Cybersecurity Preparedness: A Live Cyberattack Tabletop Exercise

February 2017
Cybersecurity
Preparedness and
Rapid Response

Skadden, Arps, Slate, Meagher & Flom LLP
and Affiliates

The Americas
Boston
Chicago
Houston
Los Angeles
New York
Palo Alto
São Paulo
Toronto
Washington, D.C.
Wilmington

Europe
Brussels
Frankfurt
London
Moscow
Munich
Paris

Asia Pacific
Beijing
Hong Kong
Seoul
Shanghai
Singapore
Tokyo
Cybersecurity is a top priority for every organization. Given the potentially catastrophic consequences of cyberattacks, together with the regulatory scrutiny, enforcement activity and private class action litigation likely to follow, cybersecurity has become a cost of staying in business.

54% of companies with a security breach reported having to devote resources to manage public scrutiny after the breach.

– Cisco 2015 Annual Security Report

43 million security incidents were detected in 2014 — a 48% increase from 2013.

Cyberattack preparedness, coupled with a well-developed and tested Security Incident Response Plan (SIRP), is essential for mitigating the legal, operational and reputational risk arising from cyber threats. Engagement with outside counsel who know the legal and regulatory landscape and the key areas of potential liability exposure is a critical part of any company’s cybersecurity strategy. The breadth of our skills, the depth of our expertise and the extent of our experience has earned the confidence of our clients to call on us both before and during a cyberattack.
Companies today appreciate the importance of implementing the most up-to-date information security technology to prevent or mitigate the impact of a cyberattack. But a company’s cyber-preparedness cannot end there. The key issues in enforcement actions and litigation following a cyberattack are how the company managed its cybersecurity planning before the attack, and how they responded during an attack. Companies should expect questions about their cybersecurity governance structure; the level of engagement by C-suite executives and board members; and the quality of the company’s crisis response plan. In building their case, the government and private plaintiffs also will scour the company’s internal and public statements about cybersecurity risk, looking for potentially damaging statements.

To best manage a cyber-incident, companies today need to build a “legal firewall.” Skadden’s Privacy and Cybersecurity Group has the expertise and experience to help companies uncover and address their legal vulnerabilities in an efficient and cost-effective manner.

**DEVELOPMENT AND REVIEW OF SECURITY INCIDENT RESPONSE PLANS**

One of the most important steps a company can take before a cyberattack is to develop and test a SIRP. Studies have shown that companies that have a tested SIRP in place respond more efficiently and effectively to an attack—a key factor in risk mitigation. We help clients create SIRPs, or review existing ones to ensure they reflect best practices and address the legal issues most likely to arise around an incident. Since the quality of the SIRP and how it was executed will be a likely focal point of regulatory actions and litigation, building the SIRP from a legal perspective is essential. We also routinely work with clients to “table test” their existing plans, pointing out legal and practical issues that may arise during an attack.

**CYBERSECURITY “AUDITS”**

In any regulatory enforcement action or litigation, the regulator or private plaintiff will rely on the documentary record to establish the company’s negligence in managing cybersecurity or usage of personal information. We review clients’ documentation relating to cybersecurity and privacy to help determine whether (i) the company has made statements that are inconsistent with, or overstate, the company’s cybersecurity planning; (ii) external consultants highlighted proposals or concerns that were not adequately addressed; and (iii) employees are properly notified of their obligations when handling data and sensitive information. We conduct this review through a “litigation lens,” always thinking of what issues may come up in litigation and how to mitigate those concerns as part of a company’s preparedness program. As part of this exercise, we also review whether a client’s use of personal information, including internal and external data flows, is consistent with its stated policies and regulatory obligations.
DEVELOPMENT AND REVIEW OF CYBERSECURITY GOVERNANCE MODELS

Regulators and private plaintiffs carefully scrutinize a company’s cybersecurity governance. They ask whether information security officers had clear accountability and access to senior management and the board, and whether the board was sufficiently informed. We help clients develop appropriately tailored cybersecurity governance practices and review the governance that clients already have in place. We advise on whether changes may be warranted to bring a client’s governance in line with regulatory expectations and best practices.

RISK ASSESSMENT ANALYSIS

Risk assessment is a fundamental building block, as well as a best practice, of cybersecurity planning. We work with clients to help identify and assess these risks, drawing on our wide range of expertise conducting such assessments from a legal perspective. This includes determining the company’s most valuable assets, how they are protected and who can access that information. Where clients have already conducted such an assessment, we review and comment on their assessment to determine if it meets accepted practices.

POLICIES AND PROCEDURES

The Skadden Privacy and Cybersecurity Group has experience creating and reviewing all of the policies and procedures companies require, including external-facing security policies; internal policies guiding the use of PII and cybersecurity; statements to be used in marketing collateral regarding security policies; written information security policies (WISPs); and language regarding cybersecurity to include in third-party contracts.

EMPLOYEE TRAINING

A company’s cybersecurity planning is only effective if employees are sensitized to the related risks through training. While companies generally design and implement such training internally, we work with clients to develop the scope and level of training that should satisfy a regulatory inquiry and best protect the company if its practices were challenged in a litigation.

INSURANCE

Cyber insurance is a critical aspect of mitigating cybersecurity risk. Our insurance team works with clients to review existing policies to determine whether cyber insurance is warranted, helps them negotiate cyber insurance coverage and advises on the scope of coverage if an attack occurs.

VENDOR MANAGEMENT ASSESSMENT

One of the most critical threat vectors that companies face is cyberattacks that exploit a third-party vendor’s network connection to a company. We review clients’ vendor management processes to determine if appropriate cybersecurity requirements are in place, and review third-party vendor agreements to determine if the client is adequately protected.

Having a strong security posture and incident response plan reduces the cost of a data breach.

– 2014 Ponemon Institute Study
Cybersecurity
Rapid Response Services

When a company discovers it is the victim of a cyberattack, every moment is critical. Companies not only must contain the attack and mitigate the damage, they also must quickly manage an array of demands and pressures from the media, government officials, customers, business partners and shareholders. Companies also must be prepared for the reality that bloggers and the media can sometimes break the news of an attack before a company is able to gather all the relevant facts, and that regulators and government officials are demanding faster response times and want to be informed immediately. The rapidity and efficiency with which a company responds to a cyberattack is now a subject matter of regulatory inquiry and claims asserted by private plaintiffs. Skadden’s multidisciplinary Cyberattack Rapid Response Team has the knowledge and experience to help companies crisis manage an attack, and minimize legal exposure.

**FORENSICS**
The Skadden team includes attorneys with technology and cybersecurity expertise who can work with a client’s forensic experts to evaluate the cyberattack, and determine the best way to approach remediation efforts. Skadden has strong working relationships with the leading forensics providers, and can help clients select the appropriate team given their specific needs.

**LAW ENFORCEMENT AND REGULATORS**
The Skadden team includes former government officials who can advise clients on the roles of various agencies, including regulators and law enforcement, and appropriate ways to work with them. Skadden has extensive experience with numerous agencies, including the FBI Cyber Division, the Computer Crime and Intellectual Property Section of the Department of Justice, the Secret Service, the Department of the Treasury, the Department of Homeland Security and various independent regulatory agencies.
DATA BREACH NOTIFICATION

The Skadden team stays up to date on all current state and federal data breach notification requirements. We can rapidly advise clients on whether disclosure to affected individuals is required and work with our Legal Project Management team to manage multistate notification processes.

