MAYER·BROWN

Preparing For and Responding To a Computer Security Incident: Making the First 72 Hours Count

Preparing For and Responding To a Computer Security Incident: Making the First 72 Hours Count

Marcus A. Christian
Partner, Mayer Brown

Stephen Lilley
Associate, Mayer Brown

Table of Contents

Foreword

Cybersecurity impacts us all—as consumers, employees, shareholders, and citizens. Organizations of all shapes and sizes face a growing number of determined, sophisticated, and evolving cyber intruders. These individuals and groups plot to steal personal or proprietary information, and, increasingly, to disrupt or even destroy vital systems. No one-size-fits-all solution exists for addressing these threats. Board members, senior management, and in-house counsel instead can best respond by developing risk-based programs and policies to protect both the privacy and security of personal data, business systems, and other assets.

Preventive measures, such as maintaining firewalls, encrypting data, and monitoring threats are essential components of any such cybersecurity program. But the fact is that even the most robust network defenses can fail. At such moments, affected companies must be ready to respond—responsibly, promptly and capably—to the challenges of maintaining central operations, supporting their customers, and defending against legal actions. The stakes often are high, but a computer security incident does not have to inflict substantial damage: a company that responds effectively can significantly mitigate the resulting harm.

Effective incident response thus is a key element of a risk-based cybersecurity program. This capability will not emerge spontaneously. Rather, it is the product of careful and strategic preparation. That work typically is difficult and often is undervalued before a crisis. Resources devoted to readiness pay great dividends during a crisis, however, particularly if a written plan has been tailored to the risks facing the company, as well as to the systems, data, and other assets it seeks to protect. Likewise, the company will benefit if it has kept the incident response plan

current, for example by updating it to incorporate lessons from prior incidents, to respond to new regulatory requirements, or to reflect corporate acquisitions.

Strengthening a company's incident response capability is an ongoing process. Whether beginning that process or refining an established plan, *Preparing For and Responding To a Computer Security Incident: Making the First 72 Hours Count* will be a valuable resource for in-house counsel, executives, and other stakeholders as they undertake this important work.

Rajesh De

Partner, Mayer Brown
Former General Counsel, United States National Security Agency

Introduction

Perfect information security is unattainable. Accidents happen. Defenses fail. When they do, an organization's response can determine whether it suffers operational damage, reputational harm, and legal liability. This response capability will be tested under substantial time pressures and with serious consequences at stake. Assessing and enhancing a company's information security incident response capability thus are urgent matters for American boards, management, and corporate counsel.

The gravity of the information security threat facing businesses—through both cyber and more traditional means—is well-recognized. Highly-skilled and well-resourced groups of hackers constantly attack American networks.[1] Disloyal insiders seek to exploit company information for corrupt ends, and hacktivists pursue paralyzing cyber attacks for political or other non-monetary reasons. The risk of accidents or mistakes persists. In short, the threat of information security incidents—and particularly computer security incidents[2] —is substantial and growing.[3]

The incidents that firms suffer take many forms. For example:

- An employee or other insider may remove sensitive information. For instance, an IT contractor hired to improve security at a South Korean credit-evaluation company allegedly used a USB stick over the course of a year to steal the personal information of approximately 20 million South Korean credit card holders, more than one-half of the country's working-age population.[4]
- An employee may expose a company's network to a hacker by opening a corrupt attachment or hyperlink in an email directed specifically to him or her. Even the most

sophisticated entities are susceptible to such a "spearphishing" attack. News reports indicated in 2012, for example, that hackers used a spearphishing campaign to breach the systems of the White House Military Office.[5]

- A laptop may be stolen, exposing sensitive personal information. In one example in 2014, the Georgia Department of Behavioral Health and Developmental Disabilities reported that a government laptop containing protected health information was stolen from an employee's car, triggering breach notification requirements.[6]
- A distributed denial of service (DDoS) attack, during which a cyberattacker overwhelms a targeted computer system's resources and Internet connection, may shut down a company's website or reduce its ability to detect an intrusion. A security researcher reported in 2013, for example, that hackers used a DDoS attack on a bank to conceal their theft of $900,000 from one of its customer's corporate accounts.[7]
- A retailer's point of sale payment system may be compromised by malware (short for "malicious software") or a skimmer (an electronic device that records data from a payment card).[8] In response to one such threat, the Secret Service issued a 2014 alert warning that over one thousand US businesses had been affected by the "Backoff" malware, which allowed hackers to exfiltrate customer data.[9]
- Ransomware may deprive an organization of access to its own data. (Such attacks generally involve the malicious encryption of an organization's data and a threat to destroy the decryption key if a ransom is not paid.) For example, a Massachusetts police department lost access to vital computer files when its system was infected by the Cryptolocker ransomware in 2013.[10] The police department

paid a $750 ransom in Bitcoin to regain access to its information.

The consequences of information security incidents often are substantial.[11] The FBI has alerted American businesses to the significant insider threat posed by disgruntled employees and has noted that resulting investigations have identified costs of up to $3 million per incident to the affected companies.[12] The loss of trade secrets can cause competitive harms. Operations also can be significantly impaired. The Department of Homeland Security issued alerts in 2014, for example, warning critical infrastructure operators of malware designed to attack industrial control systems.[13] The endless stream of media articles about high-profile data breaches likewise makes clear the reputational harm that can flow from an information security incident. The list of possible harms goes on.

Effective incident response–the focus of this book–can substantially limit the economic harm and legal liability caused by an information security incident. Containing an intrusion before it reaches systems holding consumers' or patients' sensitive information may stop a data breach from ever occurring. Limiting the loss of a business partner's confidential commercial information may avert a contractual dispute and preserve a profitable alliance. And an effective response can promote customer loyalty, maintain employee morale, and forestall regulatory scrutiny. At a minimum, an effective incident response can help stop a bad situation from getting worse.

Preparation is the best guarantee of effective incident response. A written incident response plan can provide the basic structure for a response. The sponsorship and support of a senior corporate officer can ensure that the incident response capacity has the necessary authorizations and resources and is aligned with the business's long-term needs. Moreover, lessons learned from each incident response (and each incident response exercise) can

inform improvements in prevention and response practices and procedures, thereby continuously strengthening information security and the response function.

Effective incident response can bring substantial legal benefits. Although a company cannot control what plaintiffs' lawyers will do following a cyber intrusion, it can plan and direct its own actions. By guiding an organization's computer security incident response preparation and execution, counsel can seize the opportunity to develop facts upon which a client later may be scrutinized and judged. Did the company conduct a thorough post-intrusion investigation? Did it preserve crucial evidence? Did it detect a known threat quickly? And did it comply with customer notification laws? These are but a few of the questions that plaintiffs' lawyers, regulators, and pundits may ask in the wake of a breach. Preparation for, and effective mobilization during the first hours of, an incident can ensure that companies will respond from a position of strength.

This book is a resource for businesses and other organizations seeking to establish, evaluate, or strengthen their capacities to respond in the early hours of computer security incidents. Of course, this is only a start. Businesses face different and specific risks, and their current capabilities vary. A company's unique circumstances will determine the best way to prepare for and respond to a computer security incident. This book nonetheless should help an organization answer two related questions: (1) What should we do to respond effectively in the first 72 hours after discovering a computer security incident? and (2) Are we prepared to respond effectively?

The information herein is not intended to constitute legal advice, which should be provided only in the context of an attorney-client relationship. We nonetheless hope that this book will help boards, management, and corporate counsel in this important undertaking.

Computer Security Incidents

Effective incident response requires an understanding of likely computer security incidents. To this end, the familiar goals of maintaining the confidentiality, integrity, and availability of data allow companies to categorize the seemingly countless permutations of computer security incidents that they may face:

- **Confidentiality**: "A loss of confidentiality is the unauthorized disclosure of information."[14] Breaches of data confidentiality are the most familiar form of computer security incident. Stories about large-scale breaches of consumer financial data, health records, and other personal information have appeared with increasing frequency over recent months and years. In often less-publicized losses of data confidentiality, corporate insiders and network intruders steal companies' trade secrets.
- **Integrity**: "A loss of integrity is the unauthorized modification or destruction of information."[15] Cyber attacks may corrupt data and thereby sabotage affected systems. Investigators reportedly discovered a "logic-bomb" on trading systems in 2010, for example, that could have caused significant destruction.[16] Likewise, a report by the staff of the Federal Trade Commission on the Internet of Things described experiments in which researchers were able to use the Internet to gain remote control over cars' brakes and engines and the output of insulin pumps.[17]
- **Availability**: "A loss of availability is the disruption of access to or use of information or an information system."[18] DDoS attacks provide the most common example of incidents that interrupt the availability of company data. There, a hacker, often using a botnet, attempts to overwhelm a website with requests so that it no longer can resolve appropriate requests.

Though fairly simple in design, these attacks can have devastating effects.[19]

Computer security incidents can be further characterized along a handful of key dimensions.

Actor: Behind every computer security incident is a threat actor. Threat actors include disloyal insiders or contractors who have access to an organization's networks. They also include intruders who physically connect to company networks or who access company WiFi networks as they sit outside in the company parking lot. And of course, threat actors also include hackers and organized cybercrime groups of all kinds. For example:

- Hacking groups seek financial and other data that they can monetize through sophisticated and efficient online criminal marketplaces.[20]
- Hackers target accounting departments in hopes of wiring money abroad.[21]
- Hacktivists seek to embarrass a particular government or company.[22]
- "Advanced persistent threats" target American intellectual property.[23]

Security researchers have grown increasingly confident in identifying groups they believe are behind various cyber threats. However, the attribution of a computer security incident often requires the most sophisticated forensic analysis and the extended analysis of threat information over time. Attribution may be impossible in a particular incident. Moreover, even when a group behind a cyber attack can be identified, such knowledge often will not help to remediate systems or provide any basis for legal recourse.

Difficulties in attributing attacks and seeking recourse do not render investigations useless, however. As discussed later, even when companies cannot know exactly "who" is behind an attack, they can make good use of information about "what" types of attacks active groups are committing. Companies often can use even limited information. Knowing that a threat actor is likely to target a company again or the type of tool used can be valuable information for the company as it anticipates future risks.

Tool: Threat actors use a variety of tools to exploit American networks. These include:

- Socially engineered emails to employees – for example, purporting to provide the agenda for an upcoming conference – that deliver a malicious payload when a recipient clicks a link or opens a file;
- Exploits inserted into websites that infect those websites and their visitors in "watering hole" attacks;
- Malicious command sequences entered into applications and databases to exploit known programming errors (e.g., through buffer-overflow attacks); and
- Networks of compromised computers – or botnets – that hackers direct through a sophisticated command and control structure to undertake various criminal activities including sending spam emails, committing DDoS attacks, and facilitating wire fraud.[24]

Vulnerability: A tool must find a matching vulnerability to exploit. Such vulnerabilities need not be sophisticated. Very frequently, the vulnerability is an employee who clicks on a link in an unsolicited email, uses a common password, loses a company laptop, accesses company networks with a compromised personal device, or gives his or her password to a co-worker with more limited access privileges. Likewise, system vulnerabilities can be

simple. A known software flaw may be unpatched, for example, or a server may still have the factory-default password.

