is located and the purpose and context for which it is used. A privacy impact assessment identifies the process by which data is collected, shared, and used, and identifies the risks to such data and the adequacy of measures to guard against such risks. The GDPR also requires (with certain exceptions) companies to designate a data protection officer and imposes many other requirements on those subject to the law.[38]

As further described at Part III-B, *infra*, data security is an interdisciplinary activity. In-house counsel or IT professionals alone will not be positioned to collect, evaluate, and assess the information required by a privacy assessment. It is imperative that in-house counsel involve other relevant members of the organization—both to educate them about the provisions of laws such as the GDPR and, more importantly, to promote a culture of security and compliance. A business operated without regard to such responsibilities is a business operating at a high degree of risk. In addition to the business and public-relations risks, noncompliance with the GDPR imposes the risk of serious economic harm, including penalties of up to four percent of global annual revenue, or €20 million, whichever is greater.

In sum, "patchwork" is indeed the best word to describe the law of cyber security (and privacy) in the United States. In-house counsel must be familiar with a host of federal and state law (including industry-specific laws), the enforcement powers of governmental agencies (such as the FTC), and the reach of foreign laws (such as the GDPR) that can stretch to U.S.-based companies.

III. Building Corporate Resilience

A. Develop, Implement, and Maintain a Culture of Security

The Commonwealth of Massachusetts is generally regarded as a leader in enacting comprehensive standards for the protection of its residents' personal information.[39] The regulation, Standards for the Protection of Personal Information of Residents of the Commonwealth, was promulgated by the Department of Consumer Affairs and Business Regulation in accordance with Massachusetts General Law Chapter 93H. Although many states have enacted data breach legislation that should be reviewed as applicable, it is worthwhile that in-house counsel have working familiarity with the Massachusetts legislation in particular, due to its comprehensive nature.

Under the regulation, businesses holding personal information of Massachusetts residents must comply with minimum security standards. The regulation defines "personal information" as a resident's

> first name and last name or first initial and last name in combination with any one or more of the following data elements that relate to such resident: (a) Social Security number; (b) driver's license number or state-issued identification card number; or (c) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a resident's financial account.[40]

Other states have enacted similar laws to protect the personal information of their residents, although the specific definition of the term "personal information" varies among the states' laws.[41] The Massachusetts regulation is noteworthy for its detailed provisions and practically sets forth standards that all companies should consider, whether doing business with Massachusetts residents or not.

A key element of the Massachusetts regulation is the requirement that any business that owns or licenses personal information of a Massachusetts resident must ensure administrative, technical, and physical safeguards for such information through the implementation of a written information security program (WISP).[42] Certain information must be contained in a WISP, including:

- the designation of an employee to maintain the WISP;
- the assessment of risks to the security of records containing personal information and means to mitigate such risks through such action as training sessions for employees and careful monitoring and response to security system failures;
- disciplinary measures for violations of the WISP and safeguards for preventing terminated employees from accessing records containing personal information;
- security policies for storing, accessing, and transporting records containing personal information away from business premises;
- reasonable restrictions on physical access to records containing personal information, as well at the appropriate storage of records and data in suitably secure locations;
- regular review of security measures to ensure the security of records containing personal information; and
- documentation of responsive actions to any security breach incidents, as well as post-incident review of events.

Of course, such safeguards must be consistent with any federal or state laws otherwise applicable to the business.

The regulation also requires businesses to limit personal information collected in both scope and duration. Further, the regulation sets forth the requirements for encryption of personal information, as well as minimum standards for secure computing. These items include standards around user identification and authentication, establishing limits to accessing certain information,

procedures for patching, and education and general training for employees on the topic of security.[43]

B. Interdisciplinary Approach

Company-wide buy-in is necessary for data privacy and cybersecurity policies to be effective. For in-house counsel to respond effectively to a cybersecurity attack or data breach, extensive planning and relationship-building must have occurred well in advance. Waiting until the moment of need to think through strategic alternatives and assignment of responsibilities is obviously not ideal. This part sets forth some guidelines for in-house counsel to proactively assemble a team and develop relationships. Importantly, counsel must work with others in the organization to ensure that "ownership" of cyber security is viewed as a common responsibility—not a problem for only the legal staff or the IT group. In the event of a cyber attack or data breach, all aspects of the organization will be affected. Thus, it makes sense for all stakeholders to be involved in the tasks of prevention and planning.

The first step is identifying with specificity individuals from various company departments who will commit to the cause and work cooperatively to form a response team. Such a group should consist not only of legal and IT personnel, but also C-suite management, risk management, and public-relations employees. A robust compliance function is critical. Sales should also have some involvement, given that cyber security is relevant in the buying cycle and that customer satisfaction as part of a response is a critical priority.

These response team members should then consider which external professionals will complement the team, both for planning purposes and for actual response should the need arise. In the event of an incident, there will be no time for interviewing professionals and negotiating terms of engagement. In-house counsel should work with the internal team to understand which

outside professionals might be needed, then make arrangements to finalize the group. In-house counsel must carefully consider the role of outside counsel, and especially the topic of attorney-client privilege, regarding retention of any outside consultants and the scope of legal advice related to a cybersecurity incident.

Once formed, the interdisciplinary group must agree on an incident response plan appropriate to the company that complies with obligations under applicable law. Further, the group must assume ownership of planning for an incident through periodic table-top exercises, internal employee training, and a dedicated process for evaluation and improvement of the company's resilience to threats and ability to respond.

C. Vendor/Supplier Due Diligence and Appropriate Contract Terms

Based on legal requirements and risk-management best practices, in-house counsel must ensure that the company's process for engaging vendors vigilantly protects data and serves the cybersecurity needs of the company. Set forth below is a checklist for formalizing a vendor selection process that achieves this objective.

1. Vendor Selection

- Understand the flow of company data to the proposed vendor, the nature of the data to be shared, and the necessary protection needed for such data, including applicable information-security regulations.
- Conduct diligence on the vendor's reputation for compliance and performance.
- Work with your company's information-security personnel to develop appropriate information-security questions (standards-based if applicable)

to gauge the potential vendor's sophistication, preparation, and vigilance with data security.

- Require proof of the potential vendor's cyber insurance and assess whether such insurance would be adequate to guard against risks faced by the vendor based on data to be shared.

2. Contracting

- All business stakeholders involved in the vendor selection process must understand the company's need for robust contractual terms on security. Company counsel should develop and maintain a collection of clauses that are generally acceptable. Having others in the business understand this point can help streamline the vendor selection process to avoid providers with terms that are not acceptable.
- Include cybersecurity requirements and procedures that the vendor must maintain.
- Ensure the contract identifies all costs that could stem from a breach and then allocates responsibility for the risk of such costs between the parties.
- Ensure that the contract provides clear guidance on notification procedures in the event of a breach or perhaps even in the event of an incident.
- Understand the vendor's record retention policies and procedures and ensure that such policies are consistent with your own company's requirements.
- Include the right to audit the vendor's cybersecurity procedures and programs.

- Clearly state which party has ownership of data and the circumstances under which data can be transferred (especially if outside the United States).
- Carefully negotiate limitations-of-liability provisions, reflecting the business understanding and allocation of risk regarding data handling.

3. Contract Monitoring

- Once a vendor is selected and final contractual terms have been reached, it is critical to ensure that the vendor's performance under the contract is monitored both for compliance as well as for possible adjustments or amendments.
- Immediately investigate any reports of vendor issues that may surface. Generally, the earlier issues are explored, the greater the range of possible responses.