PUBLIC DISCLOSURES

Skadden has a long history of helping clients make appropriate public statements during a crisis. In the case of a cyberattack, it is important to review all public statements to ensure that the company’s statements are consistent with legal requirements. We have close working relationships with communications and public relations firms with experience in cyberattack response.

SEC AND REGULATORY DISCLOSURES

The Skadden team includes SEC and regulatory experts who quickly help clients assess whether disclosure is required under SEC filings or as a result of the company’s regulatory obligations, and draft any necessary disclosures. We also work with clients on any presentations or reports they need to make to regulators.

C-SUITE AND BOARD SUPPORT

Cyberattacks can quickly become C-Suite and board-level issues. Skadden team members routinely advise boards on critical company matters, and we have the expertise to advise senior management and boards on cyberattacks, the company’s risk exposure and the path forward.

LITIGATION

Class action and shareholder derivative lawsuits are a reality following any cyberattack. The Skadden team includes members of our top-rated Mass Torts, Insurance and Consumer Litigation Group who can prepare the company for any type of class action lawsuits and defend against ensuing litigation.
How Skadden Can Partner With You

Skadden’s broad and diverse practice areas provide a unique platform from which we can assist clients at every stage of the cybersecurity life cycle. Our coordinated, multidisciplinary team can mobilize for a client at a moment’s notice. Our integrated CRRT provides strategic counsel on substantive issues of privacy and cybersecurity; addresses corporate governance and director responsibility concerns; navigates any concurrent civil, criminal and/or administrative proceedings; and helps manage cyber insurance claims.

Privacy and Cybersecurity

Our attorneys help companies navigate and comply with the evolving privacy and cybersecurity landscape in order to maximize the ROI of data usage while avoiding legal risk. We are well-versed in privacy laws and regulations worldwide and understand the business models and technologies underlying data usage. Our group advises companies on how to adopt “privacy by design” techniques, draft and implement privacy and security policies, create “rapid response teams,” and establish internal governance and reporting systems to minimize liability exposure in the event of a cybersecurity incident.

Compliance Obligations

Key Contacts:
Stuart Levi
James Talbot
Jessica Cohen

Corporate Governance

Key Contacts:
Marc Gerber
Stuart Levi
Patrick Fitzgerald
Michael Scudder

The firm has a long history of successfully representing our clients in critical incident situations. In particular, we are highly attuned to the disclosure and regulatory requirements that arise in the context of a privacy or cybersecurity incident, and together with our clients, we develop and execute strategies for responding to governmental agencies, shareholders, the investment community and the media.
Mass Litigation

We have represented numerous clients, including a wide variety of Fortune 500 companies, in many of the significant mass litigations of the last 20 years. The firm stands out for its depth, breadth and innovative strategies in defending class action lawsuits and is uniquely equipped to counsel clients in class actions brought by consumers whose data was compromised. We also assist clients in navigating their cyber insurance policies.

Government Enforcement and White Collar Crime

Skadden’s powerful combination of resources across the U.S. and internationally is ideally suited to helping companies decide how to interact with law enforcement and other government agencies in a cybersecurity incident, including how best to utilize government resources to protect the organization. Skadden attorneys have close working relationships with a number of key members of the government’s cybersecurity community and can provide unmatched strategic advice to clients.

Key Contacts:

Mass Torts, Insurance and Consumer Litigation

John Beisner
Tim Reynolds
Jessica Miller

Key Contacts:

Patrick Fitzgerald
Michael Scudder
Stuart Levi

They are tenacious. They play to win. They have depth of knowledge, experience and expertise.

- 2013 “BTI Brand Elite: Client Perceptions of the Best-Branded Law Firms”
Relevant Experience

CYBERSECURITY ATTACKS
We have worked with numerous clients to help them manage cybersecurity attacks and their aftermath, including data breaches, theft of confidential information, denial of service attacks and “ransomware” attacks. Our clients include companies in the media, financial services, online service and retail industries.

DATA BREACH NOTIFICATIONS
We have represented numerous companies across multiple industry sectors in drafting and disseminating multistate data breach notifications that were required under law and in advising when notification was not required.

INTERACTION WITH GOVERNMENT
We have coordinated interaction with federal and state criminal and civil enforcement authorities in connection with their investigations of multiple clients regarding cybersecurity intrusions and/or alleged criminal conduct on the part of employees.

PRIVACY AND CYBERSECURITY AUDITS
We have reviewed the privacy and cybersecurity programs and statements of multiple companies across a wide range of industries to identify and remediate any issues that may expose the client to risk.

GLOBAL PRIVACY AND CYBERSECURITY PROGRAMS
We have represented numerous global companies across multiple industry sectors in drafting external-facing and internal employee privacy policies. As part of this process, we have helped companies create implementation and training programs and conducted audits to monitor compliance.

TRANSBORDER DATA FLOW
We have advised numerous companies on the optimal approach to move data around the world. This has included drafting model contracts, assisting companies with Safe Harbor certification and structuring data flows to comply with local regulatory requirements.

SPECIFIC LITIGATION AND REGULATORY REPRESENTATIONS:
Chase Manhattan Bank against allegations that Chase violated its own consumer privacy and confidentiality policies by sharing personally identifiable information about its credit card and mortgage customers with third-party vendors. The New York Appellate Division, Second Department affirmed the New York Supreme Court’s dismissal of this case.

Citigroup in a privacy class action alleging invasion of privacy torts and Section 17200 violations by sharing customer information with third-party vendors. A commercial bank in a:
- privacy class action alleging statutory and common law invasion of privacy torts, contract claims and state statutory claims related to third-party intrusion to obtain credit and debit card information and other personal identifying information contained on a retailer’s computer system; and
- nationwide putative class action alleging negligence, breach of contract, negligent misrepresentation and statutory claims related to third-party intrusion of a retailer’s computer system to obtain credit and debit card information and other personal identifying information.

Farmers Insurance Exchange in securing a favorable settlement of computer trespass claims that Farmers brought against the Auto Club Group in the U.S. District Court for the Northern District of Illinois charging that Auto Club violated the federal Computer Fraud and Abuse Act and state computer trespass statutes after Farmers discovered that Auto Club employees illegally accessed its proprietary computer databases.

A commercial bank in a privacy class action alleging invasion of privacy torts and unfair and deceptive trade practices violations by information sharing and telemarketing with respect to mortgage customers.

Hummingbird USA Inc. in contract and tort claims arising from the loss of computer equipment on which private information of 1.8 million customers of a state student loan agency was stored and in connection with the response to Texas Public Information Act requests regarding the same incident.

An Internet services company in connection with an investigation by the New York state attorney general and FTC into its online privacy practices.

A medical records company in connection with civil and criminal issues related to a hack into personal medical records.

NIC, Inc., operator of the RI.gov website on behalf of the state of Rhode Island, in connection with the theft of Social Security numbers, driver’s license numbers, and credit and debit card numbers.

The Securities Industry and Financial Markets Association as plaintiff in obtaining a preliminary injunction in its lawsuit seeking to protect the constitutional rights of its member banks’ senior employees and their families by preventing the state of Connecticut from enforcing a provision of the Connecticut Campaign Finance Reform Act that required the collection, disclosure and publication on the Internet of the identities of spouses and dependent children of certain officers and employees of state contractors and prospective state contractors.