Of course, vulnerabilities also may be previously unknown, thus earning the moniker "zero-days." The Heartbleed and Shellshock bugs, for example, made clear that bugs may linger even in old and widely used code.[25]

Target and Objectives: As the various examples discussed above demonstrate, threat actors pursue a wide range of targets and objectives. Some, like ransomware purveyors, do not necessarily have any specific target, preferring instead to infect as many devices as possible to extort as much money as possible. Others target very specific forms of intellectual property with the goal of sale or delivery to sponsors, attack specific control systems for the goals of reconnaissance or sabotage, or hack particular companies either to show off their hacking skills or to prove a point.[26] The possible targets and objectives of actors causing a computer security incidents are virtually unlimited: anything that can be monetized or otherwise exploited is at risk.

Readiness

Time is of the essence in the wake of a computer security incident. And the failure to prepare can force an organization to waste stress-filled hours, if not days, searching for available people and companies with the necessary expertise to minimize the damage. In contrast, a pre-existing and well-prepared response team often can be mobilized and possibly contain a threat in short order. Thus, the most important actions that an organization can take to increase its response speed and effectiveness are those it undertakes to prepare for security incidents.

Building organizational readiness is hard work. It takes time, organizational buy-in, and both human and financial resources. It also raises numerous significant technical and operational questions. Preparation nonetheless is crucial. To that end, this section addresses how an organization can ensure that it has the right people, resources, vendors, and plans in place *before* it learns of an event that threatens the confidentiality, availability, or integrity of its vital systems or data.

Regulatory Expectations

Companies face a business environment that is increasingly saturated with regulatory requirements and de facto standards set through agency guidance. A company therefore will benefit from understanding these requirements and standards in advance of a computer security incident. A selection of relevant laws, regulations, and standards is discussed below.

THE FEDERAL TRADE COMMISSION

The Federal Trade Commission ("FTC") has asserted its authority to regulate data security practices through its "unfairness" authority under Section 5 of the FTC Act.[27] The FTC has made clear that it considers the development and execution of effective incident response plans to be an element of avoiding "unfairness" in the data security context.[28] This is a significant assertion of authority both because of the broad sweep of the FTC Act and because banking regulators have concluded that the FDIC Act grants them authority to enforce "unfairness" standards where the FTC lacks authority.[29] The FTC's position also carries significant practical implications, as the FTC has demonstrated not only that it will bring enforcement actions based on its own view of "unfairness" in this context, but also that it will subject companies to burdensome investigations after high-profile breaches. The civil investigative demands that have been released to date make clear the substantial number of questions that a company may face in the event of a breach (and thus should consider investigating during an incident response).[30]

THE SECURITIES AND EXCHANGE COMMISSION

Section 501(b)(3) of the Gramm-Leach-Bliley Act required the Securities and Exchange Commission (the "SEC") and members of the Federal Financial Institutions Examination Council (the "FFIEC") to "establish appropriate standards" for financial institutions "to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer."[31] The SEC promulgated Regulation S-P under that authority in 2000.[32] This regulation includes the "safeguard rule," which requires relevant entities to "[p]rotect against any anticipated threats or hazards to the security or integrity of customer records and information."[33] The

SEC has levied sanctions for violating this requirement through the failure to respond to information security incidents.[34] For example in 2011, the SEC fined the former chief compliance officer of a broker-dealer whose responsibilities included "maintaining and reviewing the adequacy of [the company's] procedures for protecting customer information."[35] In the words of the SEC, the "limited response or follow-up repeatedly revealed the firm's policies and procedures for safeguarding customer information to be inadequate."[36]

THE FFIEC

In 2001,[37] and again in 2005, the FFIEC members—the Federal Reserve Board, Federal Deposit Insurance Corporation, Office of the Comptroller of the Currency, National Credit Union Administration, and the Office of Thrift Supervision (later replaced by the Consumer Financial Protection Bureau)—clarified regulated entities' responsibilities under the Gramm-Leach-Bliley Act. *Their Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice* advised financial institutions to develop and implement response programs to "address unauthorized access to or use of customer information that could result in substantial harm or inconvenience to a customer."[38]

The FFIEC also has set the following general expectations for entities subject to the supervisory authority of its members:

> Every financial institution should develop an incident response policy that is properly integrated into the business continuity planning process. Management's ultimate goal should be to minimize damage to the institution and its customers through containment of the incident and proper restoration of information systems. A key element of incident response involves assigning responsibility for evaluating,

responding, and managing security incidents and developing guidelines for employees to follow regarding escalation and reporting procedures. Management should determine who will be responsible for declaring an incident and restoring affected computer systems once the incident is resolved. Individuals who are assigned this responsibility should have the expertise and training necessary to quickly respond in an appropriate manner. Financial institutions should assess the adequacy of their preparation by testing incident response guidelines to ensure that the procedures correspond with business continuity strategies.[39]

FINRA

The Financial Industry Regulatory Authority ("FINRA")—the self-regulatory organization for the securities industry—also has been increasingly active in addressing cybersecurity risks.[40] In February 2015, for example, FINRA issued "principles and effective practices" for responding to information security incidents as part of its report on cybersecurity practices.[41] These de facto standards cover the various elements of incident response and recommend that firms implement measures to maintain clients' confidence, including by providing credit monitoring in the event of a breach.[42]

THE DEPARTMENT OF HEALTH AND HUMAN SERVICES

Regulations issued by the Department of Health and Human Services under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") impose security incident response standards. Specifically, under 45 C.F.R. § 164.308(a)(6), covered entities must "[i]mplement policies and procedures to address security incidents," including those to "[i]dentify and respond to suspected or known security incidents; mitigate, to the

extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes."[43] HIPAA notification requirements are triggered when "such breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is a workforce member or agent of the covered entity."[44]

NERC/FERC

The North American Electric Reliability Corporation ("NERC") requires responsible entities to "document one or more Cyber Security incident response plan(s)."[45] The Federal Energy Regulatory Commission ("FERC") has mandated compliance with this standard and explained that its requirements include defining roles and responsibilities, procedures for handling incidents, communications plans, reporting to the Electricity Sector Information Sharing and Analysis Center, and annual testing.[46] NERC has brought enforcement actions before FERC for failure to comply with these requirements.[47]

The NIST Framework

Though only advisory, the framework for critical infrastructure cybersecurity issued by the National Institute of Standards and Technology (NIST) has been an important measure of government expectations regarding cybersecurity best practices. Notably, it includes incident response as one element of the Framework "Core" that identifies the particular functions that constitute cybersecurity best practices.[48] The Framework pushes responsibility for incident response (and other issues) to the management and board, as it is intended to enable consideration of cyber issues at all levels of the enterprise.[49]

STATE ATTORNEYS GENERAL AND REGULATORY AGENCIES

Forty-seven states, the District of Columbia, and multiple United States territories have data breach notification laws.[50] Many of those laws include incident response requirements. For example, the Maine Bureau of Insurance interprets the state's Notice of Risk to Personal Data Act to require a person or entity "who becomes aware of a breach of his or her computer system's security" to "investigate the problem in good faith, reasonably and promptly" to meet the goals of (1) "determining the scope of the security breach" and (2) considering "what measures are necessary to restore the reasonable integrity, security and confidentiality of the data in the breached system."[51]

Other state agencies have begun to act on cybersecurity issues more broadly. The New York State Department of Financial Services, for example, announced plans in December 2014 to expand its examination procedures of information technology "to focus more attention on cybersecurity." The examination process will include reviewing companies' "[i]ncident detection and response processes, including monitoring" and integration "of information security into business continuity and disaster recovery policies and procedures."[52] In preparing for the examinations, businesses will have to "[p]rovide a copy of, to the extent it exists in writing, or otherwise described, the organization's incident response program, including how incidents are reported, escalated, and remediated."[53]

Structure of the Plan

A written computer security incident response plan ensures that business priorities guide the response function. To achieve this goal, an incident response plan provides clear directions while avoiding becoming a checklist. The plan, in other words, provides

the structure within which the response team will be able to make the best decisions for the enterprise. While somewhat oxymoronic, an effective plan enables a sort of structured agility through which the response team is empowered to make decisions within the framework of the plan. It also promotes accountability by establishing processes and metrics against which the incident response team can guide and measure itself—and be measured by management.

Regulators have emphasized the need for a risk-based approach, including development of an incident response plan that is appropriate for the scale and complexity of an entity's operations.[54] While a computer security incident response plan must be specific to the needs and priorities of a given business, such a plan typically will:[55]

- State the goals and objectives of the plan;
- Categorize the types of incidents to which the plan applies;
- Establish incident severity categories and corresponding levels of deployment;
- Identify the membership of the incident response team for different incident types, as well as the respective roles and responsibilities of the team members;
- Provide key action steps, including:
    - Incident detection, notification, analysis, and forensics;
    - Response actions, including containment, remediation, and restoration;
    - Communications;
    - Procedures to capture lessons learned; and

- Identify necessary documentation, such as an incident response checklist, and key legal requirements (e.g., notification responsibilities).

How a company states these or other elements of its computer security incident response plan will substantially influence the effectiveness of its incident response function.[56] A computer security incident response plan accordingly should not be taken straight out of the box. A company instead should consult with technical experts and counsel to create (and then maintain and update) its computer incident security response plan. In doing so, the company should ensure that this plan complements other related corporate plans including the company's broader information security plan, its business continuity plan, crisis communications plan, and privacy policy.

The Response Team

A computer security incident ultimately is a *business* problem, not just a technical problem. An effective response team therefore is interdisciplinary.[57] It will include technical experts on topics such as threat containment and system remediation and restoration. But it also will be able and authorized to address the various legal, regulatory, public relations, and customer care issues that a computer security incident may present.[58] This team likely also will call on external experts when responding to complex incidents.[59]

RESPONSE TEAM LEADER

An effective computer security incident response will need a leader. Because of the many legal challenges that arise during and following incident response, in-house or outside legal counsel often serve as team leaders (or co-team leaders). However, chief

information officers, chief information security officers, chief privacy officers, business managers, external consultants, and others may serve in this capacity. Broadly speaking, the leader will manage and coordinate the team's efforts as it executes the response plan. This individual's responsibilities will include, among other things, identifying key actions, monitoring team members' progress, and resolving conflicts or problems that may arise. The team leader also communicates regularly with senior executives and directly or indirectly ensures that the response team has the necessary resources. Moreover, a team leader can foster coordination and communication among the team members by scheduling and holding regular update meetings.

INTERNAL MEMBERS

Business Manager: An incident response team should include members who can manage the business priorities embodied in the incident response plan and ensure accountability of the response team to the company's senior management. Some corporations may fill this role with a representative of an affected business unit, whereas others may designate a particular office to serve this function on a dedicated basis.