D. Considerations for Corporate Transactions

Although cyber security has always been an extremely important issue in highly regulated industries like healthcare and financial services, concerns arise in the context of virtually every industry. Given that cybersecurity issues can dramatically impact the value of a deal, it is critical that all parties to a potential transaction (including buyers, sellers, investors, board members, and lenders) identify any such potential issues, undertake appropriate diligence, and negotiate tailored agreements. As noted previously, data security issues are not reserved for IT or compliance personnel; the issues demand careful attention from deal makers and decision makers to ensure value is preserved.

Although some deal teams reach for a diligence checklist template from prior deals in preparing for a new transaction, effective diligence requires more critical thinking on data security issues. Before diligence is commenced, the diligence process must first be designed with specific attention to the types of data security issues that ought to be of primary concern given the specific industry, nature of the assets, and contemplated transaction. The process should be designed by a cross-functional team prepared to work together to design a process focused on the highest priority concerns. The team should consider the value of a third-party service provider, preferably one experienced with industry-specific issues, to focus exclusively on cybersecurity concerns.

In using a provider, pay careful attention to the scope of engagement, the terms of retention, and best practice/industry standards that the provider should bring to the engagement. A few key topics for the provider to examine include whether any prior data disclosures have occurred that may present liability to a new owner; the current data security posture of the company; and the corporate security policy or philosophy/implementation of the entity being acquired.

As with all corporate transactions, critical provisions for agreements with third-party service providers should include representation and warranties, indemnification rights, limitation of liability, and key definitions for terms such as “material adverse change.” Contractual rights should be clearly drafted and readily enforceable to protect the expectations of the parties. Due to the unique issues that can arise from inferior data security policies, it is important for parties to understand that even the most brilliant legal language will not fully protect a party from insufficient diligence. Deliberate and thoughtful diligence must go hand-in-hand with tailored documentation, including consideration of other protections, such as suitable insurance.

E. Ensure Cyberinsurance Coverage Is in Place

The cybersecurity insurance market has grown tremendously over the past few years. Traditional liability carriers and new players are entering the field. Such insurance is probably a wise investment, considering the expanding costs and increasing likelihood of a breach. Consider working with a knowledgeable independent risk advisor (not just a broker), and consider the options available, whether a specialized cyber policy or a commercial liability package with some level of cyber coverage. Business interruption is an important type of coverage to consider, as well as coverage for regulatory fines and litigation liabilities. You must evaluate your risk in light of the types of data your company stores and transmits. Personal financial or health data is high risk, whether your business is consumer-facing or not. Specialized cybersecurity policies are new and have not yet been subject to much litigation; however, reviewing a handful of court decisions will allow you to see which provisions may work for special cyber, computer, and commercial general liability (CGL) policies.[44]

To help control premium rates, your company should demonstrate to insurers during the application process that it has a strong cybersecurity program, including a regularly practiced and comprehensive incident response plan informed by knowledgeable counsel, secured vendor relationships, and engaged senior management. It would also help to show mandatory and regular employee training on cybersecurity risks.

IV. Preparing to Respond to a Breach—Develop, Test, and Update Incident Response Plan

A. Incident Response Plans

A response plan is not just nice to have; it is a must-have. Depending on your line of business and location, you might have a legal requirement to establish and maintain a robust response

plan. The plan, manual, or playbook must be taken seriously. Support and input from senior management is critical, including that of executives and perhaps the board. Akin to a disaster recovery plan, the cybersecurity breach plan must be user friendly, comprehensive, and familiar to those who will be expected to implement it. It cannot be tucked away on a shelf; rather, regardless of whether the document is electronic or hard copy, it must be easily accessible and refreshed often. In addition, calling it a "breach" plan can be a misnomer because the plan should also cover situations of a suspected cyber intrusion, even if a "breach" (however defined) did not actually occur.

There are several steps for creating an effective incident response plan. First, you must bring together all of your company's necessary stakeholders. As noted earlier in Part III-B, in addition to executive sponsorship, you need colleagues from compliance, public relations, internal audit, human resources, and IT. You especially need colleagues who operate the business in each division, if you have separate divisions, and who know what systems your company uses and how those systems interact with external customers and business partners. If you work in a company that does not have some of these internal functions, then you must engage with outside consultants and vendors who would be called upon in the event of an incident. Depending on your company's size and industry, you may need to engage with media, crisis-management, and forensic IT consultants. A common theme throughout this chapter is the importance of having outside consultants and vendors on standby that could address the breach during a time of panic. These third parties must be lined up and at least preliminarily acquainted with your company, its business, and the various systems in use.

A key outsider you should line up when drafting your incident response plan is, of course, outside counsel. Even a sophisticated in-house legal department with cybersecurity

knowledge will benefit from outside counsel's advice and guidance. There is a strong chance that drafting of the plan and internal communications relating to the drafting, when written at the request of counsel in order to provide legal advice, may be protected by attorney-client privilege. This protection would give internal stakeholders greater freedom to communicate their concerns and questions regarding cyber risk within the company. Outside counsel should also be fully up to speed on new developments in the law, particularly new cybersecurity legal requirements that might apply to your company. In a sense, outside counsel who is "on call" can provide you some peace of mind.

The incident response plan or playbook is a highly individualized document, unique to your company's particular line of business, company culture, and jurisdictional requirements. Do not expect to take a template and fill in a few blanks; time and thought will be necessary to do this correctly. The following are major points to consider and steps to include in your plan:

- **Reporting.** Map out how suspected cybersecurity incidents will be reported within the company. A large company may have a hotline, whereas smaller companies may need to simply promote calls to IT or the legal department.
- **Confirmation.** Your IT department, or external vendor if needed, must initially investigate the situation and confirm whether some intrusion occurred and whether any data actually left the company.
- **Escalation.** If a breach, or even meaningful attempted breach, is confirmed, the matter must be raised up to appropriate senior management within the business. You should also inform the legal department and other relevant support functions. The legal department, with or without outside counsel, must implement a legal "hold," making sure to freeze IT information and preserve internal communications.

- **Investigation.** Conduct a deeper investigation of facts to determine whether a breach occurred. This should be done under the supervision of counsel (preferably outside counsel) and may require the assistance of outside forensic consultants.
- **Project Manager.** Your company should appoint someone to coordinate and pilot all of the administrative efforts that will begin to ramp up once a breach has been confirmed. This person must be designated in advance and be ready to step up once the alarm sounds. Among other responsibilities, the project manager must carefully document all steps undertaken. This documentation will absolutely be requested by either regulators or plaintiffs' lawyers in the event of a breach.
- **Assessment/Notification.** As facts are developed, determine whether the incident meets the definition of a breach under applicable standards. This step must be headed by legal, which will decide whether any notification requirements have been triggered to customers, regulators, or law enforcement.
- **Mitigation.** The company must act quickly to stop further infiltration or leaking of data, depending on the situation. This is largely the responsibility of IT, but public-relations and marketing colleagues may also be needed to promptly notify customers or business partners to take precautions.
- **De-escalation and Recovery.** The relevant stakeholders, guided by the project manager, will begin to return systems and business to normalcy. Steps to develop long-term improvements are mapped out and implemented.
- **Lessons Learned.** This critical final step includes documenting all remediation actions and preparing applicable reports for senior management and/or the board (under the

direction of counsel). If not already done, this step might include dealing with employees deserving of termination or discipline.

It bears repeating that the above-listed steps are but a general outline of points to consider when drafting or refreshing your company's incident response plan. You must customize the plan to fit your company's specific organizational structure and to account for regulatory requirements that may apply.

There are helpful standards that you may want to consult when drafting your cybersecurity incident response plan, even if they don't directly apply. For example, the Massachusetts regulation (described in Part III-A, *supra*) sets out requirements for a WISP. The New York State Department of Financial Services Cybersecurity Requirements for Financial Services Companies[45] mandates that incident response plans also include sections on (1) goals of the incident response plan and (2) roles, responsibilities, and levels of decision-making authority.[46] The National Institute of Standards and Technology (NIST), an agency under the umbrella of the U.S. Department of Commerce, provides a wealth of cybersecurity information online, including its well-known "framework" that one should wisely consult when drafting or refreshing a response plan. Although the framework is neither specific to response plans nor a legal standard per se, it gives excellent context for many points that should be included in your response plan.