A website security provider in a lawsuit in connection with a hack into the website of a state government resulting in stolen credit card information from individuals who had done business online with state agencies.
Office Locations

The Americas
- Boston
- Chicago
- Houston
- Los Angeles
- New York
- Palo Alto
- São Paulo
- Toronto
- Washington, D.C.
- Wilmington

Asia Pacific
- Beijing
- Hong Kong
- Seoul
- Shanghai
- Singapore
- Tokyo

Europe
- Brussels
- Frankfurt
- London
- Moscow
- Munich
- Paris
New York State Delays Cybersecurity Regulation for Financial Institutions

The New York State Department of Financial Services has announced certain changes to its new cybersecurity regulation for banks, insurance companies and other financial services institutions, addressing some but not all of the comments it received on the initial draft, and delaying compliance until September 1, 2017.

As we discussed in a September Privacy & Cybersecurity Update, New York state has proposed regulation that would require certain banks, insurance companies and other financial services institutions regulated by the New York State Department of Financial Services (DFS) to establish and maintain a cybersecurity program. The proposal was the result, in part, of a DFS survey of approximately 200 regulated banking institutions and insurance companies regarding the industry’s efforts to prevent cyberattacks. The proposed regulation was subject to a 45-day notice and public comment period during which the DFS received 150 comments, many of which were critical of the proposed framework. DFS has now announced certain modifications to the proposed regulation based on those comments, which address some, but definitely not all, of the concerns that have been expressed. Significantly, the DFS has delayed the effective date of the new regulation until March 1, 2017 (previously January 1, 2017), and the compliance date to September 1, 2017 (previously July 1, 2017). Companies are now required to provide a certificate of compliance with the regulation to DFS each February (as opposed to January), beginning in 2018. The key changes are as follows:

- In response to comments that the cybersecurity requirements should be made more flexible and risk-based, the revised regulation clarifies that certain requirements can be linked to the amount of risk an institution faces. DFS noted, however, that a simple cost-benefit analysis of “acceptable losses” would not be appropriate.

---

1 View the September 2016 special edition of the Privacy & Cybersecurity Update here.
2 View the DFS press release here.
3 View the proposed regulation here.
Privacy & Cybersecurity Update

- DFS has narrowed the definition of nonpublic information (NPI). Specifically, the revised regulation eliminated a very broad category of NPI, which included all information an individual provided when obtaining a financial product, and replaced it with a more commonly used definition that includes the person’s name and various other identifiers, such as social security number, driver’s license number, account number, access code or passwords that would permit access to an individual’s financial account, and/or biometric records. Similarly, DFS eliminated as a category any information that could be used to “trace” an individual’s identity, which many thought created an overly broad category of NPI.

- The revised regulation narrows the obligation to oversee vendors by limiting the obligation to third-party service providers that maintain, process or otherwise are permitted access to NPI through their provision of services.

- The revised regulation somewhat narrows the requirements surrounding notification of a cybersecurity event. For example, notice to the superintendent of a cybersecurity event now has a materiality qualifier. Specifically, notice is required within 72 hours from the determination of the occurrence of a cybersecurity event or event that has a reasonable likelihood of materially harming any material part of the normal operation(s) of the covered entity. Notice is required to be provided to any government body, self-regulatory agency or any other supervisory body.

- In response to concerns that the regulation required the hiring of a chief information security officer, the revised regulation clarifies that DFS is not requiring an individual to have that specific title, or for there to be an individual exclusively dedicated to CISO activity.

- The revised regulation mandates penetration testing annually (as opposed to “at least” annually) and vulnerability assessments, including systematic scans or reviews of information systems, on a semi-annual (instead of quarterly) basis.

- The revised regulation allows entities to use third-party service providers to manage the covered entity’s cybersecurity risks and to perform or oversee the performance of the core cybersecurity functions.

- The revised regulation changes the definition of smaller entities that are exempt from many of the regulations. Specifically, exempted entities are now defined as those with fewer than 10 employees including any independent contractors, or less than $5,000,000 in gross annual revenue in each of the last three fiscal years, or less than $10,000,000 in year-end total assets, calculated in accordance with generally accepted accounting principles, including assets of all affiliates.

While the revised regulation provides additional flexibility in these areas, the New York state regulation imposes the strictest requirements on financial institutions of any state and will require covered entities to carefully review their cybersecurity programs and policies to ensure compliance.

Return to Table of Contents

5th Circuit Rules That Phishing Scam Not Covered Under Crime Protection Insurance Policy’s Computer Fraud Coverage

A U.S. appeals court has determined that a policyholder is not covered under the crime protection insurance policy for a $1.4 million loss resulting from a phishing scam, signaling to policyholders that stand-alone cyber insurance coverage may be necessary to adequately protect against phishing scams and other cyber risks.

A recent decision by the U.S. Court of Appeals for the 5th Circuit serves as a reminder to policyholders that conventional, non-cyber insurance policies may not be sufficient to adequately protect against new and evolving cyber risks. In Apache Corp. v. Great American Insurance Company,4 the 5th Circuit held that Apache Corporation, a Texas-based oil and gas company, was not covered under its crime protection insurance policy’s computer fraud coverage for a $1.4 million loss arising out of an email-related phishing scam because the loss was not directly caused by computer fraud, reversing the decision of the district court.

The phishing scam underlying the coverage dispute in Apache began when an Apache employee received a telephone call from an individual posing as an employee of Petrofac Facilities Management Limited, one of Apache’s vendors. The caller informed the Apache employee that Petrofac had recently changed its bank account information and requested that Apache update its payment routing information. In reply, the Apache employee instructed the caller to submit a formal written request on Petrofac letterhead.

A week later, Apache’s accounts payable department received a seemingly legitimate email from an individual with an “@petrofac.com” email domain, which closely resembled Petrofac’s true “@petrofac.com” email domain. The email advised that Petrofac’s bank account information had changed and attached a forged letter on Petrofac letterhead providing the old bank account information and “new” bank account information with instructions to “use the new account with immediate effect.”

An Apache employee then called the number listed on the forged Petrofac letterhead and spoke with who they believed to be a Petrofac employee to verify the new banking information. Satisfied with the authenticity of the change request, the change was approved and Apache began transferring funds for payment of Petrofac’s invoices into the fraudulent Petrofac bank account. Apache transferred roughly $7 million into the fraudulent bank account over the course of a month before discovering that it had fallen victim to a phishing scam. Apache was able to recoup a substantial portion of the fraudulently transferred funds, but ultimately suffered a loss of approximately $2.4 million, $1.4 million of which was potentially recoverable under its crime protection policy after accounting for a $1 million policy deductible.

Apache submitted a claim for the $1.4 million loss to Great American Insurance Company, which insured Apache under a crime protection policy during the relevant time period. The policy provided computer fraud coverage that obligated Great American to pay for loss “resulting directly from the use of any computer to fraudulently cause a transfer of ... property.” Great American denied coverage on the grounds that the “loss did not result directly from the use of a computer nor did the use of a computer cause the transfer of funds.” Apache then filed suit in Texas state court against Great American challenging the denial of coverage. After removal to the U.S. District Court for the Southern District of Texas, both parties moved for summary judgment.