Information Technology: A company's information technology staff has an important role to play in the response to a computer security incident. These team members contribute a detailed understanding of company networks and systems, can provide and review relevant logs, can administer patches or other remedial tools, and can help assess the technical consequences of various contemplated actions. Information technology departments also may have advanced capabilities, such as an advanced digital forensics capacity. Companies will benefit, however, from realistic expectations about the services their

information technology departments (as opposed to external experts) will provide.

Information Security: Any Chief Information Security Officer should be represented on an incident response team. That representative can contribute a detailed understanding of the company's existing information security policies and practices. He or she also is more likely to be trained in digital forensics and to have current knowledge of digital threats and responses. Again, however, a company will benefit from understanding the limitations of these resources. Only a very limited set of businesses can afford to maintain an information security team of the scale and sophistication to address complex computer security incidents. And even assuming that a business determines that maintaining such a team makes economic sense, dedicated and expert external providers still likely will make unique contributions to responses to the most sophisticated computer security attacks.

Corporate Counsel: An incident response team will face numerous questions about relevant legal requirements, regulatory obligations, and privacy issues. The company's legal department thus has a central role to play in any computer security incident response team. This role includes determining when to bring in outside counsel.

Communications: An incident response team likewise may face various communications challenges as result of a computer security incident. Customers, regulators, investors, and elected officials may look to the company for information about the incident. Any reply may prove significant by shaping both public perception and the course of future litigation. The incident response team thus should aim to provide prompt and effective communications where possible. Often, it will only be able to do so if it has established a mechanism through which priority

communications can be approved promptly by corporate leadership.

Customer Care: Although not involved in any technical response to the incident, a company's customer care function can support the work of the incident response team. A failure to provide adequate customer care or information in the aftermath of a computer security incident may have long-lasting effects on a company's business. Conversely, a company may benefit significantly from leveraging its customer care function in a response to an incident that disrupts product delivery, threatens customers' personal information, or otherwise triggers customers' concern.

Compliance: A company's compliance function maintains various mechanisms to discover wrongdoing and other compliance risks. The compliance unit's mechanisms, which usually include an anonymous reporting hotline, provide an ongoing means of incident detection, particularly for incidents involving insiders. Moreover, during incident response, the compliance department can work to ensure that an organization meets statutory, regulatory, and contractual obligations triggered by a computer security incident.

Physical Security: The security department normally will be involved with securing the physical location of affected servers and other critical areas during incident response. Moreover, the security department may be responsible for securing the incident response team's war room and facilities used for business continuity.

Human Resources: Some incidents will involve employees or former employees. An organization's human resources department can provide timely information pertinent to the investigation of an employee or former employee who may have been involved in a computer security incident. In addition,

human resources professionals can advise managers about permissible ways to protect the business from the threat posed by an employee suspected, but not proven, to have contributed to a computer security incident.

EXTERNAL MEMBERS

Technical Expertise: Specialist digital forensic, remediation, and recovery skills may strengthen the response to a complex computer security incident. Of course, a business will not want to invest in bringing the mostly highly skilled—and highly paid—technical experts to bear on an incident that could be resolved more economically. But false economies also may hurt businesses here—a business does not benefit if an internal team fails, after great delay and harm to the corporation, to resolve an incident before the company engages an external team with the necessary expertise and experience.

Outside Counsel: The numerous legal requirements and issues associated with a computer security incident also frequently demand the participation of outside counsel. While they may not need to participate in addressing a more limited incident, outside counsel frequently play a "quarterback" role in responding to complex computer security incidents. This is not only because of the centrality of legal and other compliance issues in a computer security incident, but also because of the significance of the investigatory function in a response, the need for an effective conduit between the various team members and management, the possible need to work closely with members of law enforcement, and the increased privilege and confidentiality protections that generally are available in the relationship with outside counsel (which are discussed further in the next section).

Crisis Communications Specialist: Computer security incidents also can demand specialized communications skills. A company

will face important decisions about the content, timing, and medium of its communications and often will benefit from the advice of an experienced crisis communications specialist. A company may want to follow up on a formal corporate announcement, for example, by reaching out through emails or social media to its customers to highlight the steps the company is taking to safeguard their information or minimize any resulting harms to customers. This approach—like every other communications strategy in the aftermath of an incident—bears risks. A crisis communications specialist can help a company weigh the risks and benefits of different approaches and otherwise help it navigate a perilous media landscape.

RELEVANT ADDITIONAL THIRD PARTIES

Other third-party providers also may have important roles to play in an incident response, even if they are not formally integrated into the incident response team. These include:

- **Internet service providers**: A company should have a close working relationship with its Internet service provider and a clear understanding of the services it may be able to deliver in the event of a computer security incident.
- **Software and hardware vendors**: A company likewise should know the appropriate point of contact at its software and hardware vendors, so it may secure prompt assistance in the event that a vulnerability is discovered in such a product, a remediation strategy implicates the product, or another issue arises that requires the input of the product vendor.
- **Industry working groups**: The various industry-specific information sharing and analysis centers (ISACs) and other industry working groups collect and disseminate valuable threat intelligence as well as timely information about

successful defense and remediation strategies. Engagement with such a group during an incident response thus may help contain or limit the harm of a computer security incident.

- **Insurance provider**: A company may be under a contractual obligation to notify its insurer—and particularly an insurer that provides a cybersecurity policy—in the event of certain computer security incidents. (It also may be required to share its incident response plan with the insurer during underwriting.)
- **Law enforcement**: Engagement with law enforcement agencies can raise a host of complex legal issues for a company. Those issues can be best addressed if the company has an ongoing relationship with appropriate agencies, designates a response team member (e.g., external counsel) to contact law enforcement, and identifies points of contact at relevant law enforcement agencies.
- **Other governmental agencies**: A range of other governmental agencies may be relevant to a company's response to a computer security incident. Federal or state CERT teams may have a role to play in supporting the remediation and recovery processes. Notification to regulatory agencies also may be necessary.[60] Here again, companies benefit from building relationships with such agencies in advance.

Relationship Management: The importance of building relationships with external members of the response team and with other third parties in advance of a computer security incident merits emphasis. Technical teams and outside counsel will be most useful if they are engaged in the response within 24 hours after a computer security incident is detected. Waiting until an incident occurs before first contacting such external providers is sure to result in undue delays. A company consequently will benefit from developing relationships and expectations in

advance so that it knows whom it will call when an incident occurs as well as how those parties will respond. To that end, a company should consider contracting with external security contractors and engaging outside counsel in anticipation of a future computer security incident and should ensure that relevant team members know when and how to contact those external team members.

Logistical Needs

A computer security incident response team may benefit from various logistical supports. These include:

Dedicated Laptops: A computer security incident response team needs basic resources that permit it to assess and respond to a computer security incident. This includes the availability of dedicated laptops, loaded with appropriate software (e.g., packet sniffing software, etc.), that the response team may connect to a compromised network. The availability of a laptop that can be compromised (and subsequently restored) is essential to many, if not all, incident response scenarios. And of course, the response team will want to use various laptops and other devices that the team will keep separate from compromised networks and use to record, assess, and respond to the incident.

Secure Communications: A computer security incident may degrade or otherwise compromise the company's communications systems. A company should be prepared to ensure that members of the response team can communicate effectively and securely. Companies may wish, for example, to consider maintaining a supply of mobile phones that can be activated and used in the event of a loss of secure communications.

War Room: The response team may benefit from the availability of a dedicated space for coordination and communication, ideally one with access to systems that are likely to be needed by and relevant to decision makers. A company accordingly may wish to plan in advance how it will provide a war room in the event of a computer security incident.

Call Center: A computer security incident that results in a large-scale compromise of consumer information may prompt equally large-scale engagement with customers. Companies may decide to reach out proactively and thus preempt customer calls, and they may create a dedicated call center to address customer questions and concerns. Companies therefore may wish to consider identifying the provider (or internal capacity) they would use to address such a future need.

Training and Exercises

Practice strengthens a company's incident response function. Such practice can take many forms. Response team members may be trained on the practical significance of the incident response plan as well as lessons learned in prior incident responses. Team members also may meet to discuss how to respond under various possible scenarios. In addition, the team may practice its response through table-top exercises or other simulations.

Oversight of training and exercises provides corporate counsel and company management with an opportunity to ensure that the response team constantly works to be as well-prepared as possible to respond to computer security incidents. To that end, they can assess the quality of the training and exercises undertaken by the response team. Updating or replacing stale materials that do not reflect current best practices within the

company or the industry likewise can enhance the incident response capacity.

Threat Knowledge

Company networks face various threats, as discussed above. Understanding those threats as they apply to the particular information that a company holds, as well as the particular systems the company employs, is a key element of proper preparation by the response team and by the company more broadly. To put it bluntly, every company is a target. Fortunately, much information about the threats facing businesses is available. Relevant information sharing organizations (e.g., the relevant ISAC) and other industry groups provide threat information, and regulators increasingly expect companies to avail themselves of such information.[61] Service providers likewise can provide valuable threat intelligence (e.g., through the managed services offered by an Internet service provider or through a security vendor). Even when this threat information does not prevent an attack, companies that work with such third parties on an ongoing basis generally will be better prepared to address a computer security incident.

Active Response

A company must turn theory into practice when a computer security incident occurs. This is active response: the execution of the incident response plan to restore systems, minimize consequences, and reduce future risk. Here, we summarize best practices for incident response, including the recommendations of NIST and the Department of Homeland Security (DHS).[62] We emphasize, however, that the appropriate processes for an individual business will depend on its unique circumstances.

Ongoing Priorities

INVESTIGATING THE INCIDENT

A response team identifies and records the material facts of a computer security incident. It accomplishes this function through a number of key tools, including technical means (e.g., forensic network assessment), administrative evaluations (e.g., assessing whether policies and procedures were followed), and interviews of relevant personnel. For example, an effective investigation will: (1) maintain privilege (see below); (2) ensure confidentiality; (3) build facts in a logical and constructive order; (4) reflect the credibility assessments of the investigators; (5) respect the privacy rights of individuals whose data may be held within the compromised systems or may be subject to packet-sniffing or other technological tools; and (6) record the company's own good-faith efforts to identify the source and nature of the injury.

Learning what happened is not the only goal of active response. Trying to find a culprit may add little in some circumstances. A company that knows that a sophisticated criminal hacking ring in Eastern Europe was behind a spearphishing attack may only gain

diminishing benefits, for example, from learning more about the precise identity of the perpetrator.

Investigation nonetheless remains at the core of active response. A company with inadequate or incomplete information will struggle to make effective decisions about how to defend its networks. An informed company, in contrast, can rebuild stronger on a sound foundation.