There are also other preparatory efforts that may fall outside the corners of the cybersecurity incident response plan document. For example, will your company contact law enforcement if hacked from an outside source? Will your company pay ransom if demanded in order to unlock critical or confidential data? There are pros and cons either way, and these questions should be considered in advance of a breach, preferably with the advice of

experienced outside counsel. Although it's hard to decide for sure until the facts of a real situation present themselves, making it hard to include these topics in your response plan, you are well served to think through questions about law enforcement and ransom payments without the stress of an actual breach at hand. At the very least, you should map out authorizations for decision-making so that the necessary people, including executives, can be pulled in quickly.

Once your incident response plan is polished, you cannot relax. Aside from remembering that the document must be reviewed and updated at least once a year to account for changes in both law and internal staff, you must also remember to practice the plan. This means conducting an all-hands mock breach exercise, or what is often called a "tabletop" exercise. The exercise must be done regularly in order to keep it in mind and to ensure all employees on the response team are well-versed, especially in light of normal employee turnover. Senior executives should be included. The exercises should be conducted at the request of counsel for the purpose of seeking legal advice about the adequacy of the plan.

Post-exercise reports also must be written at the request of counsel so that counsel can provide legal advice about the results of your mock exercise. It is important that participants be open and honest about areas of concern and weaknesses in the plan, knowing that their comments are intended to be held confidential under the attorney-client privilege. It is useful to include IT and public-relations consultants in the exercise if they will be part of the actual breach response team. Consultants should be retained directly by counsel so that steps can be taken to protect their work product. Under *United States v. Kovel*,[47] nonlegal professionals may receive attorney-client privileged materials within the scope of the privilege, and their communications with counsel may be protected, where those professionals are retained by

counsel to provide advice and expertise that assists counsel in providing legal advice and/or services to his or her client. Application of the attorney-client privilege is fact-specific in these types of circumstances; therefore, careful guidance by outside counsel is important. As discussed more fully below, if a court finds the materials and communications related to breach preparation efforts were business documents rather than created for a legal purpose, the privilege likely won't apply. In addition, sharing these materials with regulators may waive the privilege and subject them to FOIA requests, but you should consult each state's FOIA rules.

A final point worth noting in connection with breach preparation is the overlap with an old-fashioned disaster recovery plan. Hopefully your company has a disaster recovery plan, which should be consulted as you polish your cybersecurity incident response plan. At a minimum, a robust and up-to-date disaster recovery plan will immediately help in cutting the time needed to recover from a breach and return to normal internet-connected operations. It will also help resist the urge to pay a ransom in the heat of a breach situation.

B. Responding to a Data Incident

There is no difference between responding to a potential breach and an actual breach, at least initially. Thus, in the event of a cybersecurity incident that could evolve into a breach situation, the response plan must be quickly consulted (not "dusted off" if you've been updating it regularly!), and all employees must know to contact your legal department right away. In-house or outside counsel should quickly roll out a legal hold, preserving all communications and alerting relevant employees to resist sending internal e-mails discussing the incident and related investigation. You must also quickly contact IT to determine whether any systems must be shut down or frozen (within the confines of carrying on business).

The key players must be contacted and assembled, whether in a room or electronically. Remember that counsel, whether in-house or external, must determine if an actual breach occurred as facts are uncovered. This depends on which federal and state laws apply: on one hand, an unauthorized intrusion into the company's systems may not constitute a breach under some state laws if, for example, the confidential personal information was not actually extracted and shared or was encrypted. On the other hand, other state laws define a mere attempt to access certain personal data as a breach.[48] Even unauthorized disclosure of certain financial account information, without associated names, may be a breach.[49]

Once it is determined that a breach occurred, the project manager must take control, as set out in the response plan. Public-relations colleagues, internal or external, should also be brought in. Notification requirements to both consumers and regulators must be quickly determined by looking at sources such as HIPAA, GLBA, FCC, and various state laws.[50] As counsel, your focus is now on ensuring compliance with notice requirements and preparing for regulatory inquiries and litigation—all while mindful of the attorney-client privilege, including the fact that materials created during the breach investigation may end up disclosed to regulators, state attorneys general, and/or plaintiffs' attorneys. If your internal investigation includes employee interviews, both human resources and the investigating counsel should be present, depending on the situation.

A business should not wait until a breach occurs to determine its notification requirements. Although states' notification laws have many similarities, there are differences that can greatly impact when and how you respond to a data breach. For example, many states require notification only when electronic information is compromised, but some also apply breach notification requirements to disclosure of personal information contained in a tangible form.[51]

Some states provide that notification is not required when a business can establish that misuse of the acquired personal information is not reasonably possible, but states such as New York, California, and Texas do not provide such a limitation. Florida's notification law requires that consumers be notified without unreasonable delay and in no event later than 30 days after a business determines, or has reason to believe, a breach occurred, unless the business is notified by the police in writing to hold off.[52] In contrast, New Jersey law can be read to require a business to report the breach of security to the police prior to notifying the consumer, and to delay the notification until after the police provide that notifying the consumers will not compromise the investigation.[53]

Companies and their executives understandably have the urge to keep a breach private until they acquire sufficient information to explain the problem and answer questions. However, some notice requirements will not allow much delay, and regulators and litigants will seize upon delayed notification as another legal liability. In October 2017, Hilton Hotels agreed to pay a large fine and undergo annual assessment of its Payment Card Industry Data Security Standard (PCI DDS) credit-card processing procedures after a joint investigation by the New York and Vermont attorney general offices. The regulators alleged that Hilton violated the states' consumer protection and breach notification laws by failing to maintain reasonable data security and by waiting more than nine months after a 2015 breach to notify consumers that their credit-card information may have been stolen. In addition, as mentioned early in this chapter, in late 2017 the large-scale data breach announced by Uber resulted in much criticism from consumer groups and regulators, mainly because of the long delay in announcing the breach to the public. These cases demonstrate that company executives and their counsel not only face the pressure of

legal problems, but also risk reputational harm to the company upon post-breach scrutiny of response actions.

Unless you are working in a truly local company in which a breach might possibly be handled in a quiet manner, the specter of litigation (most likely class actions) must be front and center. The law develops by the day in regard to standing to assert a claim and what kind of damages would pass muster to maintain a lawsuit. The Supreme Court's holding in *Spokeo, Inc. v. Robins*[54] resulted in an ambiguous new test for standing as applied in cybersecurity breach cases: harm that is intangible, but "concrete" is enough to obtain standing, even if there are no tangible damages. Courts have applied this standard to causes of action in data breach cases based on contract, tort, or statutory violation. There is division among courts on whether standing may be met solely by the increased risk of future identity theft.[55] Parties must be cognizant of the case law in their specific circuit and the patterns of specific judges, given the evident split on what constitutes standing. In a recent development, the Illinois Biometric Information Privacy Act has given potential standing for yet additional causes of action for data breaches involving confidential biometric information.[56]

Not only should you anticipate litigation from consumers affected by the compromise, but your company may also anticipate additional litigation from business partners. If you are a vendor who provides services to other companies and you suffer a breach, you may then face claims pursuant to contractual obligations to your business customers. Take, for example, the lawsuit filed by Chase Bank against Landry's following a data breach. Chase claimed that Landry's failed to comply with credit-card industry data security standards and was contractually liable to indemnify Chase.[57]