The district court ruled in Apache’s favor, concluding that the phishing scam fell within the policy’s computer fraud coverage. It reasoned that while there were several “intervening steps” between the computer use and Apache’s transfer of payments to the fraudulent Petrofac account, computer use was nevertheless a central factor in the fraudulent scheme and the loss therefore fell within the policy’s computer fraud coverage. The district court further opined that interpreting the computer fraud provision as covering only direct computer hacking would render the provision largely meaningless.

On appeal, the 5th Circuit reversed, holding that Apache’s loss did not fall within the scope of the policy’s computer fraud provision because it did not directly result from computer fraud. In a *per curiam* decision, the three-judge panel reasoned that while the fraudulent email to Apache was part of the phishing scheme, it was “but one step” in the “multi-step” scheme that ultimately led to the fraudulent transfer of Apache’s funds, and was therefore “incidental” to Apache’s loss. The court found that the involvement of email communication in a fraudulent scheme does not automatically transform the scheme into computer fraud, noting that in an era where electronic communication is ubiquitous, “few – if any – fraudulent schemes would not involve some form of computer-facilitated communication.” Cautioning against an overly broad reading of the policy’s computer fraud provision, the panel further stated that “[t]o interpret the computer-fraud provision as reaching any fraudulent scheme in which an email communication was part of the process would ... convert the computer-fraud provision to one for general fraud.”

* * *

It remains to be seen whether courts in other jurisdictions will adopt the narrow interpretation of computer fraud espoused by the 5th Circuit in *Apache*. More generally, the 5th Circuit’s decision adds to the mixed body of case law throughout the country with respect to coverage for cyber incidents under non-cyber insurance policies. In the face of uncertainty with respect to coverage for cyber incidents under traditional insurance policies, policyholders should undertake a careful review of their policies and consider purchasing cyber insurance to the extent necessary. In addition, policyholders should take steps to mitigate cyber risk by investing in information security and educating personnel on cybersecurity best practices. These measures should help to manage and minimize the risk of cyber incidents as well as the risk of potentially costly coverage gaps in the event of a cyber incident.

---


On November 21, 2016, the Federal Insurance Office of the U.S. Department of the Treasury (FIO) released its first annual “Report on the Protection of Consumers and Access to Insurance”5 (Report). The FIO was created by the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 and is authorized to monitor virtually all aspects of the insurance industry. The Report examines the use of big data, cyber risk and data privacy, among other key insurance consumer protection issues, to highlight how technological developments in the insurance industry.
industry can be beneficial to insurers and consumers alike, while also creating new risks to consumers and, as a result, new needs for state regulators to implement consumer protection measures to mitigate such risks.

**The Use of Big Data**

According to the Report, the increasing use of big data — “the ability to gather large volumes of data, often from multiple sources, and with it produce new kinds of observations, measurements and predictions” — is advantageous to both insurers and consumers in that it facilitates innovation and modernization in insurance product design, distribution and delivery. Big data, the Report notes, is particularly useful with respect to the underwriting process. The use of data generally supports what is known as “risk classification,” a method used by insurers to establish insurance premiums whereby insurers analyze data points that are then used to assign consumers to rating tiers associated with particularized coverage limits and premiums. The use of big data in risk classification provides insurers with a greater number of data points and variables to assess, thereby producing more finely tuned risk assessments and more tailored insurance products. According to the Report, big data also supports price optimization — the use of predictive modeling to perceive consumers’ sensitivities to price changes for the purpose of setting individual premiums.

The Report cautions, however, that big data usage by insurers may be detrimental to consumers in some instances. For example, big data methodologies may conceal discrimination, intentionally or unintentionally, against classes of individuals that are protected under the law by generating consumer segments that correlate with race, gender, ethnicity or religion. In addition, the practice of price optimization involves insurers’ use of nontraditional factors to price risk, which can lead to individual consumers paying different amounts for identical risks. The Report also states that the lack of oversight of big data vendors, which provide analytical services to insurers, presents a risk to consumers. In most cases, big data vendors fall outside the scope of state insurance regulations, which, according to the Report, is problematic because these vendors develop the pricing formulas upon which many insurers rely, thereby directly affecting the affordability of insurance products.

The Report urges state insurance regulators to confront the various regulatory and public policy challenges arising from the use of big data. It recommends that state insurance regulators take action to ensure that big data is being used by insurers in a manner that is consistent with applicable state and federal laws and regulations, and that the methodologies and criteria used by insurers and big data vendors for pricing do not unlawfully discriminate against protected classes. The Report also empha-

**Data Privacy and Cyber Risk**

The Report also addresses data privacy and cyber risk issues presented by insurers’ routine collection, storage and use of a wide range of consumer information, including personally identifiable information and personal health information, in connection with the provision of insurance products and the need to protect consumers’ private information. According to the Report, insurers are particularly vulnerable to cyberattacks because they routinely collect unique personal information. Insurers, therefore, must take steps to minimize cyber risk and protect against data breaches.

As the Report points out, both federal and state regulators have made efforts with respect to cybersecurity in the insurance sector. At the federal level, the Treasury acts as the federal interface for matters involving cybersecurity for all institutions in the financial services sector. In this capacity, the Report notes, the Treasury actively works with state insurance regulators on the development of cybersecurity best practices and the implementation of a “consistently rigorous” approach to cybersecurity oversight for insurers. The Report also discusses some of the efforts that have been made at the state level, where the insurance industry is primarily regulated. Significantly, state insurance regulators established the Cyber Security Task Force in 2013, the purpose of which is to “consider issues concerning cybersecurity as they pertain to the role of state insurance regulators.” The Report also notes that in March 2016, state insurance regulators released for public comment the Insurance Data Security Model Law, which addresses the protection of personal information and data breaches. Regulators also have revised the Financial Condition Examiners Handbook, which is used to assess insurers’ financial condition, to include specific guidance for examiners reviewing insurers’ cybersecurity practices.

Despite these efforts, additional consumer protection measures are necessary, the Report maintains. It recommends that all insurers implement baseline protections against cyber risk based on industry standards and best practices. Of equal importance, the Report states, insurers that rely on third-party vendors should review and assess the adequacy of those vendors’ cyber risk management framework. With respect to state lawmakers, the Report calls for a review of existing and proposed laws and regulations and the uniform enactment of laws that heighten protection of consumer privacy.

* * *
The Report’s findings on big data, cyber risk and data privacy underscore the importance of striking an appropriate balance between protecting insurance consumers and over-regulation of the insurance industry in an increasingly connected world. It also leaves open the question of how the incoming Trump administration will address the myriad issues in this arena. While technological developments can be utilized to improve insurance products for consumers, as the Report explains, such developments also interject new cybersecurity and data privacy risks, which regulators and insurers must work together to address in order to maintain a fair and stable insurance marketplace.

Federal Communications Commission Chairman Signals Increased Oversight of Internet-of-Things Devices

Chairman Wheeler’s letter outlined a regulatory program aimed at reducing IoT threats, which would be complemented by ISPs’ responsibility to protect consumers and their ability to protect their networks as afforded through the FCC’s Open Internet Order. While recognizing the limitations of relying solely on market incentives to motivate ISPs to fully address harmful cyber activities, Chairman Wheeler wrote that complete cyber accountability would require both market-based incentives and appropriate regulatory oversight, where there are gaps in market effectiveness.