MAINTAINING PRIVILEGE

Counsel have an important role to play during any incident response, and their role grows even more important in the event of significant incidents. Employing counsel in a central role can both provide the company with valued privilege and help the company anticipate the legal risks it will face. Using outside counsel can enhance these benefits, because the work that they perform, as well as the work of consultants they retain (e.g., forensic experts), generally enjoys a greater presumption of protection under the attorney-client privilege and attorney work product doctrine than the work of in-house lawyers. (Courts may scrutinize the actions of in-house counsel more closely for signs that the lawyer was acting as a business advisor rather than as a legal advisor.)

Having a counsel as a member or a leader of the incident response team does not throw a curtain of privilege over every element of its activities. While protections vary by jurisdiction,[63] communications with attorneys for the purpose of seeking legal advice likely will be protected by the attorney-client privilege. Those protections can reach any employee who is directed to speak to counsel for the purpose of obtaining legal advice, but courts have frequently indicated that the privilege is more likely to apply in the event that senior employees speak with company counsel, rather than if counsel speak with more junior employees.

Companies accordingly should establish clear and reasonable expectations about who will speak with counsel for the purpose of obtaining legal advice and what communications will be protected. Likewise, companies should set clear expectations about who may waive those protections and in what circumstances. An incident response may involve a large number and a wide array of third parties, including representatives of law enforcement, regulatory agencies (which may return later in an adversarial capacity), and the company's auditors or insurers. Disclosure of attorney-client communications to any such third parties most likely will waive the privilege for those communications and, possibly, for other undisclosed attorney-client communications on the same subject. Discipline about privilege and confidentiality accordingly is very important. Employees should be asked to keep conversations with attorneys confidential. Privilege considerations should be maintained even when speaking with board members. Warnings also should be given where appropriate to ensure that employees understand that any privilege belongs to (and can be waived by) the company. And communications should bear an appropriate legend that indicates coverage by the attorney-client privilege and (as discussed next) work product protections.

Large portions of a counsel's investigation during an incident response also may be protected by work product protections (which likewise vary by jurisdiction).[64] An internal investigation must be conducted in anticipation of litigation to qualify for protection as attorney work product. To that end, the entity that asks the counsel to participate in or lead the incident response should authorize, in writing, the attorney's investigation into the incident. The letter should indicate that counsel is being retained to develop factual information for the purpose of providing advice concerning potential liabilities and claims against third parties and its own employees, as well as to defend the company in

anticipated potential litigation and to recommend future legal actions, such as improved compliance programs. The letter should indicate the basis for anticipating possible litigation by the government or a private party.

MAXIMIZING COORDINATION

Collaborative and constructive coordination helps the incident response team achieve its goals. Such coordination is enhanced when the members of a response team understand their roles and responsibilities and how they relate to the roles and responsibilities of other team members. Teams also must effectively communicate tasks and goals throughout the active response process. In addition, team structure and leadership will dictate the best methods for developing and communicating strategy, and the stress of incident response may raise challenges. But the goal remains the same: ensuring that the entire response team is executing a single strategy in a coordinated manner.

ENSURING HIGH-VALUE COMMUNICATIONS

Coordination will not be possible without adequate means of communication. A computer security incident may pose significant communications hurdles, however. Use of the company's existing communications system may be impossible or imprudent after an incident. As NIST has explained, "[c]apacity planning is needed because different types of threats (e.g., natural disasters, targeted cyber attacks) can result in a reduction of the available processing, telecommunications, and support services originally intended to support the organizational missions/business functions. Organizations may need to anticipate degraded operations during contingency operations and factor such degradation into capacity planning."[65]

MAINTAINING DISCIPLINE

Companies can suffer self-inflicted and unnecessary injuries in the response process. Self-serving or panicked emails are a leading culprit, particularly as the consequences of a breach tempt employees to create a permanent digital record that their prescient wisdom had gone unheeded. Emails along those lines are unhelpful and unprofessional. They also may be the difference between the company facing a lawsuit or receiving sympathy. It does not matter whether the emails are false, misleading, or later recanted—the damage of a lack of discipline already will have been inflicted.

DOCUMENTING ACTIONS AND FACTS

Investigators should document a broad set of facts and actions, including the information gained from forensic analysis, witness interviews, and other investigatory techniques. The documentation of the nature, time, purpose, sequence, and effect of actions taken by the response team can establish the thorough and responsible manner in which the company investigated the incident and mitigated the ensuing harms. Such records may prove invaluable during subsequent discussions with regulatory or enforcement agencies, or in civil litigation or government enforcement actions that follow. They certainly will advance efforts to learn from the incident. These facts, properly documented, also are key to the accountability of the incident response team to company management. Memories fade rapidly and may grow increasingly self-serving over time. Documenting actions and facts as they occur will allow responsible management to recognize the mistakes and successes of the active response process and derive appropriate lessons in response. Response teams accordingly should consider assigning responsibility to an appropriate team member—possibly a

representative of inside counsel—to keep the official record of actions taken and decisions made while being sensitive to the risk that such a record may be subject to review by regulators or produced in litigation.

NOTIFYING REQUIRED THIRD PARTIES

The company may be under legal obligations to notify various third-party entities very soon after a computer security incident. Contractual obligations may require notification to business partners, service providers, or insurers. Various statutes or rules may require the disclosure of a breach of personally identifiable information to law enforcement or regulatory agencies.[66] The incident response plan should account for many of the necessary notifications in advance, but without knowing the impact of a computer security incident and the accompanying legal requirements, team members will be unable to know, in advance, all of the notifications that will be required. Thus, the active response process includes assessing and reassessing the need to deliver such notifications—and it may even include delivery.[67]

Phases of Active Response

The process of actively responding to a computer security incident can be unpredictable, defeating neat categorization. Discussed below are the general phases of an active response, with a particular emphasis on legal issues that may arise.

LEARNING OF AN INCIDENT

An organization may learn about its incident from many sources. A company may discover an incident through an automated systems it has put in place, such as network monitors, traffic

analysis applications, or intrusion detection systems. But a company also may learn about an incident from non-technical sources. An employee may call a dedicated hotline after noticing that the website has been defaced or receiving an email threatening to lock various network assets unless certain demands are met. The news of an intrusion may come from a government agency, particularly if it is a significant incident. The first indication of an event even may come in the press.

Each source of incident discovery has different ramifications.

- A government agency may disclose only limited information about an incident to protect sensitive sources and methods. The agency may seek information about the company's systems, forcing the company to confront a broad set of privilege, confidentiality, and privacy issues.
- A security researcher may know less, but be willing to share more. Disclosure by such a researcher may limit the company's control over public understanding of the incident at issue.
- A cyber criminal's ransom demand is itself evidence of a felony and should be handled accordingly.
- Notification through the press may put a company on the defensive and pressure it to let its public reaction get ahead of its analysis.

Of course, the first evidence of an incident may be only the tip of the iceberg. Learning of network anomalies may be followed swiftly by discovery of an extensive and long-standing network compromise. Either way, any initial information should be gathered and then routed to and evaluated by appropriate members of the incident response team.

IDENTIFICATION AND TRIAGE

Alerting the Response Team: Notifying the response team of an incident in a systematic and pre-planned manner sets the structured and organized tone that is invaluable to any breach response. Companies should be sensitive to the fact that responding to incidents can be hard and stressful work. Alerts that provide useful information to the response team will support those teams more effectively than dumps of raw log data that have not been processed through appropriate algorithms or other filters.

Most basically, an alert should convey who has responsibility for the initial response and what those initial responsibilities entail. To the extent that the response team already has a basic playbook providing plans for various scenarios, the alert should be tailored to those concepts and expectations.

Companies also should consider how and when to notify third-party members of the response team. External counsel should be notified as soon as possible after the company determines that it is experiencing an incident that reaches a predetermined threshold of some measure. Generally, more incident response team event awareness is better, but there are limits. External counsel do not need to know about every network anomaly. However, it is preferable to provide an initial notification to alert counsel and then provide a subsequent all-clear message, than to defer notice and then discover that counsel cannot get to the company's location within the necessary time frame.

Determining Incident Type: Categorizing and prioritizing an incident is a crucial step in any successful response.[68] The gathering of relevant facts should be done urgently, but methodically. The steps taken should be memorialized to record how the team reached its conclusions, how it ruled out alternative

theories, and how it remained alert to other scenarios that it could neither confirm nor reject.

This process should allow the response team—working through an assigned principal investigator—to determine the nature of the incident and the proper technical response. These include:

- Whether the incident is ongoing;
- Which systems are implicated and whether they include high-value or business-critical systems;
- Whether the incident is contained;
- Whether the incident involves the compromise of the confidentiality, integrity, or availability of systems;
- Whether personally identifiable information, financial records, intellectual property, or other assets have been compromised;
- Whether there is evidence of a breach of a technical control, or whether an intruder has exploited access to network credentials, such as by first tricking an employee into providing a network password;
- Whether the intrusion had a clearly discernible goal; and
- Whether third-party systems are implicated in a manner that will materially affect incident response.

Answers to these questions may trigger decision trees that are complex in theory but common sense in practice. If an incident is the work of an employee on his last day before joining a competitor, for example, the team likely will need to secure physical work stations and take available and legal steps to prevent the employee from walking out with a thumb drive full of trade secrets. But if the response team thinks that is only one of three explanations for the incident, it likely will need to take more

limited steps while simultaneously assessing the likelihood of the other possible scenarios.

Of course, the response team may only be able to provide partial answers to many of these questions. A key function at this step, however, is to provide understandable assessments of the incident as quickly as possible to the rest of the team and then to business managers as appropriate. Regardless of its uncertainty, a response team should provide clear and appropriately qualified assessments based on established criteria. It also should describe the reasonable steps taken to understand and categorize an incident. Meeting such expectations not only is a matter of good business practice but is also key to limiting liability in the event of future litigation. An executive who understands the information provided—including its limitations—can make better decisions than one who must piece together relevant facts from a disorganized update. Similarly, a response team that follows rational processes, documents its steps, and enables oversight by management strengthens the company's response to the scrutiny of regulators, enforcement agencies, and private litigants.

Estimating the Scope: Understanding the scope of an incident also is crucial to threshold determinations of how to structure and prioritize a response. An incident may have been contained in a limited corner of the company's networks when a device was patched automatically. Another incident may have spread virulently across the company's network.

Incident scope should be measured by more than the number of devices affected. A complex intrusion into a limited set of systems may prove much more significant than the effects of a new malware variant that has been spread broadly but that can be removed automatically. The response team again should gather information that permits informed decision-making: the number of accounts or the volume of personally identifiable information

compromised; the volume of data exfiltrated; and the cost or person-hours necessary for recovery (among other facts). The nature of the incident, the kind of systems at issue, and the nature of the business all will help determine which information should be prioritized in assessing and communicating the scope of an incident. That information will permit informed decision-making within the response team about how to scale and structure the response, as well as responsible oversight by relevant management.