As mentioned above, counsel should oversee breach response actions to the extent possible. Although attorney-client privilege will not apply to all of the various steps undertaken, some being purely business functions, the privilege can protect internal strategy and communications if requested by in-house or outside counsel during the course of providing legal advice. Once breach recovery efforts are underway and counsel is providing advice intended to prepare for likely litigation, work-product protection may also apply, but be cautioned that the determination of whether legal privilege will protect internal work product from discovery by regulators or plaintiffs' attorneys is very fact-specific. Courts will examine the specific role of counsel and the context of the work performed to determine whether legal advice and/or anticipation of litigation was actually present or is being created in hindsight merely to oppose disclosure.[58] In addition, if you choose to disclose any conclusions (as opposed to facts) of a privileged forensic investigation, be cautioned that all of the back-up documents created in connection with that investigation may become subject to discovery when you otherwise might have been able to shield them.[59]

As the breach response and recovery winds down, it is extremely important to assemble the team for a "lessons learned" open discussion. Although it may be tempting to skip this step and get back to business as usual, a huge opportunity is lost if time is not taken to review how the situation was handled and what process improvements should be inserted into the next updated version of your response plan. Discussions and communications examining the breach response should be conducted by counsel who is providing legal advice about actions well performed or those needing improvement.

V. Practice Tips/Recommendations

A. Threat Sources

- Train employees in order to minimize internal risks.
- Secure your IT systems and test for penetration.
- Stay current with breach threats so your defenses will be on alert.
- Ensure that vendors have robust cybersecurity protections.

B. Legal Framework

- Develop and maintain intimate familiarity with industry-specific domestic legislation and regulation.
- Understand and stay informed of governmental enforcement activities applicable to the industry in which your company operates.
- Develop a working knowledge of the principles and requirements of the GDPR and "best practices" even if not directly applicable.
- Commit to involving other relevant members of your organization in promoting a culture of security and compliance.
- Develop and maintain a network of trusted advisors who can help in implementing the above steps on a continuous basis.

C. Building Corporate Resilience

- Develop a culture of security that includes well-functioning relationships at the operations level along with appropriate management and board-level supervision.
- Protect against insider threats through continuous employee training as well as policies and procedures that are implemented and maintained.
- Ensure a robust recovery plan is in place. Practice plan implementation, review for areas of improvement, and repeat on a regular basis.
- Ensure that all aspects of the company's process for engaging and working with vendors vigilantly protect and serve the cybersecurity needs of the company.
- Periodically evaluate sources of potential risk for the company and critically analyze existing insurance coverage and whether additional coverage is needed to help minimize economic harm from risks for which insurance is desired.

D. Preparing to Respond to a Breach

- Understand and inventory your company's data/IT assets.
- Gather a cross-functional team to prepare an incident response plan.
- Outline decision-making procedures and authority in advance.
- Conduct mock exercises, with lessons learned, under the direction of counsel.
- Stay educated in state and federal notice requirements.

E. Resources

- NIST Cybersecurity Framework and Risk Management Framework (National Institute for Standards and Technology, www.nist.gov).
- Your company IT and HR departments (or outside consultants who perform those functions).
- Outside counsel, vetted and educated about your company and its systems.
- International Association of Privacy Professionals, IAPP.org (requires paid membership to access some materials).
- Regulator/law enforcement sources (FBI Internet Crime Complaint Center (IC3); U.S. Computer Emergency Readiness Team; Infragard (membership required); "Order Free Resources" at ftc.gov; www.HealthIT.gov).

Efficient resolution of disputes arising from a data breach should be a top concern for in-house counsel. Disputes that linger pose not only a liability risk, but also a cost concern, given that litigation expenses can quickly escalate. Of course, the key interest of a company affected by a data breach will be responding to and recovering from the breach. Response and recovery will often require interaction with multiple third parties, such as customers, vendors, insurers, regulators, partners, and others. Interests of commercial parties will include confirmation that the specific cause of the breach has been identified and remedied, that the costs of collateral damage created by the breach are covered, and that changes are implemented to reduce the risk of similar breaches in the future.

In situations of widespread harm involving personally identifiable information (PII), it is not uncommon for class-action lawsuits to ensue. In addition to consumers, governmental authorities commonly assert interests in a data breach, seeking compliance with regulatory obligations. Keep in mind that mediation has been used to help parties reach closure on the economic consequences of a breach without having to engage in full-fledged litigation. A successful mediation depends on identifying key interests at stake, as well as options to satisfy those interests. For example, in the fall of 2017, a mediated settlement was preliminarily approved between current and former employees of Seagate Technology LLC and the company

arising out of a 2016 data phishing attack that affected approximately 12,000 employees. In the attack, a Seagate employee forwarded PII of fellow employees to attackers who then used the information to file fraudulent tax returns. The settlement provides each current and former employee with two years of credit monitoring and up to $3,500 for out-of-pocket expenses. In sum, when a breach occurs, in-house counsel should consider the possibility of using mediation to help parties identify interests and explore options for satisfying those interests, which can help contain the impact of the breach and avoid collateral consequences.

VI. Conclusion

This chapter has provided in-house counsel with a practical overview of major considerations in the area of data privacy and cyber security. Although in private practice now, the two key authors have in-house experience at major corporations working directly with business teams on a variety of issues. With that experience in mind, the chapter began with a summary of various threat sources and risks that in-house counsel must understand. The chapter then provided a summary of the legal framework governing cybersecurity issues. Next, the chapter discussed essential steps for corporate resilience on which in-house counsel must focus regularly to achieve success in this area. These steps include fostering an internal culture of security, working to develop an interdisciplinary approach, effectively managing vendor relationships, building discipline around corporate partnerships and acquisitions, and ensuring adequate and appropriate insurance is put in place to cover risks the company does not want to absorb. The chapter then moved on to considerations in designing, testing, and updating an incident response plan—a core aspect of corporate resilience and a requirement under many laws. The chapter concluded with a summary list of recommendations for in-house counsel to consider, including the recommendation that in-house counsel keep abreast of developments in this area. This area of the

law is evolving rapidly and changes often, so you must stay informed. This should be done in close consultation with other leaders of the business, given that ownership of these issues is, and will remain, a responsibility shared across functional lines.

---

[1] Olga V. Mack & Katia Bloom, *Yahoo's 10K: Lessons on What Not to Do in a Breach,* ACC DOCKET, Nov. 27, 2017, http://www.accdocket.com/articles/yahoo-10k-lessons-on-what-not-to-do-in-a-breach.cfm.

[2] Yahoo! Inc., Form 10K 2016, *available at* SEC EDGAR, https://www.sec.gov/Archives/edgar/data/1011006/000119312517065791/d293630d10k.htm.

[3] *Id.*

[4] *Id.*

[5] Mike Isaac, Katie Benner & Sheera Frenkel, *Uber Hid 2016 Breach, Paying Hackers to Delete Stolen Data*, N.Y. TIMES, Nov. 21, 2017, https://www.nytimes.com/2017/11/21/technology/uber-hack.html.

[6] *Id.*

[7] *Id. See also* Eric Newcomer, *Uber Pushed the Limits of the Law. Now Comes the Reckoning,* BLOOMBERG, Oct. 11, 2017, https://www.bloomberg.com/news/features/2017-10-11/uber-pushed-the-limits-of-the-law-now-comes-the-reckoning.

[8] *Id.*

[9] Brendan Pierson, *Anthem to Pay $115 Million to settle U.S. Lawsuits Over Data Breach,* https://www.reuters.com/article/us-anthem-cyber-settlement/anthem-to-pay-record-115-million-to-settle-u-s-lawsuits-over-data-breach-idUSKBN19E2ML (last visited July 12, 2018).