The proposed regulatory program, titled “5G/IoT Cybersecurity Risk Reduction Program Plan,” covers three broad areas of regulatory activities, which include: (1) federal advisory committees and voluntary stakeholder engagement; (2) leveraging interagency relationships; and (3) regulatory and rulemaking activities. These activities are briefly outlined below.

Federal Advisory Committee and Voluntary Stakeholder Engagement

Under this prong of regulatory engagement, Chairman Wheeler recommended that the FCC’s federal advisory committees could be charged with developing cyber risk reduction standards and best practices, as well as promoting ISP-wide adoption and implementation. Also proposed is the creation of an advisory committee, which could provide recommendations by targeting specific members of the communications ecosystem to prevent edge-based attacks. Finally, it was proposed that increased information sharing opportunities should be created, where market actors could candidly discuss cyberthreats and risk reduction challenges in an effort to foster collaboration.

Leveraging Interagency Relationships

In leveraging existing interagency relationships, Chairman Wheeler proposed that the Cybersecurity Forum for Independent and Executive Branch Regulators coordinate regulatory approaches to IoT risks across broader regulatory environments. A second proposal would be to convene a task force within the forum to assess the full scope of IoT cyberthreats to critical infrastructure and existing regulatory authorities, and outline mitigation recommendations. Finally, Chairman Wheeler called for continued collaborations with partners at various levels of government to identify unique state and local challenges.

Regulatory and Rulemaking Activities

Key proposals under regulatory and rulemaking activities include exploring a cybersecurity certification process for devices and creating consumer labeling requirements. Moreover, Chairman Wheeler has proposed issuing notices of inquiry on IoT cybersecurity in order to develop a record, in addition to identifying...
residual risks in IoT commons to determine where a market failure may exist in the ISP, network element manufacturer or device manufacturer community. Chairman Wheeler also called for changes to data gathering practices by the FCC and has proposed that the FCC identify data gaps in its network outage reporting framework. Such refined outage data could then enable the FCC to formulate best practices. Finally, it was proposed that regulators work with the Broadband Internet Technical Advisory Group and stakeholders in fifth-generation wireless technology and the IoT to build upon evolving risk reduction initiatives.

Key Takeaways
Chairman Wheeler’s letter signals increased regulatory attention to IoT threats and the wider IoT community. Moreover, it affirms that ISPs not only have the authority to protect consumers and their networks, but may have a responsibility to do so in accordance with the Open Internet Order.

However, Chairman Wheeler’s letter also reignites a debate over which government agency is uniquely equipped to regulate the internet and by extension IoT devices. When the FCC issued its 2015 Open Internet Order, it reclassified broadband providers as common carriers, effectively stripping the Federal Trade Commission (FTC) of authority over broadband providers. To justify FCC authority over IoT devices, Chairman Wheeler cites in his letter “a recent D.C. Circuit decision upholding the Commission’s authority over broadband networks [and thus] empower[ing] it to address core network issues,” such as IoT threats. While Chairman Wheeler did not cite the case by name, it is likely the June 2016 decision in *U.S. Telecom Association v. FCC*, No. 15-1063 (D.C. Cir.), which upheld the FCC’s reclassification of broadband providers as common carriers. Therefore, while it is clear that IoT devices and providers may face increased consumer responsibility and regulatory oversight, it is yet to be determined if such oversight will be done by the FTC or the FCC, as the legal objections to the FCC’s reclassifications are ongoing.

The “wild card” in this ongoing debate is how the Trump administration and a new FCC chair will address these issues. President-elect Trump has come out strongly against government regulations, but he also has been equally strong on the need to combat cyberattacks on U.S. companies. Regulation regarding cybersecurity may be an area where these two stated goals will need to be reconciled.

Return to Table of Contents

---

**Home Depot Directors Prevail in Cybersecurity Liability Claim: ‘Directors’ Decisions Must Be Reasonable, not Perfect’**

On November 30, 2016, the United States District Court for the Northern District of Georgia dismissed a shareholder derivative complaint against various current and former directors and officers of The Home Depot, Inc. relating to a breach of the company’s payment card data systems and theft of customers’ financial data. The decision, *In re The Home Depot, Inc. Shareholder Derivative Litigation*, No. 1:15-CV-2999-TWT (N.D. Ga. Nov. 30, 2016), serves as an important reminder that directors should be protected from liability in shareholder litigation in the event of a data breach, and are well-served when the record reflects regular board and board committee discussion and oversight of cybersecurity matters.

**Background**
In September 2014, Home Depot learned that hackers breached its payment card data systems and managed to steal the financial data of 56 million customers between April and September of 2014. Shareholder lawsuits against the company’s directors and officers followed soon thereafter. The plaintiffs alleged that Home Depot’s directors and officers failed to put sufficient internal controls in place to oversee the risk of a data breach. In particular, the plaintiffs pointed to the 2012 dissolution of the company’s infrastructure committee, which had been tasked with oversight of information technology and data security, as well as the fact that, although Home Depot’s proxy statements indicated that the audit committee was overseeing information technology and data security, the audit committee’s charter was never amended to reflect this added responsibility. The complaint asserted state law claims against directors and officers for breach of the fiduciary duty of loyalty and corporate waste, as well as claims for false and misleading proxy disclosure under the federal securities law. The defendants moved to dismiss the complaint.

**The Court’s Analysis**
As Home Depot is incorporated in Delaware, the state law claims were governed by Delaware law. The court noted that in the context of shareholder derivative litigation, Delaware law requires that plaintiffs first demand that the board of directors...
take action (i.e., bring a suit against the defendant directors and officers) unless making a demand is excused because it would have been futile. In this context, as no demand on the board had been made, establishing demand futility required a showing by the plaintiffs of director conduct that was so egregious on its face that a substantial likelihood of director liability existed.

A claim that directors breached their fiduciary duty of loyalty due to a failure of oversight requires showing that directors either knew they were not discharging their fiduciary obligations or that directors demonstrated a conscious disregard for their responsibilities, such as by failing to act in the face of a known duty to act. The court described this as an “incredibly high hurdle.” The court viewed as irrelevant the question of whether failure to amend the audit committee charter impacted the committee’s authority to oversee data security matters. More important, the court stated, was that the board and audit committee believed the committee had such authority and that the complaint detailed numerous instances of the audit committee receiving regular reports from management on data security matters, and the board in turn receiving regular briefings from both management and the audit committee. The complaint also acknowledged that before the data breach occurred, the board had approved a plan to address the company’s data security weaknesses. Thus, the record showed a board and audit committee engaged in cybersecurity oversight rather than directors completely failing to undertake their responsibilities. The fact that implementation of the plan, in hindsight, may have been too slow or incomplete was insufficient to establish a failure of oversight. The court noted that “directors’ decisions must be reasonable, not perfect.”

The court went on to dismiss the corporate waste claim, finding that the board’s decisions on cybersecurity matters fell within the board’s discretion under the business judgment rule. Finally, on the proxy disclosure claims, the court concluded that the plaintiffs failed to point out specific statements that were false or misleading.