Mobilizing Resources: Decisions about the resources necessary for a response can be driven first by the data gathered in the initial response and then revisited as additional data is provided. As elsewhere, it is not essential that the response team make exactly the correct decisions at first. Most important is that prudent processes are followed, decisions are documented, and an iterative process is put in place that uses further data to refine those decisions as need be.

Key resources that a response team should consider mobilizing include:

- Secure communications;
- A command center;
- Additional laptops or other devices for the response team; and
- Additional personnel.

Regardless of what resources are chosen for a response, decisions should be communicated clearly and promptly. Incident response team members should understand the resources that will be available and have the opportunity to provide feedback as the response matures. Individuals responsible for making resources available and operational also will benefit from clear instructions and expected delivery times.

Preserving Evidence: A response team is very likely to find itself walking into a crime scene. Quickly restoring this crime scene to its proper state—by restoring systems to a known state—may be a business imperative. Minutes wasted can cost businesses significant productivity and economic losses or customer good will. But restoring systems to operating status is almost certain to destroy crucial evidence. Doing so may prevent a business from understanding the incident sufficiently to improve the entity's security going forward, harm any future defense in private litigation or regulatory enforcement actions, or prevent law enforcement from pursuing the perpetrators or collecting intelligence.

The response team thus may face the competing prerogatives of evidence preservation and protecting customers and information. As noted previously, preparation is a great advantage for companies facing such challenges. Organizational buy-in also will support the incident response team here as elsewhere. A team that is bombarded by high-level executive demands to get a website back online at all costs will serve a business less effectively than one that is held accountable to a plan that has enterprise-level support. Clear, risk-based, and context-specific decision-making is preferable here, not just an ability to follow executive demands to restore revenue-generating systems at all costs.

Each of the following also should be considered during the evidence preservation process:

The business will benefit from a clear understanding of the evidence held by third-party providers and of the mechanisms that can be used to access that evidence.

- It will be important to maintain and record a chain of custody over complex forensic evidence. This evidence may be crucial in litigation, whether with a private party or a business

partner, but efforts to use it at trial will be frustrated if the forensic expert cannot testify to the means by which it came into his or her possession or to the way it previously had been gathered or stored.[69]

- The company may be under a legal obligation to preserve data in anticipation of litigation. In some circumstances, counsel also could be under an ethical obligation to help the company avoid future sanctions for spoliation.[70]

ASSESSING LEGAL RAMIFICATIONS

A company that has suffered a computer security incident may face multiple rounds of costly private litigation and government enforcement actions. A detailed assessment of all of those interrelated risks is beyond the scope of active response. Nonetheless, the incident response team—and particularly the counsel serving on that team—will want to assess the legal obligations that result from the security incident. Key questions for counsel include:

- Whether personally identifiable information has been compromised and whether the incident triggered reporting requirements under various breach notification statutes;
- Whether the incident involved the compromise of information subject to a contractual obligation to disclose, such as data belonging to a joint venture in which each partner has a contractual obligation to inform the other if that data is compromised;
- Whether the incident triggered reporting requirements to the entity's primary regulator (if it has one);
- Whether the incident appears to have involved a corporate insider and what contractual or other rights that employee may have;

- Whether the incident response revealed evidence of other crimes; and
- Whether there is evidence of misfeasance by a service provider or partner that indicates that the company should assert any contractual rights to ensure that the third-party company secures evidence and restores systems in an appropriate manner.

CONTAINMENT

Full elimination of a computer security compromise often requires significant time and planning. But the harm caused by malware can increase quickly, and incidents may become vastly more complicated and expensive to remedy the longer they continue.[71] Containment of a computer security incident—with as limited a loss of functionality as possible—is thus an important function of incident response.

Strategies for containing incidents are case-specific. NIST has identified a number of criteria to help determine the best strategy:

- Potential damage to and theft of resources;
- Need for evidence preservation;
- Service availability (e.g., network connectivity, services provided to external parties);
- Time and resources needed to implement the strategy; and
- Effect of the strategy (e.g., partial containment, full containment).[72]

Business prerogatives thus play a substantial role in determining how to contain a security incident. Legal consequences also should be considered. Legal counsel should be consulted about

the risks associated with different containment strategies. This applies with particular force to strategies that do not immediately contain unauthorized network activity. An incident response team, for example, may wish to cut off a connection between a compromised device on the company network and an external host. But the response team also may suspect that cutting off that connection will trigger further harm on the network. Alternatively, it may realize that doing so will require first shutting down various systems and the business functions they support. In either event, further harm is possible, whether to consumers or to business partners.

The response team should record the steps taken to contain the incident. This documentation should be specific, describing the essential details—who did what, where, and when—of the containment. The response team likewise should gather appropriate statistics that demonstrate the success of the containment strategy, as well as when this containment was accomplished, and how long it lasted.

ERADICATION

The incident response team may be subject to substantial pressure from the public, customers, and individuals within the enterprise to restore services affected by a computer security incident. But mere delivery of services is not the measure of a successful incident response. The assurance of systems' confidentiality, integrity, and availability will precede any incident response being deemed complete. At times, this may require a complete system rebuild. DHS, for example, has identified the following circumstances in which that remedy should be considered:

- The intruder gained root or administrative-level access to the system;

- Back-door type access has been granted;
- System files were replaced by the malware or directly by the intruder; or
- The system is unstable or does not function properly after antivirus software, spyware detection and removal utilities, or other programs eradicate the malware.[73]

As with containment, eradication should not be assumed. Instead, it should be verified. Appropriate technical steps should be taken to determine with all available confidence that the eradication plan was successful. Here, again, technical steps should be recorded in a manner that permits ready comprehension within the enterprise. Business management should understand the measures by which success is gauged. Sufficient detail also should be included to permit meaningful comprehension by a reviewer.

RECOVERY

Once malicious code and other unauthorized network activities have been eradicated, the response team should turn to recovery. Simply restoring a device to service in its pre-incident condition is insufficient. A compromised device very well may have been compromised through a specific vulnerability that now is known to the company. Patching that device and other appropriate network assets and taking other necessary steps to harden them against future attacks are essential. Liability risks from unknown exploits and tools are significant, but the risks from known vulnerabilities and exploits—and particularly those that have been used against the company successfully in the past—are yet more substantial.[74]

The response team also can ensure that an appropriate period of monitoring is put in place for the recovered systems. The risks of

too short a monitoring period are straightforward: an attacker may return to exploit a backdoor that was not successfully removed during the remediation process or a determined attacker may find the flaw in a patch developed to remediate the compromise.

LEARNING FROM AN INCIDENT

Computer security incidents expose technical vulnerabilities of company systems. A company can address those vulnerabilities and thereby prevent company systems from being exploited in the same manner in the future.

Active responses also put company's incident response plans and protocols to the test. Weaknesses or inadequacies in the incident response should be identified, analyzed, and addressed. A full review may be necessary in the event of significant breakdowns in the active response process, while a single meeting may be sufficient to cover any lessons learned from a number of different computer security incidents. Whatever the scale of the assessment, it should be rigorous and frank while conducted in a manner that does not create counterproductive records of preliminary or contradictory conclusions. Team structures can be assessed, and performance can be rated. Process flaws should be identified, and the strengths and weaknesses of different alternatives should be considered. Subsequent steps should be reasonable in all events. Lessons learned should be incorporated in enterprise-wide actions. Incident response teams in different business units or different locations likewise should learn from one other's experiences. Business units may have different systems and may require different incident response protocols, but a company should not allow silos within its organizational structure to cost the enterprise as a whole opportunities to improve its incident response capacity.

Breach Notification

Congress continues to consider adopting a national breach notification law. Until it does, companies face a patchwork of state laws that impose varying breach notification standards across 47 states. Determining whether notification is required in each state and what notice should be given can be an extremely time-consuming task. As discussed previously, a company can prepare in advance of a computer security incident for any necessary breach notification. A breach notification plan that is appropriate for the types of information that the company holds will facilitate any subsequent notification. Knowing the triggers for notification requirements under HIPAA, the Gramm-Leach-Bliley Act, or the various state breach notification statutes also will help a company determine more promptly whether notification is necessary.

A full description of the various notification statutes is beyond the scope of this book.[75] However, a few general questions will guide the scope of a company's notifications to consumers:

- Does the company hold data that is subject to state data breach notification statutes or that triggers obligations under HIPAA or the Gramm-Leach-Bliley Act?
- Was this data acquired by an unauthorized person during the breach?
- What information was so acquired?
- Was the compromised data encrypted, or will anti-fraud tools prevent any financial loss to consumers?
- In which states do the company's customers reside?
- Will notification of a breach impede a criminal investigation?

- What level of certainty does the company have about the scope of the breach or the number of affected persons?

Companies increasingly feel pressure to over-notify and to do so as early as possible after a data breach. The breach notification process thus likely will run in parallel to the technical response to a computer security incident and will help prioritize questions for the incident response team. Such notifications also may reach beyond consumers. A computer security incident may implicate the privacy interests of employees, for example. Delay in notifying employees or their union may result in employee dissatisfaction or even litigation.[76]

Preventing Further Harm

The risks associated with a computer security incident do not end simply because the underlying harm has been remediated. Instead, affected companies will be wise to anticipate and address risks that threaten to compound the harms already suffered.

Customer Satisfaction

The significance of computer security incidents as a business issue may manifest itself most clearly in a drop in customer satisfaction. Businesses built on customer trust or on the delivery of online services face the greatest risk, but each company is exposed to broad reputational harm. While this may seem fundamentally unfair, companies benefit from accepting that their status as the victims of criminal behavior will not insulate them from reputational damage. Companies also should recognize that the response may have as significant an effect on the long-term business consequences of an incident as the fact of the breach itself. Put more positively, incident response is an opportunity to maintain customer satisfaction. A company, for example, that promptly and proactively provides information to consumers may be able to preempt any significant loss in customer good will. A company also has multiple tools at its disposal to assist customers whose personal information has been compromised and should consider using them as circumstances require.

Regulatory Scrutiny and Enforcement Actions

Regulatory scrutiny is sure to follow a significant computer security incident. State attorneys general may well demand

answers, for example, about a company's response to an incident, even including its conclusion that no sensitive information was compromised.[77] A computer security incident also may cause a company's regulator to scrutinize the company's information security practices and procedures through a supervisory exam, or the FTC may issue a burdensome civil investigative demand.[78] Indeed, Congress may even prompt regulators to act in the aftermath of a computer security incident, including through calls for a regulatory investigation. As discussed, various agencies have asserted authority in this field. Accordingly, a company should assume that regulatory attention will follow a computer security incident and should take appropriate steps to ensure that the response team keeps adequate records to satisfy such regulatory curiosity.

A public company that suffers a substantial computer security incident likely will consider whether to disclose information about the breach through statements filed with the Securities and Exchange Commission. SEC staff interpretive guidance issued in 2011 indicated the staff's view that registrants should do more to disclose the cyber risks they face as well as the cyber incidents they have experienced.[79] The guidance identified a series of disclosures that may be appropriate for registrants in certain circumstances, including a "[d]escription of cyber incidents experienced by the registrant that are individually, or in the aggregate, material, including a description of the costs and other consequences."[80] Appropriate record-keeping by the response team will help a company decide what, if any, information it should share through an SEC filing.