[10] *Id.*

[11] *Id.*

[12] Smith v. SunTrust Bank, Inc., No. 1:18-cv-02200-MHC, at 6 (N.D. Ga. 2018).

[13] Am. Tooling Ctr., Inc. v. Travelers Cas. & Sur. Co., 2018 U.S. App. LEXIS 19208 (6th Cir. July 13, 2018).

[14] Medidata Solutions., Inc. v. Fed. Ins. Co., 2018 U.S. App. LEXIS 18376 (2d Cir. July 6, 2018).

[15] Mazie Slater Katz & Freeman LLP v. Bank of Am. NA, No. L-49-18 (N.J. Super. Ct.).

[16] Castillo v. Seagate Tech. LLC, 2017 U.S. Dist. LEXIS 178852 (N.D. Cal. 2017).

[17] Surfside Non-Surgical Orthopedics v. Allscripts Healthcare Sols., Inc., No. 1:18-cv-00566, Complaint at 3 (N.D. Ill. 2018).

[18] Pub. L. No. 104-191. The final HIPAA regulations may be found at 45 C.F.R. pt. 160, 164.

[19] Pub. L. No. 111-5, 123 Stat. 15.

[20] ONC is organizationally situated within the U.S. Department of Health and Human Services and is tasked with coordinating national efforts to implement health information technology in the U.S. health care system. The website for ONC is quite informative, at https://www.healthit.gov.

[21] *See* 45 C.F.R. pt. 162 for a complete list of transactions causing HIPAA obligations to flow to a healthcare provider. These transactions generally include activities associated with insurance verification and electronic claim processing.

[22] 45 C.F.R. § 160.103.

[23] 45 C.F.R. pt. 164(C), §§164.302–164.318.

[24] 45 C.F.R. § 164.406.

[25] 45 C.F.R. § 160.103; *see generally* definition for "individually identifiable health information."

[26] The Privacy and Security Rules are located in 45 C.F.R. pt. 164, with security standards located in sections 300 and 400 and privacy standards in section 500.

[27] Part 2 regulations have been around since the early 1970s as part of The Comprehensive Alcohol Abuse and Alcoholism Prevention, Treatment, and Rehabilitation Act of 1970, 42 U.S.C.S. § 290dd-3; and the Drug Abuse Office and Treatment Act of 1972, 42 U.S.C.S. § 290ee-3. With the advent of integrated provider networks and health information exchanges, Part 2 requirements were affecting care coordination efforts. Accordingly, the Substance Abuse and Mental Health Services Administration (SAMHSA) updated Part 2 regulations in early 2017, https://www.samhsa.gov/42CFRPart2Final.

[28] 15 U.S.C. §§ 1681 *et seq*.

[29] N.Y. COMP. CODES R. & REGS. tit. 23, § 500.00 *et seq.* (West 2017).

[30] Pub. L. No. 105-277 (1998).

[31] 18 U.S.C. § 2510, *et seq*.

[32] 15 U.S.C. § 45(a)(1).

[33] FTC v. Wyndham, 799 F.3d 236 (3d Cir. 2015).

[34] LabMD, Inc. v. Federal Trade Commission, 891 F.3d 1286 (11th Cir. 2018).

[35] *See* Lesley Fair, *What Vizio was doing behind the TV screen*, FED. TRADE COMM'N, Feb 6, 2017, https://www.ftc.gov/news-events/blogs/business-blog/2017/02/what-vizio-was-doing-behind-tv-screen.

[36] *See* Jamie Hine, *Mergers and privacy promises*, FED. TRADE COMM'N, Mar 25, 2015, https://www.ftc.gov/news-events/blogs/business-blog/2015/03/mergers-privacy-promises.

[37] *See* https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf.

[38] For example, companies are prohibited from transferring information to a country that has not been approved by the European Commission. GDPR art. 46(1). Of note, the United States, as of the date of this publication, has not been approved. However, the European Commission has acknowledged that companies that are compliant with Privacy Shield framework are an exception. *See* https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en.

[39] Its standards appear at 201 CODE MASS. REGS. § 17.00 (West 2018).

[40] *Id.* § 17.02.

[41] For example, Illinois includes e-mail user name with password and biometric data in its definition of personal information. 815 ILCS 530/5. Further, California and Delaware require companies that collect PII about their residents through the internet to post a privacy policy informing the public about what they collect and how they use that information. *See* CAL. BUS. & PROF. CODE § 22575–22579; DEL. CODE tit. 6 § 205C.

[42] 201 CODE MASS. REGS. § 17.03.

[43] *Id.* § 17.04.

[44] Medidata Solutions., Inc. v. Fed. Ins. Co., 2018 U.S. App. LEXIS (2d Cir. July 6, 2018, *rehearing en banc denied* Aug. 23, 2018) (court held computer fraud provision in crime policy covered losses caused by employee who approved transfer of money based on phony internal e-mails, rejecting argument that policy covered only fraud carried out by third parties); Am. Tooling Ctr., Inc. v. Travelers Cas. & Sur. Co., 2018 U.S. App. LEXIS (6th Cir. July 13, 2018, *rehearing en banc denied* Aug. 28, 2018) (computer fraud provision covered wire transfer executed in response to fake e-mail, reversing lower court and finding a "direct" loss); Aqua Star Corp. v. Travelers Cas. & Sur. Co., No. 16-35614, 2018 U.S. App. LEXIS 9660 (9th Cir. Apr. 17, 2018) (affirming district court decision holding exclusion in computer crime policy barred claim for loss caused by social engineering scam); Posco Daewoo Am. Corp. v. Allnex USA, 2017 U.S. Dist. LEXIS 180069 (D.N.J. Oct. 31, 2017) (travelers wrap and crime policy did not cover loss of money that was a receivable but not owned by insured when supplier's employee fell victim to fraudulent e-mail and wired funds to an improper account); Innovak Int'l Inc. v. Hanover Ins. Co., F. Supp. 3d 1340 (M.D. Fla. 2017) (court ruled that insurer had no duty to defend purported class action, given that the "personal and advertising injury" section of CGL policy did not cover a data breach when the insured did not publish the material); P.F. Chang's China Bistro, Inc. v. Fed. Ins. Co., No. CV-1501322-PHX-SMM, 2016 U.S. Dist. LEXIS 70749 (D. Ariz. May 31, 2016) (breach-related expenses imposed by credit-card processor bank against insured not covered due to exclusion for liability assumed by contract).