**Implications for Companies**

Over the past few years, directors have gained an increased understanding of the risks faced by companies from cybersecurity and data breaches. These risks remain ever-present and require constant vigilance. Similarly, director oversight of these matters cannot be a one-time event. Boards and board committees with responsibility for oversight of cybersecurity risks should receive regular briefings from management or other advisers to understand how the risks are evolving and the steps the company is taking to manage and mitigate those risks. While a cyber breach perhaps may be inevitable, building a record of robust board oversight in this area should adequately protect directors from claims that they breached their fiduciary duties.

### The Commission on Enhancing National Cybersecurity Releases a New Report Detailing Recommendations for the Trump Administration

The Obama administration’s Commission on Enhancing National Cybersecurity released a report with suggestions on how to harden the nation’s cybersecurity and cyber response capabilities.

### The History of U.S. Cybersecurity Efforts and the Cybersecurity Commission

Recent presidential administrations have taken several actions in response to the nation’s evolving cybersecurity challenges. Common measures have included improving the security of infrastructure, encouraging joint efforts between the public and private sector, increasing the public awareness of cybersecurity and increasing investments in cybersecurity research.

During the Clinton administration, the focus was mainly on cybersecurity infrastructure, while the policies during the Bush administration transitioned to focus on homeland security and expanding the roles of different stakeholders in cybersecurity issues. The Obama administration has been very active in further developing cybersecurity policies, augmenting the policies regarding identity in cyberspace and secure information sharing among businesses and government agencies.

In February 2016, President Obama established the Commission on Enhancing National Cybersecurity (the Commission). The Commission consists of 12 members from various sectors with deep knowledge and experience in cybersecurity, the digital economy, national security and law enforcement, corporate governance, risk management, information technology and privacy. The president charged the Commission with developing actionable recommendations (both short and long term) for securing the digital economy. In December 2016, the Commission released the “Report on Securing and Growing the Digital Economy” (the Report), key points of which are summarized as follows.7

### The ‘Report on Securing and Growing the Digital Economy’

The Report identified successfully implemented measures, areas of weakness and areas for growth, as the Commission focused on ways to incentivize a culture of cybersecurity awareness in both the public and private sectors. The Report suggested ways to protect privacy; ensure public safety and economic and national security; foster discovery and development of new technical

---

7 View the report [here](#).
solutions; and bolster partnerships between the private sector and all levels of government to promote the use of cybersecurity technology, policies and best practices.

As a preliminary matter, the Commission identified the significant cybersecurity challenges facing the public and private sector today. The broad findings included the following:

1. Technology companies are under significant market pressure to innovate and move to market quickly, often at the expense of cybersecurity;
2. Organizations and their employees require flexible and mobile working environments, which are often prone to significant cybersecurity threats;
3. Many organizations and individuals still fail to do the basics;
4. Both offense and defense adopt the same innovations;
5. The attacker has the advantage;
6. Technological complexity creates vulnerabilities;
7. Interdependencies and supply chain risks abound;
8. Governments are as operationally dependent on cyberspace as the private sector; and
9. Trust is fundamental.

**Imperatives, Recommendations and Action Items**

In response to the findings, the Commission set forth six broad, overarching imperatives and further detailed specific action items (in the short and medium term) for their achievement:

1. **Protect, defend and secure today’s information infrastructure and digital networks.** The Commission recommended that the private sector and the presidential administration collaborate to improve the security of digital networks by better defending attacks on users and the nation’s network infrastructure. Additionally, as the cyber and physical worlds increasingly converge, the federal government should work closely with the private sector to develop a new model for how to defend this infrastructure. Finally, the Commission recommended that the Trump administration launch a national public-private initiative to improve identity management by increasing the use of strong authentication protocols and develop concrete efforts to support and strengthen the cybersecurity of small and medium-sized businesses.

2. **Innovate and accelerate investment for the security of digital networks and the digital economy.** The Commission recommended that the federal government and private-sector partners should join forces to improve the security of the internet of things (IoT). The report also suggested that the federal government make the development of usable, affordable, secure, defensible and resilient systems its top priority for cybersecurity research and development.

3. **Prepare consumers to thrive in and navigate through the digital age.** The Commission proposed the following two action items: First, business leaders in the IT and communications sectors need to work with consumer organizations and the FTC to provide consumers with better information so that they can make informed decisions regarding their privacy. Second, the federal government should strengthen investments in research programs to improve the cybersecurity and usability of consumer products and digital technologies through greater understanding of human behaviors and their interactions with connected technologies.

4. **Build cybersecurity workforce capabilities.** The Commission recommended that the nation should proactively address workforce gaps through capacity building (namely, job growth in lagging sectors), while simultaneously investing in innovations, such as automation, machine learning and artificial intelligence that will inevitably redistribute workforce required in the future.

5. **Better equip government to function effectively and securely in the digital age.** The Commission noted that the federal government should take advantage of its ability to share components of the IT infrastructure by consolidating basic network operations among federal agencies. The Report stated that the president and Congress, in particular, should promote technology adoption and accelerate the pace at which technology is refreshed within the federal sector. The government should move federal agencies from a cybersecurity requirements management approach to one based on enterprise risk management, and should better match cybersecurity responsibilities within the executive branch. Finally, government at all levels must clarify its cybersecurity mission responsibilities across departments and agencies to protect and defend against, respond to, and recover from cybersecurity incidents.

6. **Ensure an open, fair, competitive and secure global digital economy.** The Commission concluded that the Trump administration should encourage and actively coordinate with the international community to create and harmonize their cybersecurity policies with existing global practices and international agreements on cybersecurity law.
Next Steps

The Commission concluded the Report by highlighting the importance of urgent action, recommending that the Trump administration prepare a cohesive, thorough plan for implementing the recommendations of the Report, including metrics that focus on outcomes to measure progress toward a more secure environment. The Report concluded with a call to action, encouraging parties and stakeholders not to hesitate to improve their own security while the Commission’s recommendations are being considered.

If you have any questions regarding the matters discussed in this newsletter, please contact the following attorneys or call your regular Skadden contact.

**Stuart D. Levi**
Partner / New York
212.735.2750
stuart.levi@skadden.com

**James R. Carroll**
Partner / Boston
617.573.4801
james.carroll@skadden.com

**Brian W. Duwe**
Partner / Chicago
312.407.0816
brian.duwe@skadden.com

**David C. Eisman**
Partner / Los Angeles
213.687.5381
david.eisman@skadden.com

**Patrick Fitzgerald**
Partner / Chicago
312.407.0508
patrick.fitzgerald@skadden.com

**Todd E. Freed**
Partner / New York
212.735.3714
todd.freed@skadden.com

**Marc S. Gerber**
Partner / Washington, D.C.
202.371.7233
marc.gerber@skadden.com

**Lisa Gilford**
Partner / Los Angeles
213.687.5130
lisa.gilford@skadden.com

**Richard J. Grossman**
Partner / New York
212.735.2116
richard.grossman@skadden.com

**Amy S. Park**
Partner / Palo Alto
650.470.4511
amy.park@skadden.com

**Ivan A. Schlager**
Partner / Washington, D.C.
202.371.7810
ivan.schlager@skadden.com

**David E. Schwartz**
Partner / New York
212.735.2473
david.schwartz@skadden.com

**Michael Y. Scudder**
Partner / Chicago
312.407.0877
michael.scudder@skadden.com

**Jennifer L. Spaziano**
Partner / Washington, D.C.
202.371.7872
jen.spaziano@skadden.com

**Helena J. Derbyshire**
Of Counsel / London
44.20.7519.7086
helena.derbyshire@skadden.com

**Jessica N. Cohen**
Counsel / New York
212.735.2793
jessica.cohen@skadden.com

**Peter Luneau**
Counsel / New York
212.735.2917
peter.luneau@skadden.com

**James S. Talbot**
Counsel / Washington, D.C.
202.371.4133
james.talbot@skadden.com

**Joshua F. Gruenspecht**
Associate / Washington, D.C.
202.371.7316
joshua.gruenspecht@skadden.com
Pending LabMD Case May Limit Enforceability of FTC Act in Data Breach Matters