Litigation

Putative class action lawsuits have followed promptly after recent major computer security incidents. The threat of such litigation

should not disrupt the prudent decision-making that drives an effective incident response. Nonetheless, companies facing computer security incidents that affect consumer privacy or have significant financial consequences would be prudent to keep this litigation threat in mind as they proceed through the incident response process.

Specifically, the leaders of the active response team should recall that non-privileged communications and records may soon be subject to civil discovery. (Of course, this assumes that the plaintiffs have standing, have adequately a claim, and are not barred by the economic loss doctrine or another legal requirement—threshold issues that have doomed many lawsuits to date).[81] Effective incident response can help ensure that such discovery confirms that the company had appropriate security policies and procedures in place, that its security was compromised even despite those reasonable policies and procedures, and that the company responded in a reasonable and effective manner when that occurred.

Collateral Harms

Computer security incidents can cause substantial direct or foreseeable harms to a company such as the loss of money from a corporate bank account or the lost revenue resulting from an inability to deliver its products. Other harms are less foreseeable, but, nonetheless, may compound the damage caused by a computer security incident. For example:

- A significant data breach may capture the attention of politicians, requiring a company to respond to congressional investigations or scrutiny. Shortly after Home Depot announced a data breach in September 2014, for example, Senators Richard Blumenthal and Edward Markey wrote to

the Federal Trade Commission requesting an investigation and questioning the effectiveness of the retailer's incident response.[82] (Among other things, the senators criticized the company for allegedly taking 0.3 days—or approximately seven hours—longer than the average retailer to remove malware.) Such letters require government relations and crisis management expertise during the incident response.

- A significant data breach can cause equally significant movement in a public company's stock price. A company insider who knows about the breach and has a sense of its severity may be tempted to cash out of company stock. To avoid the distraction of a criminal investigation into company insiders (and terrible press on the subject), the company may wish to consider imposing trading restrictions on company insiders before that risk is realized.[83]
- A company may subject the intellectual property of a joint venture to a non-disclosure agreement. Any compromise of that intellectual property may trigger notification obligations under that non-disclosure agreement or even put the company in breach of that agreement. A company should broadly evaluate whether its agreements with third parties have been implicated by a computer security incident.
- A computer security incident may compromise the confidentiality of an organization's trade secrets. Some of these trade secrets may be patentable. Companies should consider accelerating applications for appropriate patents to prevent the innovation being patented by a third party or to avoid unnecessary impediments to patentability.[84]

Media Scrutiny

Cybersecurity has become a priority issue in national and international politics, and computer security incidents have captured the imagination of the press and the public. Companies consequently should expect intense and sustained media scrutiny of any substantial incident they suffer. A drum-beat of critical articles may exacerbate any loss in customer confidence and weaken employee morale. Companies therefore may benefit substantially from a sustained communications response to a significant computer security incident. While the details of such a response are beyond the scope of this book, the significance of the threat posed by ongoing media scrutiny deserves special mention.

Improved Computer Security

Lessons learned during the active response process provide an opportunity—and responsibility—to enhance computer security. The good news is that a company that emerges from an effective incident response likely will be able to protect itself from a broader array of threats and also likely will have honed its own active response capabilities. The bad news is that the company finds itself back at the beginning of the cycle, preparing to face its next computer security incident. Computer security, in short, remains an ongoing process—of which incident response will be an unfortunate, but important, part.

Conclusion

American businesses face an ever-expanding array of information security threats. While a consensus now acknowledges that these incidents cannot uniformly be prevented, businesses increasingly operate under de facto or actual regulatory requirements that they respond effectively when computer security incidents do occur. To do so, companies must address technical issues, thoroughly investigate the facts, maintain operations, meet varying legal requirements, manage communications, provide robust customer care, and meet sundry other requirements. In light of these challenges, American companies will continue to be best served by risk-based approaches to incident response that are well grounded in the needs of the particular businesses and the legal and operational risks they face.

Legal counsel has an important role to play in helping companies to develop and deploy effective computer security incident response plans, to investigate an incident, to facilitate appropriate notifications, and to help the company minimize related legal risks. Given the continuing regulatory and enforcement activity relating to these actions, counsel's role is likely to grow. Companies thus should continue to work with legal counsel as they prepare for and respond to computer security incidents.

Endnotes

[1] The Securities and Exchange Commission has reported, for example, that 88% of registered broker-dealers and 74% of registered investment advisers have been the subject of a computer security related incident after being attacked directly or through a vendor. *See* Office of Compliance Inspections and Examinations, Securities and Exchange Commission, *Cybersecurity Examination Sweep Summary* 2-3 (Feb. 3, 2015), *available at* http://www.sec.gov/about/offices/ocie/cybersecurity-examination-sweep-summary.pdf.

[2] *See* National Institute of Standards and Technology, *Computer Security Incident Handling Guide* 6, Spec. Pub. 800-61 rev. 2 (Aug. 2012) ("NIST CSI Guide"), *available at* http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf (describing computer security incidents as "violation[s] or imminent threat[s] of violation of computer security policies, acceptable use policies, or standard security practices").

[3] For example, according to Verizon, the number of cyber espionage attacks increased threefold from 2012 to 2013. *See* Verizon, *2014 Data Breach Investigations Report*, Executive Summary 8, *available at* http://www.verizonenterprise.com/DBIR/2014/reports/rp_dbir-2014-executive-summary_en_xg.pdf.

[4] *An Enormous Data Heist May Dim Koreans' Love Affair with Credit Cards*, The Economist (Jan. 25, 2014), *available at* http://www.economist.com/news/finance-and-economics/21595059-enormous-data-heist-may-dim-koreans-love-affair-credit-cards-card-sharps.

[5] Jennifer Martinez, *White House Thwarts Hacker Attack on Unidentified Computer System*, The Hill (Oct. 1, 2012), *available at* http://thehill.com/policy/technology/259461-hackers-attack-white-house-computer-system.

[6] Georgia Department of Behavioral Health and Developmental Disabilities, Press Release, *DBHDD Investigates Data Breach Involving Stolen Laptop* (Oct. 9, 2014), *available at* http://dbhdd.georgia.gov/press-releases/2015-01-14/dbhdd-investigates-data-breach-involving-stolen-laptop.

[7] *See* Krebs on Security, *DDoS Attack on Bank Hid $900,000 Cyberheist* (Feb. 13, 2013), *available at* http://krebsonsecurity.com/2013/02/ddos-attack-on-bank-hid-900000-cyberheist/.

[8] *See*, e.g., Krebs on Security, *All About Skimmers* (last accessed Feb. 22, 2015), *available at* http://krebsonsecurity.com/category/all-about-skimmers/.

[9] *See*, US-CERT, Department of Homeland Security, *Alert (TA14-212A): Backoff Point-of-Sale Malware* (Aug. 27, 2014), *available at* https://www.us-cert.gov/ncas/alerts/TA14-212A.

[10] Ryan W. Neal, *CryptoLocker Virus: Swansea, Mass Police Pay $750 Bitcoin Ransom To Retrieve Files*, International Business Times (Nov. 20, 2013), *available at* http://www.ibtimes.com/cryptolocker-virus-swansea-mass-police-pay-750-bitcoin-ransom-retrieve-files-1479482.

[11] In September 2014, Home Depot announced that its payment data systems had been breached by a cyber intruder. The attacker accessed the company's network using a vendor's user name and password and installed malware on Home Depot's point of sale systems and obtained information for approximately 56 million of the company's customers' credit and debit cards used in its United States and Canadian stores from April 2014 to September 2014. The breach also included more than 54 million of Home Depot's customers' email addresses. By November 2, 2014, Home Depot faced 44 lawsuits and had spent approximately $43 million to investigate the data breach, provide services to protect the identities of affected customers, fund call center personnel, and pay legal and other professional costs. *See* Home Depot, Quarterly *Report Pursuant to Section 13 or 15(d) of the Securities Exchange Act of 1934 (Form 10-Q)* at 7-8 (Nov. 26, 2014).

[12] *See* Federal Bureau of Investigation, Public Service Announcement, *Increase in Insider Threat Cases Highlight Significant Risks to Business Networks and Proprietary Information* (Sept. 23, 2014), *available at* http://www.ic3.gov/media/2014/140923.aspx.

[13] *See, e.g.*, Department of Homeland Security, ICS-CERT, Alert (ICS-ALERT-14-281-01B), *Ongoing Sophisticated Malware Campaign Compromising ICS (Update B)* (Dec. 10, 2014), *available at* https://ics-cert.us-cert.gov/alerts/ICS-ALERT-14-281-01B.

[14] *See generally* National Institute of Standards and Technology, Standards for Security Categorization of Federal Information and Information Systems, FIPS Pub. 1999 at 2 (Feb. 2004), *available at* http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf (quoting definition of "confidentiality" in 44 U.S.C. § 3542 as "[p]reserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information").

[15] *See id.* (quoting definition of "integrity" in 44 U.S.C. § 3542 as "[g]uarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity").

[16] *See, e.g.*, Michael Riley, *How Russian Hackers Stole the Nasdaq*, Bloomberg Businessweek (July 17, 2014), *available at* http://www.bloomberg.com/bw/articles/2014-07-17/how-russian-hackers-stole-the-nasdaq.

[17] *See* Federal Trade Commission, *Internet of Things: Privacy and Security in a Connected World* 12 (Jan. 2015), *available at* http://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf).

[18] *See* FIPS Pub. 199, *supra* note 14, at 2 (quoting definition of "availability" in 44 U.S.C. § 3542 as "[e]nsuring timely and reliable access to and use of information").

[19] *See, e.g.*, John Markoff, *Before the Gunfire, Cyberattacks*, N.Y. Times (Aug. 12, 2008), *available at* http://www.nytimes.com/2008/08/13/technology/13cyber.html?_r=0.

[20] *See, e.g.*, Lillian Ablon, Martin C. Libicki & Andrea A. Golay, *Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar* (2014).

[21] The SEC has reported, for example, that "[o]ver half of the broker-dealers (54%) and just under half of the advisers (43%) reported receiving fraudulent emails seeking to transfer client funds. Over a quarter of those broker-dealers (26%) reported losses of more than $5,000 related to fraudulent emails; however, no single loss exceeded $75,000." *See* SEC, *supra* note 15.

[22] *See, e.g.*, Kim Zetter, *Anonymous Hacks Security Firm Investigating IT; Releases E-mail*, (Feb. 7, 2011), *available at* http://www.wired.com/2011/02/anonymous-hacks-hbgary/.

[23] *See, e.g.*, Department of Justice, Press Release, *U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage* (May 19, 2014), *available at* http://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor.