[45] tit. 23, § 500.00.
[46] *Id.* § 500.16.
[47] United States v. Kovel, 296 F.2d 918 (2d Cir. 1961).
[48] *See, e.g.,* the definition of "cybersecurity event" in the New York DFS Regulations, 23 N.Y.C.R.R. § 500.01(d).
[49] South Dakota Ch. 22-40 (2018).
[50] New York, for example, requires notice to consumers and to the Department of Financial Services via the DFS Web Portal 23 N.Y.C.R.R. 500.17(a); www.dfs.y.gov/about/cybersecurity.
[51] *See* ALA. STAT. §§ 45.48.010-45.48.090; MASS. GEN. LAWS ch. 93H; N.C. GEN. STAT. § 75-65.
[52] FLA. STAT. § 501.171(4)(a) (West 2014).
[53] N.J. STAT. ANN. § 56:8-163 c(1)–(2) (West 2006).
[54] Spokeo, Inc. v. Robins, 136 S. Ct. 1540 (2016).
[55] *See, e.g.,* Stevens v. Zappos, Inc., 884 F.3d 893 (9th Cir. 2018) (risk of future harm arising from theft of consumer private data is enough for standing); Dieffenbach v. Barnes & Noble, Inc., 887 F.3d 826 (7th Cir. 2018) (appeal court reinstated case finding standing, but cautioned that damages will be hard to prove); Attias v. CareFirst, Inc., 865 F.3d 620 (D.C. Cir. 2017) (grant of motion to dismiss class action reversed based on finding plaintiffs had adequately alleged the data breach exposed them to a substantial risk of identity theft that was "fairly traceable" to CareFirst); *In re* Supervalu Customer Data Sec. Breach Litig., 870 F.3d 763 (8th Cir. 2017) (court reversed in part lower court's dismissal finding that one of the named plaintiffs had sufficiently alleged actual injury when his credit card was fraudulently charged); Torres v. Wendy's Int'l LLC, 195 F. Supp. 3d 1278 (M.D. Fla. 2017) (plaintiffs seeking class-action status due to stolen credit-card information and alleged lost reward points and cash-back rewards as well as suffering restricted use of their credit cards*); In re* Banner Health Data Breach Litig., No. 2:16-cv-02696-PHX-SRB (D. Ariz. Apr. 2017) (court dismissed breach-of-contract claims but allowed purported class to proceed with data-breach-related allegations based on unjust enrichment, negligence, and violation of state consumer-fraud law).
[56] *See* Wade v. AMB Indus., Inc., No. 18-ch-03855 (Ill. Cir. Ct. Mar. 3, 2018).
[57] Paymentech, LLC. v. Landry's Inc., No. 4:2018cv01622, Complaint at 11 (S.D. Tex. May 17, 2018).
[58] *In re* Premera Blue Cross Customer Data, No. 3:15-md-2633-SI, 2017 U.S. Dist. LEXIS 178762 (D. Or. Oct. 27, 2017) (post-breach documents produced merely at request of counsel without legal purpose not privileged, including public-relations documents and forensic vendor's report, but drafts with attorneys' comments embedded may be privileged); *see In re* Experian Data Breach Litig., SACV 15-01592 AG (DFMx), 2017 U.S. Dist. LEXIS 162891 (C.D. Cal. May 18, 2017) (post-breach work product by forensic vendor protected by attorney-client privilege when vendor was specifically hired by outside counsel to assist counsel, and work was separate from pre-breach business function performed by same vendor); *In re* Target Corp. Customer Data Sec. Breach Litig., 2015 U.S. Dist. LEXIS 34554 (D. Minn. Mar. 19, 2015) (dual-track, post-breach investigation served to protect internal communications that had demonstrably legal purpose under either attorney-client privilege or work-product doctrine).
[59] Leibovic v. United Shore Fin. Servs., LLC, No. 15-12639, 2017 BL 301590, (E.D. Mich. Aug. 28, 2017), *mandamus denied*, 2018 U.S. App. Lexis (6th Cir. Jan. 3, 2018).

Panel

- **Cliff Dutton**
  Epiq, New York
- **David Fisher**
  Integra Ledger, Denver
- **Rebecca Fruchtman**
  Bank of America Merrill Lynch, Chicago
- **Elizabeth B. Vandesteeg**
  Sugar Felsenthal Grais & Helsinger LLP, Chicago
- **John G. Loughnane, Moderator**
  Nutter McClennen & Fish LLP, Boston

Agenda

- **Firms under Attack**
- **Protecting Data**
  Client Perspective, Ethical Considerations, Best Practices
- **Blockchain's Role in Keeping Data Secure**
- **Resources**

Firms Under Attack

"From patent disputes to employment contracts, law firms have a lot of exposure to sensitive information. . . . This makes them a juicy target for hackers that want to steal consumer information and corporate intelligence."

Dan Steiner,
Hackers Are Aggressively Targeting Law Firms' Data (Aug. 3, 2017)
https://www.cio.com

Firms Under Attack

THE WALL STREET JOURNAL.

$1 FOR 2 MONTHS

Home World U.S. Politics Economy Business Tech Markets Opinion Life & Arts Real Estate WSJ Magazine

WSJ PRO CYBERSECURITY

PRO CYBER COMMENTARY & ANALYSIS

Law Firms Increasingly Questioned Over Cybersecurity

By Adam Janofsky and Samuel Rubenfeld
Dec 29, 2016 5:56 p.m. ET

A surge in high-profile law firm data breaches is shifting the way businesses are shopping for lawyers, say cybersecurity experts, academics, and attorneys.

Clients with sensitive information like patents, medical records, and financial data are placing greater emphasis on data security when hiring a law firm, these experts say. Many businesses are starting to send their law firms cybersecurity questionnaires and request periodic vulnerability assessments.

Protecting Data – Client Perspective

Target:
Stolen information involved at least 70 million people

Vendor best practices

What you should know about your vendor

- Who is responsible if information is breached due to vendor action or inaction?
- Who is financially liable?
- Can you shift vendors/resources and recover quickly?

Best Practices

- Perform site review; leverage security and process experts in your company
- Allow vendor access only to required data
- Limit and segregate log-ins to mitigate potential breaches
- Address responsibilities and liability if your vendor becomes compromised and impacts your business
- Understand vendor's loss recovery processes and service level agreements currently in place
- Do your homework – check references, awards, company standards regarding product, data security processes, procedures to ensure balanced risk-reward decision
- Hold your vendor to the same "Best Practice" standards you adopt internally

Protecting Data – Ethical Considerations

- ABA Standing Committee on Ethics and Professional Responsibility "Formal Opinion 483" (issued October 17, 2018)
  - describes a lawyer's obligations under the Model Rules of Professional Conduct (MRPC) after an electronic data breach or cyberattack that compromises client data.

- Lawyers have a duty to notify clients of a breach, under Model Rule 1.4,
  - "in sufficient detail to keep clients 'reasonably informed,'" and
  - with sufficient explanation "to permit the client to make informed decisions regarding the representation."

Ethical Obligations

MRPC Rule 1.1

MRPC Rule 1.6

MRPC Rule 5.3 (Cmt. 3)

Best Practices

STEP 1: Become aware of threats

STEP 2: Analyze vulnerabilities

STEP 3: Inventory Data

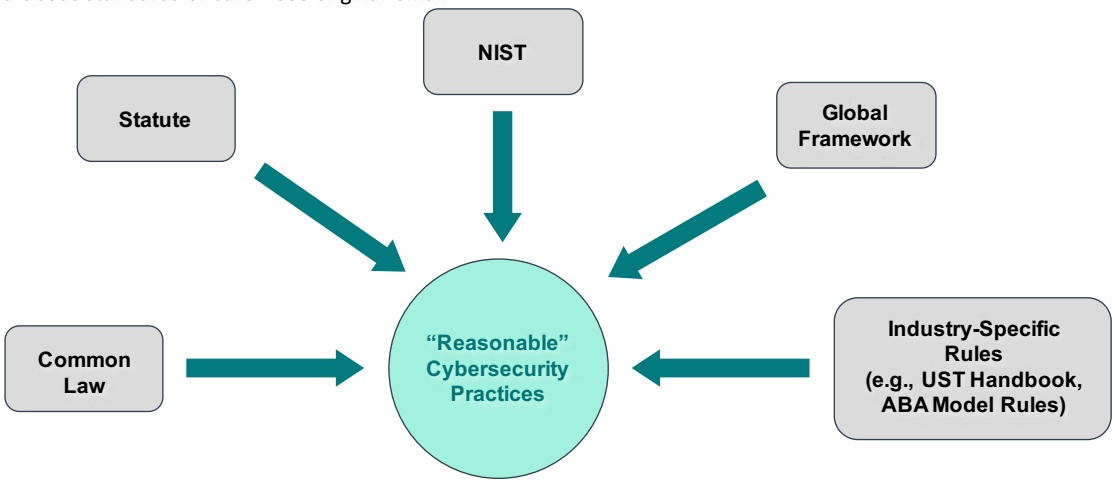
STEP 4: Understand the standard of care

STEP 5: Meet the standard of care

STEP 6: Develop and implement a security program

Best Practices

Subhead about standards of care – see original email



Protecting Data – Best Practices

- NIST Framework -- voluntary standards, guidelines, and best practices to manage cybersecurity-related risk.