An 11th Circuit panel issued an order earlier this month delaying enforcement of the Federal Trade Commission’s (FTC) order against LabMD, finding that the company would be irreparably harmed without a stay because of the costs LabMD would incur in complying with the FTC’s order, and that LabMD’s data security practices may not have been unfair within the meaning of the FTC Act.

Background

As previously reported, LabMD — a now defunct Atlanta-based cancer detection company — suffered two separate data breaches during which personal health data belonging to approximately 10,000 consumers was disclosed, with one uncovered in 2008 and the other in 2012. Employees of a data security firm, Tiversa Holding Company (Tiversa), uncovered the LabMD data files on a peer-to-peer network while conducting a search for exposed sensitive data in an attempt to generate demand for its security services. Tiversa gave LabMD’s name to the FTC as part of a list of companies with allegedly poor information security infrastructure after LabMD refused to use Tiversa’s security services.

In August 2013, the FTC filed an action against LabMD under Section 5 of the FTC Act alleging that LabMD’s failure to implement appropriate data protection measures likely would cause substantial harm to consumers and constituted an unfair business practice under the FTC Act. An administrative law judge dismissed the complaint due to lack of proof that anyone aside from Tiversa had ever accessed the sensitive files, therefore concluding the breach was unlikely to be a source of harm to consumers. The

---

1 LabMD, Inc. v. Federal Trade Commission, case number 16-16270, in the U.S. Court of Appeals for the 11th Circuit.
2 See our previous article on the matter here.
FTC reversed and issued a final order requiring LabMD to take certain remedial measures, including ordering the company to implement an information security system, obtain biennial assessments by an outside auditor and notify patients affected by the data leaks. Citing the burden of the FTC case, LabMD announced in January 2014 that it was winding down its operations but continued to battle the FTC’s claims. LabMD requested a stay of the final order and appealed to the 11th Circuit in September 2016 after the FTC denied its request.

**Appeal to the 11th Circuit**

The 11th Circuit found that “there are compelling reasons why the FTC’s interpretation [of the unfairness prong of the FTC Act] may not be reasonable” and, as such, LabMD is likely to succeed on the merits. The court doubted that the FTC Act encompasses intangible emotional or reputational harms to consumers arising from the disclosure of sensitive data. In addition, the court found that the FTC’s interpretation of “causes or is likely to cause substantial injury to consumers,” a requirement for enforcement under the unfairness prong of the FTC Act, was not reasonable, as the FTC interpreted this to mean “significant risk,” based on the sensitive nature of the data, rather than “probable risk.” In other words, the mere fact that sensitive data was exposed is not sufficient to show that consumers are likely to be harmed.

The 11th Circuit also found that LabMD proved it would be irreparably harmed without a stay, citing the fact that the costs of complying with the order to implement remedial measures would exceed the less than $5,000 cash the company currently had on hand. The court also found that there would be no substantial injury to other parties since LabMD is no longer operating, and thus, that there is no current risk of breach.

**Next Steps**

The appeal will now proceed on the merits, but the fact that the court granted a stay suggests that the 11th Circuit may be receptive to LabMD’s arguments for reversal of the FTC’s order. The outcome of the case could limit the FTC’s ability to enforce the FTC Act with regard to data breaches where the harm to consumers is intangible, or risk of harm to consumers is low, even in cases where the data at issue is sensitive in nature.

---

**NIST Guides Industry Players in Effort to Secure the Internet of Things**

The National Institute of Standards and Technology has issued a framework for securing devices connected to the internet that focuses on the engineering necessary to help prevent system compromises, recover from cyberattacks and protect the personal data collected by such devices.

The National Institute of Standards and Technology (NIST) has released detailed guidance on securing devices connected to the internet. Recent cyberattacks have spurred increased attention on the nascent industry and what can be done to secure the devices that constitute the fast-growing internet of things.

**Background**

On November 15, 2016, NIST, part of the Department of Commerce, released 257 pages of guidance that it has developed over four years regarding incorporation of strong security features into devices connected to the internet. The Department of Homeland Security recently released a similar document, which focuses on higher-level security issues, while the NIST guidance concentrates on more granular implementation strategies. One driver for the release of this guidance is that products, and the software within them, are growing more interconnected and complex, and some projections indicate that the breadth of the internet of things could reach 50 billion devices by 2020. As part of this growth, more issues related to hacking, service disruption and data leaks are likely to emerge.

The release of the NIST publication was moved up in the aftermath of a massive distributed denial-of-service (DDoS) attack in late October 2016 that blocked access to many popular web destinations, including Netflix, Amazon and Twitter. The attack exposed how easy it can be to hack millions of devices and how much damage attacks can cause if left unchecked by more aggressive security protocols. The October attack was carried out using tens of millions of internet protocol addresses linked to webcams and DVRs around the world and was targeted at the domain service provider, Dyn. The webcams and DVRs were infected with malware known as Mirai, which exploited the fact

---

³ A copy of the guidance can be found [here](#).
that many such systems use default usernames and passwords that do not need to be changed by end users. This intrusion demonstrated that the threat posed by an unsecured internet of things goes beyond that of exposed data to a destabilized internet infrastructure.

Important Aspects

Titled “Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems,” the NIST guidance aims to provide a framework to secure the plethora of devices connecting to the growing internet of things. Though these guidelines are voluntary, the implementation of a standards-based structure is aimed at altering the status quo and increasing investment in securely engineered systems.

The document focuses on the engineering that is necessary to (i) help prevent system compromises, (ii) recover from cyberattacks and (iii) protect the personal data that is increasingly stored in internet of things devices. As such, this guidance goes beyond mere “cyber hygiene,” which includes building firewalls and patching systems. It includes 30 technical standards and security principles that aim to guide the construction of a fundamental architecture and design that contributes to overall security. The goal is to build security safeguards directly into the products and remain aware of security at every stage of the product life cycle and, to this end, the framework offers guidance on the complete product life cycle: Agreement Process, Organizational Project-Enabling Process, Technical Management Process and Technical Process. By taking this approach, NIST essentially has provided a preventative maintenance handbook that tries to avoid the pitfalls inherent in addressing problems only as they surface. NIST has taken into account that all organizations and systems are unique, and as such the guidance is intended to be flexible enough to fit many companies’ needs.

Implications for Companies

Many experts believe that the threat from cyberattacks, like those carried out against Dyn, will remain substantial into the future, and this guidance may help to prevent similar problems if manufacturers embrace stronger security protocols while the internet of things is still in its infancy. This publication and the conversation surrounding the recent cyberattacks against Dyn present an opportunity for companies to reassess cybersecurity systemwide.