[24] *See, e.g.*, FBI, Press Release, *GameOver Zeus Botnet Disrupted*, (June 2, 2014), *available at* http://www.fbi.gov/news/stories/2014/june/gameover-zeus-botnet-disrupted.

[25] *See, e.g.*, Brett Molina, *Three Questions about the Heartbleed Bug*, USA Today (April 9, 2014), *available at* http://www.usatoday.com/story/tech/2014/04/09/heartbleed-five-questions/7501033/; Krebs on Security, *Shellshock' Bug Spells Trouble for Web Security, Krebs on Security* (Sept. 14, 2014), *available at* http://krebsonsecurity.com/2014/09/shellshock-bug-spells-trouble-for-web-security/.

[26] *See, e.g.*, Zetter, *supra* note 22.

[27] *See* 15 U.S.C. § 45.The FTC's authority to regulate data security through its "unfairness" authority has been upheld in court. *See, e.g., FTC v. Wyndham Hotels & Resorts, LLC,* No. 14-3514 (3d Cir. 2015) (holding that the FTC has authority

under the "unfairness" provision of Section 5 of the FTC Act to bring enforcement actions against companies for alleged failures to implement adequate cybersecurity safeguards to protect consumer information).

[28] *See* Complaint ¶ 24(i), *FTC v. Wyndham Worldwide, Corp.*, No. 12-cv-01365 (D. Ariz. June 26, 2012) (alleging that company "failed to follow proper incident response procedures, including failing to monitor [its] computer network for malware used in a previous intrusion").

[29] *See, e.g.,* OCC Advisory Letter AL 2002-3, *Guidance on Unfair or Deceptive Acts or Practices 3* (Mar. 22, 2002) ("Under section 8 of the Federal Deposit Insurance Act, 12 USC 1818, the OCC may take appropriate enforcement actions against national banks and their subsidiaries for violations of *any* law or regulation, which necessarily includes section 5 of the FTC Act.").

[30] *See* Exhibit 1 to Petition of Wyndham Hotels & Resorts, LLC and Wyndham Worldwide Corporation to Quash or, Alternatively, Limit Civil Investigative Demand, FTC File No. 1023142 (Jan. 20, 2012) (civil investigative demand to hotel operators that asks extensive questions about information security practices); Exhibit 1 to Hannaford Bros. Co. & Kash N' Karry Food Stores, Inc's Petition to Quash or, Alternatively, Limit Civil Investigative Demands, FTC File No. 0823152 (Dec. 13, 2010) (similarly extensive civil investigative demand regarding information security practices to operators of food markets).

[31] *See* 15 U.S.C. § 6801(b).

[32] *See* 15 U.S.C. § 6804; 17 C.F.R. Part 248.

[33] *See* 17 C.F.R. § 248.30. *See also* 17 C.F.R. § 160.30 (comparable requirement imposed by Commodity Futures Trading Commission).

[34] *See, e.g.*, SEC Release No. 64220 at 1-2 (April 7, 2011) (alleging, for example, that "no single person or department directed or coordinated the firm's responses to the thefts,"), *available at* http://www.sec.gov/litigation/admin/2011/34-64220.pdf.

[35] *Id.* at 1. After multiple laptop computers were stolen (including at least one with customers' names, dates of birth, and Social Security numbers) and a terminated employee had inappropriately obtained the password credentials of another employee, the SEC determined that the former chief compliance officer had "willfully aided and abetted . . . violations of Rule 30(a) of Regulation S-P under the Exchange Act." *Id.* at 5. Among other things, the SEC found that the company's failure to notify affected customers or take any further actions (beyond filing a report with the local police department) following the theft of one laptop containing customer information fell below minimum standards. *Id.* at 3-6.

[36] *Id.* at 5.

[37] *See Interagency Guidelines Establishing Standards for Safeguarding Customer Information and Rescission of Year 2000 Standards for Safety and Soundness*, 66 Fed. Reg. 8616 (Feb. 1, 2001).

[38] *See Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice*, 70 Fed. Reg. 15736, 15751 (Mar. 29, 2005); see also 12 C.F.R. Part 30, app. B, Supplement A (OCC); 12 C.F.R. Part 208, app. D-2, Supplement A and Part 225, app. F, Supplement A (Board); 12 C.F.R. Part 364, app. B, Supplement A (FDIC); and 12 C.F.R. Part 570, app. B, Supplement A (OTS). The guidance described an "effective response program" as including the following components: assessment of the nature and scope of the incident and identification of what customer information has been accessed or misused; prompt notification to its primary federal regulator once the institution becomes aware of an incident involving unauthorized access to or use of sensitive customer information; notification to appropriate law enforcement authorities, in addition to filing a timely Suspicious Activity Report, in situations involving federal criminal violations requiring immediate attention; measures to contain and control the incident to prevent further unauthorized access to or misuse of customer information, while preserving records and other evidence; and notification to customers when warranted. 70 Fed. Reg. at 15752. The National Credit Union Administration issued similar guidance pursuant to Gramm-Leach-Bliley in 2001. Codified at 12 C.F.R. Part 748, the guidance requires each federally insured credit union to have a "written security program" that will guide how it responds to incidents of "unauthorized access to or use of the information that could result in substantial harm or serious inconvenience to a member."

[39] *See* FFIEC, Incident Response, IT Examination Handbook InfoBase, *available at* http://ithandbook.ffiec.gov/it-booklets/business-continuity-planning/other-policies,-standards-and-processes-/incident-response.aspx.

[40] The National Futures Association, the self-regulatory organization for the U.S. derivatives industry, also has indicated that it may issue guidance regarding its members' regulatory responsibilities. *See* http://www.nfa.futures.org/news/newsBoard.asp?ArticleID=4545.

[41] *See* FINRA, Report on Cybersecurity Practices (Feb. 2015), *available at* http://www.finra.org/web/groups/industry/@ip/@reg/@guide/documents/industry/p602363.pdf.

[42] The guidance advises firms to: (1) prepare incident responses for the types of events that the firm most likely will encounter, such as the loss of customers' personally identifiable information, corruption of data, DDoS attacks, network intrusions, and infection by malware; (2) incorporate updated threat intelligence to identify the most likely types of incidents and attacks; (3) develop containment and mitigation strategies for multiple types of incidents; (4) include eradication and recovery plans for systems and information; (5) specify processes for investigation and damage assessment; (6) draft plans for communication and notification plans to inform relevant stakeholders, including customers, regulators, members of law enforcement, intelligence agencies, and information sharing bodies; (7) participate in industry and organization-specific training exercises that are tailored to the size and particulars of a firm's business; and (8) implement measures to maintain

clients' confidence, such as providing credit monitoring for individuals whose sensitive personal information has been improperly disclosed and reimbursing customers for financial losses. *See id.* at 23.

[43] *See* 45 C.F.R. § 164.308(a)(6); National Institute of Standards and Technology, An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule (Oct. 2008) (mapping rule section to Spec. Pub. 800-53 IR-1), *available at* http://csrc.nist.gov/publications/nistpubs/800-66-Rev1/SP-800-66-Revision1.pdf; *id.* at 27 (describing need to "[d]ocument incident response procedures that can provide a single point of reference to guide the day-to-day operations of the incident response team").

[44] 45 C.F.R. § 164.404(a)(2).

[45] *See* North American Electric Reliability Corporation, CIP-008-5 R1.

[46] *See* Federal Energy Regulatory Commission, *Mandatory Reliability Standards for Critical Infrastructure Protection*, 73 Fed. Reg. 7368 ¶¶ 653-688 (Feb. 7, 2008).

[47] *See*, e.g., Docket No. NP11-104-000 (Feb. 1, 2011) (including in violation # SPP200900192 that the entity's response plan did not provide "the incident handling procedures to be followed in the event of an incident"), *available at* http://www.nerc.com/pa/comp/CE/Pages/Actions_2011/Enforcement-Actions-2011.aspx.

[48] *See* National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity Version 1.0*, at 19, 33-34 (Feb. 12, 2014) (including as subcategories "Response Planning," "Communications," "Analysis," "Mitigation," and "Improvements"), *available at* http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.

[49] *See generally* Office of the Press Secretary, The White House, *Background Briefing on Launch of the Cybersecurity Framework* (Feb. 12, 2014) ("We believe that from today on we'll have a new shared vocabulary about cybersecurity that will allow CEOs, boards of directors and policymakers–not just here in the U.S., but around the world–to set baselines and chart the course for improvement and actually make those improvements."), *available at* http://www.whitehouse.gov/the-press-office/2014/02/12/background-briefing-launch-cybersecurity-framework.

[50] *See* Alaska Stat. § 45.48.010 *et seq.* (2014); Ariz. Rev. Stat. § 44-7501 (2015); Ark. Code Ann. § 4-110-101 *et seq.* (2015); Cal. Civ. Code § 1798.29, 1798.80 *et seq.* (2015); Colo. Rev. Stat. § 6-1-716 (2015); Conn. Gen Stat. § 36a-701b (2015); Del. Code Ann. tit. 6, § 12B-101 *et seq.* (2015); Fla. Stat. §§ 501.171, 282.0041, 282.318(2)(i) (2015); Ga. Code Ann. §§ 10-1-910 to -912; § 46-5-214 (2015); Haw. Rev. Stat. § 487N-1 *et seq.* (2015); Idaho Code Ann. §§ 28-51-104 to -107 (2015);