Cybersecurity Framework Components

The Framework consists of 3 main components

Framework Core

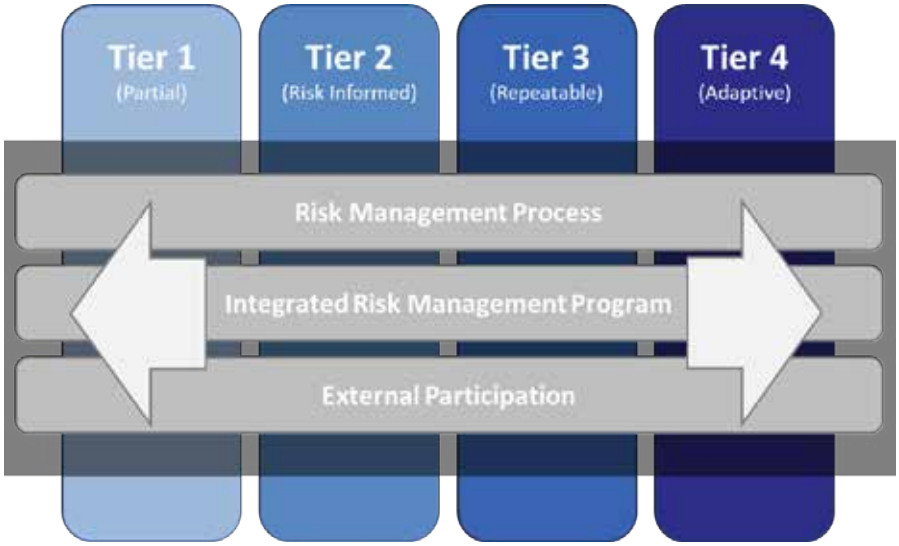
	Function	Category	ID
What processes and assets need protection?	Identify	Asset Management	ID.AM
		Business Environment	ID.BE
		Governance	ID.GV
		Risk Assessment	ID.RA
		Risk Management Strategy	ID.RM
		Supply Chain Risk Management	ID.SC
What safeguards are available?	Protect	Identity Management & Access Control	PR.AC
		Awareness and Training	PR.AT
		Data Security	PR.DS
		Information Protection Processes & Procedures	PR.IP
		Maintenance	PR.MA
		Protective Technology	PR.PT
What techniques can identify incidents?	Detect	Anomalies and Events	DE.AE
		Security Continuous Monitoring	DE.CM
		Detection Processes	DE.DP
What techniques can contain impacts of incidents?	Respond	Response Planning	RS.RP
		Communications	RS.CO
		Analysis	RS.AN
		Mitigation	RS.MI
		Improvements	RS.IM
What techniques can restore capabilities?	Recover	Recovery Planning	RC.RP
		Improvements	RC.IM
		Communications	RC.CO

Subcategories & Informative References

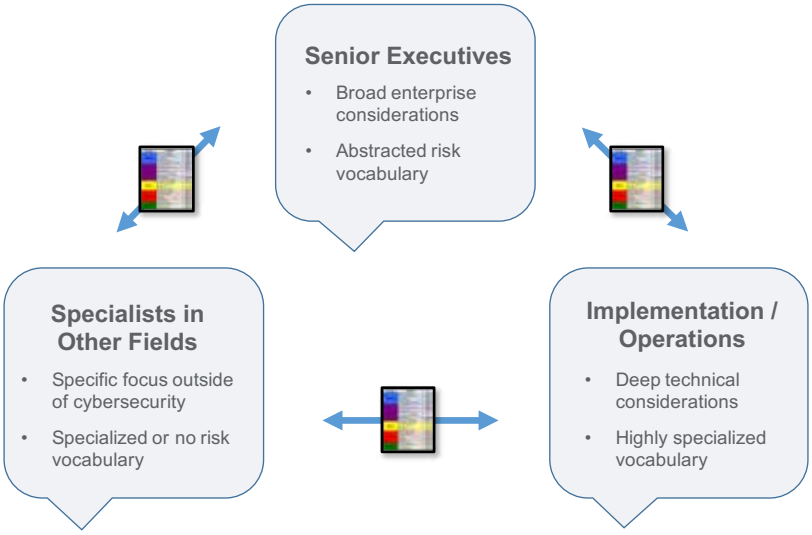
Function	Category	ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
	Supply Chain Risk Management	ID.SC
Protect	Identity Management & Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
Respond	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM
Recover	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

Subcategory	Informative References
ID.BE-1: The organization's role in the supply chain is identified and communicated	**COBIT 5** APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 **ISO/IEC 27001:2013** A.15.1.3, A.15.2.1, A.15.2.2 **NIST SP 800-53 Rev. 4** CP-2, SA-12
ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	**COBIT 5** APO02.06, APO03.01 **NIST SP 800-53 Rev. 4** PM-8
ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	**COBIT 5** APO02.01, APO02.06, APO03.01 **ISA 62443-2-1:2009** 4.2.2.1, 4.2.3.6 **NIST SP 800-53 Rev. 4** PM-11, SA-14
ID.BE-4: Dependencies and critical functions for delivery of critical services are established	**ISO/IEC 27001:2013** A.11.2.2, A.11.2.3, A.12.1.3 **NIST SP 800-53 Rev. 4** CP-8, PE-9, PE-11, PM-8, SA-14
ID.BE-5: Resilience requirements to support delivery of critical services are established	**COBIT 5** DSS04.02 **ISO/IEC 27001:2013** A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 **NIST SP 800-53 Rev. 4** CP-2, CP-11, SA-14

Framework Implementation Tiers



Core: A Translation Layer

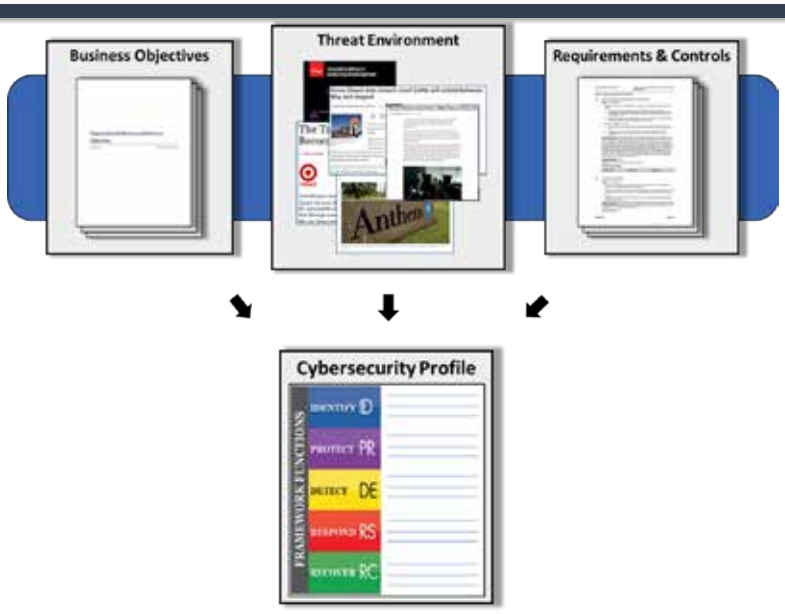


17

Framework Profiles

- Alignment with business requirements, risk tolerance, and organizational resources
- Enables organizations to establish a roadmap for reducing cybersecurity risk
- Used to describe current state or desired target state of cybersecurity activities