815 Ill. Comp. Stat. §§ 530 /1 to 530/25 (West 2015); Ind. Code § 4-1-11 *et seq.* (West 2015), 24-4.9 *et seq.* (2013); Iowa Code §§ 715C.1, 715C.2 (2015); Kan. Stat. Ann. § 50-7a01 *et seq.* (2015); Ky. Rev. Stat. Ann. §§ 365.732, 61.931 to -934 (West 2015); La. Rev. Stat. Ann. § 51:3071 *et seq.*, 40:1300.113 (2014); Me. Rev. Stat. tit. 10 § 1346, 1347 *et seq.* (2015); Md. Code Ann. Com. Law § 14-3501 *et seq.* (West 2015), Md. Code Ann. State Govt. § 10-1301 *et seq.* (West 2015); Mass. Gen. Laws ch. 93H § 1 *et seq.* (West 2015); Mich. Comp. Laws §§ 445.63, 445.72 (2015); Minn. Stat. §§ 325E.61, 325E.64 (2015); Miss. Code Ann. § 75-24-29 (2015); Mo. Rev. Stat. § 407.1500.1 (2015); Mont. Code Ann. §§ 2-6-504, 30-14-1701 to 1705, 30-14-1712 to -1713 (2015); Neb. Rev. Stat. §§ 87-801 to 87-807 (2014); Nev. Rev. Stat. § 603A.010 *et seq.*, 242.183 (2014); N.H. Rev. Stat. Ann. §§ 359-C:19 to -C:21 (2015); N.J. Stat. Ann. §§ 56:8-161, 56:8-163 (West 2015); N.Y. Gen. Bus. Law § 899-aa (McKinney 2015), N.Y. State Tech. Law 208 (McKinney 2015); N.C. Gen. Stat § 75-60 *et seq.* (2015); N.D. Cent. Code § 51-30-01 *et seq.* (2015); Ohio Rev. Code Ann. §§ 1347.12, 1349.19, 1349.191, 1349.192 (West 2015); Okla. Stat. tit. 74 § 3113.1 (West 2015), tit. 24-161 to -166 (West 2014); Or. Rev. Stat. §§ 646A.600 to .628 (2015); 73 Pa. Stat. Ann. § 2301 *et seq.* (2014); R.I. Gen. Laws § 11-49.2-1 *et seq.* (2014); S.C. Code Ann. § 39-1-90 (West 2015); Tenn. Code § 47-18-2107 (2015); Tex. Bus. & Com. Code § 521.001 *et seq.* (West 2015), Tex. Educ. Code § 37.007(b)(5) (West 2015); Utah Code Ann. §§ 13-44-101 to -301 (West 2014); Vt. Stat. Ann. tit. 9 §§ 2430, 2435 (2014); Va. Code ann. §§ 18.2-186.6, 32.1-127.1:05 (2014); Wash. Rev. Code § 19.255.010 *et seq.*, 42.56.590 (2015); W.Va. Code § 46A-2A-101 *et seq.* (2015); Wis. Stat. § 134.98 (2015); Wyo. Stat. Ann. § 40-12-501 *et seq.* (2014); D.C. Code § 28- 3851 *et seq.* (2015); 9 Guam Code Ann. § 48-10 *et seq.* (2014); P.R. Laws Ann. tit. 10 § 4051 *et seq.* (2013); V.I. Code Ann. tit. 14, § 2208 (2014). Alabama, New Mexico, and South Dakota do not have notification laws

[51] *See* Maine Bureau of Insurance, Notice of Risk to Personal Data Act, Frequently Asked Questions, *available at* http://www.maine.gov/pfr/insurance/faq/data_breach_faq.htm, last accessed February 19, 2015.

[52] *See* Letter from Benjamin M. Lawsky to All NYS-Chartered or Licensed Banking Institutions, Re: New Cyber Security Examination Process 1 (Dec. 10, 2014).

[53] *Id*, at 3.

[54] *See, e.g.*, Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, 70 Fed. Reg. 15736, 15752 (Mar. 29, 2005) (explaining that "every financial institution should also develop and implement a risk-based response program to address incidents of unauthorized access to customer information in customer information systems that occur nonetheless. A response program should be a key part of an institution's information security program. The program should be appropriate to the size and complexity of the institution and the nature and scope of its activities").

[55] Various federal agencies have described elements that may be included in an incident response plan. *See, e.g.*, Control Systems Security Program, Department of Homeland Security, *Recommended Practice: Developing an Industrial Control Systems Cybersecurity Incident Response Capability* 10-13 (Oct. 2009) ("DHS ICS Recommendations") (describing "key sections [that] should be considered" as "Overview, Goals, and Objectives," "Incident Description," "Incident Detection," "Incident Notification," "Incident Analysis," "Response Actions," Communications," and "Forensics"); NIST CSI Guide, *supra* note 2, at 8 (stating that a response plan should include: "Mission," "Strategies and goals," "Senior management approval," "Organizational approach to incident response," "How the incident response team will communicate with the rest of the organization and with other organizations," "Metrics for measuring the incident response capability and its effectiveness," "Roadmap for maturing the incident response capability," "How the program fits into the overall organization").

[56] NIST separates what we refer to as a plan into two documents, a "policy" that "defines which events are considered incidents, establishes the organizational structure for incident response, defines roles and responsibilities, and lists the requirements for reporting incidents, among other items," and a "plan" that "indicates both short- and long-term goals for the program, including metrics for measuring the program," and "indicate[s] how often incident handlers should be trained and the requirements for incident handlers." *See id.* at 19.

[57] NIST notes that incident response teams typically are responsible for delivering other services such as incident detection. *See id.* at 18. We focus here on the incident response function, not on other functions the team may perform.

[58] *See, e.g.*, National Institute of Standards and Technology, An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule 27 (Oct. 2008) (asking whether "members of the team have adequate knowledge of the organization's hardware and software," have "received appropriate training in incident response activities," and "have the authority to speak for the organization to the media, law enforcement, and clients or business partners").

[59] NIST discusses various possible configurations and staffing choices for incident response teams in Section 2.4 of its Incident Handling Guide. *See NIST CSI Guide, supra* note 2, at § 2.4. DHS has provided similar recommendations relating to cybersecurity incidents relating to industrial control systems. *See* DHS ICS Recommendations, *supra* note 53, at 7-9 (Oct. 2009).

[60] *See, e.g.*, Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, 70 Fed. Reg. 15736, 15752 (Mar. 29, 2005) (indicating that "an institution's response plan should contain procedures for . . . [n]otifying its primary Federal regulator as soon as possible when the institution becomes aware of an incident involving unauthorized access to or use of *sensitive* customer information").

[61] *See, e.g.*, National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity Version 1.0*, at 11 (Feb. 12, 2014) (including in "Tier 4" security practices that "[t]he organization manages risk and actively shares information with partners to ensure that accurate, current information is being distributed and consumed to improve cybersecurity before a cybersecurity event occurs"), *available at* http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.

[62] *See, e.g.*, DHS ICS Recommendations, *supra* note 55; National Institute of Standards and Technology, Security and Privacy Controls for Federal Information Systems and Organization IR-1, NIST Spec. Pub. 800-53 rev. 4 (Apr. 2013); Nat'l Inst. for Standards and Technology, Guide to Malware Incident Prevention and Handling, Special Pub. 800-83 (2013) http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-83r1.pdf; Nat'l Inst. for Standards and Technology, An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, Spec. Pub. 800-66 Rev. 1 (2008); NIST CSI Guide, *supra* note 2.

[63] *See generally* Restatement (Third) of Law Governing Lawyers § 68 (2000).

[64] *See generally* Restatement (Third) of Law Governing Lawyers § 87 (2000).

[65] *See generally* National Institute of Standards and Technology, Security and Privacy Controls for Federal Information Systems and Organization, NIST Spec. Pub. 800-53 rev. 4 (Apr. 2013).

[66] See, *supra* note 50 (citing state statutes).

[67] We discuss consumer notification at the end of this section.

[68] NIST recommends prioritizing incidents on the basis of their functional impact, information impact, and recoverability. *See* NIST CSI Guide, *supra* note 2, at 32.

[69] *See generally* Fed. R. Evid. 901.

[70] *See generally* Robert J. Scott & Julie Machal-Fulks, Ethical Considerations for Attorneys Responding to a Data-Security Breach, 6 Nw. J. Tech. & Intellectual Property 171, 175-76 (2008).

[71] *See generally* Nat'l Inst. for Standards and Technology, Guide to Malware Incident Prevention and Handling, Special Pub. 800-83 (2013).

[72] *See* NIST CSI Guide, *supra* note 2, at 35.

[73] *See* DHS ICS Recommendations, *supra* note 55, at 30. Though appearing in a report relating to industrial control systems, these recommendations are broadly applicable.

[74] *See, e.g.*, Complaint ¶ 24(i), *FTC v. Wyndham Worldwide, Corp.*, No. 12-cv-01365 (D. Ariz. June 26, 2012).

[75] See *supra* note 50 for a listing of these statutes.

[76] *See, e.g.*, Cory Bennet, The Hill, Postal Workers Union Files Complaint to NLRB After Data Breach (Nov. 11, 2014) (describing complaint that delay in notifying employees of a breach prevented those employees in addressing any resulting harm).

[77] *See, e.g.*, Matthew Goldstein, *State Attorneys General Press JPMorgan for More Details on Hacking*, Dealbook, N.Y. Times (Jan. 14, 2015).

[78] *See* Petition of Wyndham Hotels & Resorts, LLC and Wyndham Worldwide Corporation to Quash or, Alternatively, Limit Civil Investigative Demand, FTC File No. 1023142 (Jan. 20, 2012) (attaching and describing burden of FTC civil investigative demand).

[79] *See* Division of Corporate Finance, Securities and Exchange Commission, CF Disclosure Guidance: Topic No. 2, Cybersecurity (Oct. 13, 2011).

[80] *Id.*

[81] In *Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138 (2013), the Supreme Court held that plaintiffs who feared their communications would be subject to surveillance lacked standing to sue––and that it was not enough to allege that they incurred costs to avoid the risk of surveillance (such as cross-country flights for in-person meetings). The Court held that a "theory of *future* injury is too speculative to satisfy" Article III. Defendants in data breach actions subsequently have used *Clapper* to win dismissal of data breach litigation on standing grounds. 113 S. Ct. 1143. *See, e.g., In re LinkedIn User Privacy Litig.*, 932 F. Supp. 2d 1089 (N.D. Cal. 2013); *Galaria v. Nationwide Mutual*, 998 F. Supp. 2d 646 (S.D. Ohio 2014). Those defenses have not be uniformly successful, however. For example, In re Adobe Systems, Inc. Privacy Litig., No. 13-CV-05226-LHK, 2014 WL 4379916, *9 (N.D. Cal. Sept. 4, 2014), saw the district court conclude that plaintiffs had Article III standing based on an alleged violation of a contractual obligation to provide "reasonable . . . security controls."

[82] *See* Letter of Sen. Richard Blumenthal and Sen. Edward Markey to the Hon. Edith Ramirez (Sept. 9, 2014), *available at* http://blumenthal.senate.gov/download/home-depot-data-breach.

[83] As the Supreme Court explained in *United States v. O'Hagan*, 521 U.S. 642, 651-52 (1997), "[u]nder the 'traditional' or 'classical theory' of insider trading liability, § 10(b) and Rule 10b-5 are violated when a corporate insider trades in securities of his corporation on the basis of material, nonpublic information. Trading on such information qualifies as a 'deceptive device' under § 10(b)."

[84] *See* 35 U.S.C. § 102(b) (creating a one-year grace period for patentability after public release).

About Mayer Brown

Mayer Brown is a global legal services organization advising clients across the Americas, Asia and Europe. Our presence in the world's leading markets enables us to offer clients access to local market knowledge combined with global reach.

We are noted for our commitment to client service and our ability to assist clients with their most complex and demanding legal and business challenges worldwide. We serve many of the world's largest companies, including a significant proportion of the Fortune 100, FTSE 100, DAX and Hang Seng Index companies and more than half of the world's largest banks. We provide legal services in areas such as banking and finance; corporate and securities; litigation and dispute resolution; antitrust and competition; US Supreme Court and appellate matters; employment and benefits; environmental; financial services regulatory & enforcement; government and global trade; intellectual property; real estate; tax; restructuring, bankruptcy and insolvency; and wealth management.

Please visit www.mayerbrown.com for comprehensive contact information for all Mayer Brown offices.