Building a Profile

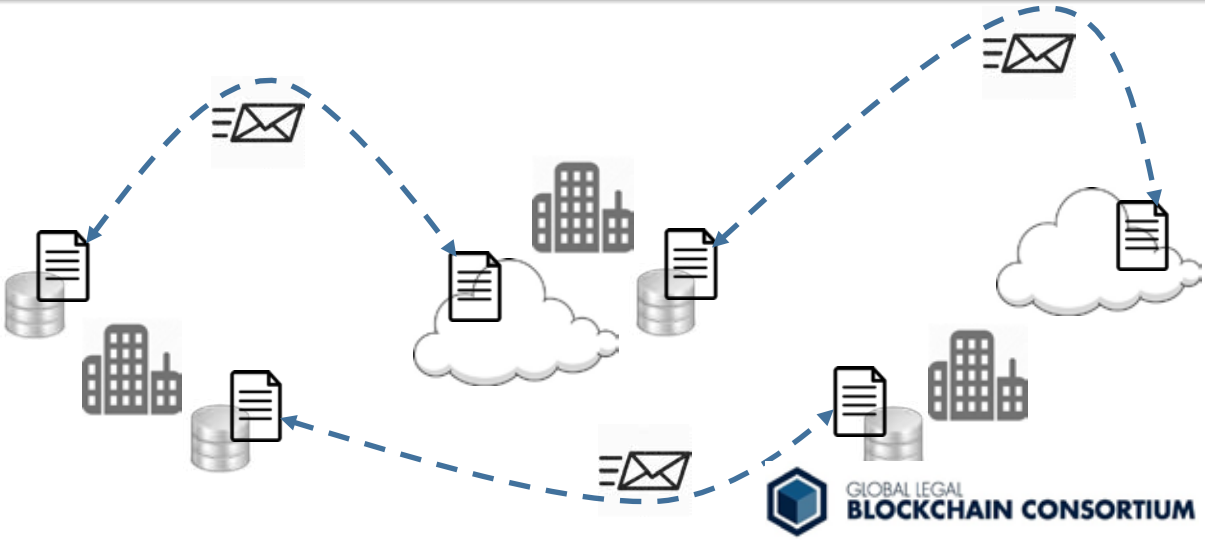


Resource and Budget Decision Making

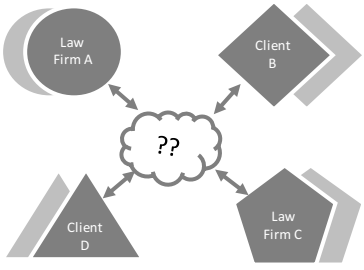
Subcategory	Priority	Gaps	Budget	Activities (Year 1)	Activities (Year 2)
1	Moderate	Small	$$$		X
2	High	Large	$$	X	
3	Moderate	Medium	$	X	
…	…	…	…		
98	Moderate	None	$$		Reassess

…and supports on-going operational decisions, too

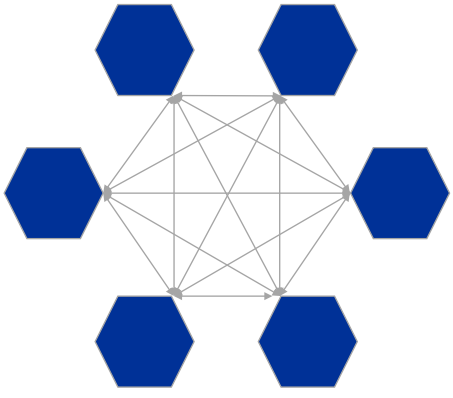
The world's document, contract, and legal data ecosystem is chaotic and vulnerable



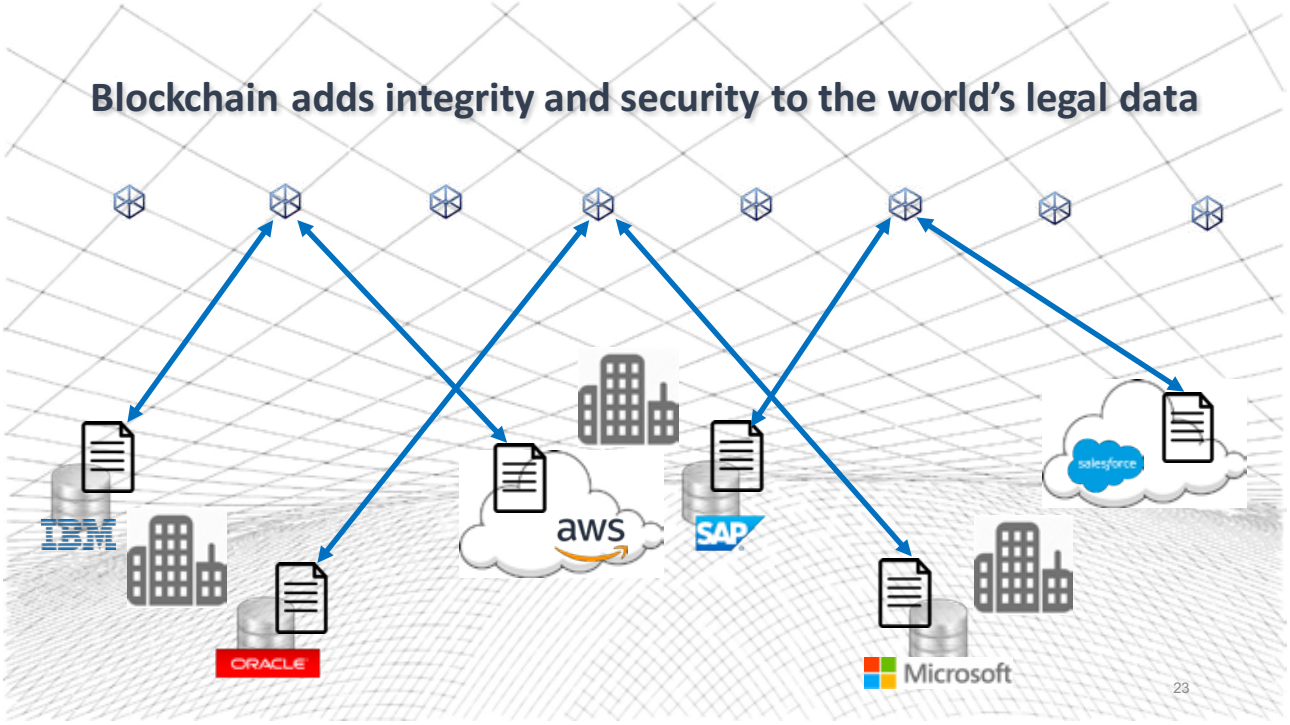
Blockchain solves the digital intermediary problem



Today: Trusted intermediaries



Future: Peer-to-peer trust



GLOBAL LEGAL
BLOCKCHAIN CONSORTIUM

Largest blockchain consortium in the world for the legal industry

www.legalconsortium.org

Resources

- Association of Corporate Counsel, *Model Information Protection and Security Controls for Outside Counsel Possessing Company Confidential Information*
- Corporate Legal Operations Consortium, *Cybersecurity Initiative*
- National Institute of Standards and Technology, *Cybersecurity Resources (including NIST Framework)*
- *American Bar Association, Cybersecurity and the Lawyers Standard of Care*
- *EdX, Blockchain Fundamentals*
- *Omar Barzilay, Contributor, Forbes, 3 Ways Blockchain Is Revolutionizing Cybersecurity*
- ABA Journal, *Lawyers can contribute to the rise of blockchain by understanding it*
- "The ABA Cybersecurity Handbook: A Resource for Attorneys, Law Firms, and Business Professionals, Second Edition"
- National Cyber Security Alliance (NCSA) – https://staysafeonline.org/about/
- US-CERT – United States Computer Emergency Readines Team – https://www.us-cert.gov/


HACKED
Questions?