Not only will companies face technological challenges from this evolving landscape, but potential legal and regulatory pitfalls are evident for those who do not properly address security flaws. For example, though the guidance is voluntary, because it sets out generally applicable standards, those standards may become common practice in the industry. If companies do not comply with common practice, companies may find themselves facing potential liability from regulators or private litigants. In addition to the specter of legal liability, there are implications for companies’ insurance policies, as underwriters may look to this framework in gauging risk when offering insurance products related to cybersecurity for manufacturers of these devices.

New Chinese Cybersecurity Law May Have Far-Reaching Impact on Foreign Business

A controversial Chinese cybersecurity law presents new obstacles for multinational companies conducting business in China. The new law includes data localization requirements for both personal and business data, and obligations to submit to government security reviews.

On November 7, 2016, the Standing Committee of China’s National People’s Congress, the top legislative body of the People’s Republic of China, approved a new cybersecurity law that grants the Chinese government increased centralized power to “ensure network security, to safeguard cyberspace sovereignty, national security and the societal public interest.” The law was first published as a draft in July 2015 and has since garnered criticism from the international business community and rights organizations throughout its drafting process. Despite persistent pushback from overseas critics, the law will go into effect on June 1, 2017. The law will apply to the construction, operation, maintenance and use of information networks in China, as well as supervision and management of network security within China.

Corporate critics of the cybersecurity law have focused on the breadth of key provisions, suggesting that parts of the new law will make it difficult for multinationals to operate in China, or, at the very least, make it significantly more expensive for them to do so. Analysts also have suggested that the law’s vagueness indicates that the Cyberspace Administration of China will have broad latitude to direct how the law is interpreted and enforced.

The new law places increased obligations on three types of entities conducting business in China: (i) critical information infrastructure operators, (ii) network operators, and (iii) network products and services providers. The obligations imposed on each are briefly outlined below.

4 An official English version of the new law has not yet been released by the Chinese government. An unofficial English translation can be found [here](#).
Obligations Imposed on Critical Information Infrastructure Operators

The law imposes a number of new requirements on entities that are critical information infrastructure operators. However, the definition of such entities is vague, making those new requirements applicable to any number of companies. Under the terms of the new law, critical information infrastructure includes “public communication and information services, power, traffic, water, finance, public service, electronic governance and other critical information infrastructure that if destroyed, losing function or leaking data might seriously endanger national security, national welfare and the people’s livelihood, or the public interest, on the basis of their tiered protection system.”

As provided in Article 37, companies deemed critical information infrastructure operators are required to store within mainland China any personal information and “other important data” — currently undefined by the new law — gathered or produced during operations. The law provides one exception to its data localization requirement, namely where a business requirement to share such data outside of China is “truly necessary.” However, what qualifies as “truly necessary” remains undefined, and companies seeking reprieve under this exception would still have to submit to a security assessment, which some have noted may require companies to disclose sensitive information to the government. An earlier draft of the law suggested that disclosure of source code would be required as part of the security assessment, but the reference was removed following protests from other countries.

Obligations Imposed on Network Operators

Under the new law, broad obligations are placed on network operators, which are defined as “network owners, managers and network service providers.” A network “refers to systems comprised of computers or other information terminals and related equipment that follow certain rules and procedures for information gathering, storage, transmission, exchange and processing.” Network operators are expected to adhere to social mores, commercial ethics and to “accept supervision from the government and public.” What is meant by “supervision from the government” is currently unclear.

Moreover, network operators that provide “network access and domain registration services for users, phone network access or provide users with information publication or instant messaging services” must require their users to provide “real identity information.” If a user refuses to provide such information, network operators must refuse to provide them with relevant services. Pursuant to Article 28, network operators also should be prepared to provide “technical support” to public security and state security organizations to aid in their efforts to preserve national security and investigate crimes. The law has not defined what is contemplated by “technical support.” However, some have speculated that this support obligation could mean turning over personal data or encryption keys to the Chinese government.

Network operators additionally are obligated to perform a series of security protection duties, which include: (i) formulating internal security management systems; (ii) adopting preventative cybersecurity technological measures; (iii) adopting monitoring and recording technological measures, including retaining logs for at least six months; and (iv) classifying and encrypting data.

Finally, the new law offers increased protection to data subjects, at least as such protection relates to their internet service providers, if not the Chinese government. Absent data subject consent, network operators must not provide personal information to third parties, unless the data subject is “unidentifiable and cannot be recovered.” Under the new rules, data subjects have the ability to correct flawed personal information and may have such information deleted if the network operator “violated the provisions of laws, administrative regulations or agreements between the parties to gather or use their personal information.”

Obligations Imposed on Providers of Products and Services

Providers of network products and services must inform users and “competent departments” whenever a security flaw or vulnerability is discovered. The new law specifically highlights “critical network equipment” and “specialized network security products,” which either must meet certification standards or meet safety inspection requirements before being sold on the Chinese market. The law does not specify such standards or requirements.

Penalties for Non-Compliance

The law provides for a number of enforcement mechanisms that can be invoked against companies and individuals for violating the law, depending on the nature of the violation. Regulators can shut down websites, freeze assets and revoke business licenses, and, in some cases, individuals may be detained for up to 15 days. Fines also may be imposed on companies or management personnel; fines against companies range from approximately $7,500 to $150,000, and fines against individuals range from approximately $750 to $15,000.

Key Takeaways

Given the law’s broad definitions of entities to which it applies, companies that typically may not identify themselves as critical information infrastructure operators, network operators, or network product and service providers may nonetheless find
themselves subject to the requirements of the new law. Companies that may fall within these definitions and that consider China a significant part of their business model should compare their current practices with the requirements of the law and identify any changes that would need to be implemented to comply by June 1, 2017. It is anticipated that Chinese government agencies and industry organizations will issue more detailed implementing regulations and standards prior to the June effective date, which should provide further guidance to companies seeking to comply with the new law.

Return to Table of Contents

Russian Court Allows Communications Agency to Block LinkedIn

Russia has blocked access to LinkedIn, citing the company’s violation of a Russian data protection law that requires personal data of Russian users to be stored on servers located in Russia.

On November 18, 2016, Russia blocked access to LinkedIn, the world’s largest professional social network, after a Moscow court paved the way for the ban. The court upheld a decision to block LinkedIn within Russia after the company was alleged to have violated a Russian data protection law. The law, passed in September 2015, requires online service providers to store the personal data of Russian users on servers within the country’s borders. The controversy with LinkedIn marks the first time Russia has enforced this data localization law.

Background

In August, the Russian communications agency Roskomnadzor, which is responsible for matters in the telecom, information technology and mass communications fields, filed a complaint against LinkedIn in the Tagansky District Court. That court ruled in favor of Roskomnadzor, concluding that LinkedIn violated the Russian data protection law on two counts. First, it ruled that LinkedIn did not store personal information about Russian users within the country, and second, that the company processed information about individuals who were not registered on the site and had not agreed to the company’s user agreement. LinkedIn appealed the ruling, but a Moscow court upheld the lower court on November 10, 2016, allowing Roskomnadzor to block the website.

Ramifications for Other Worldwide Internet Service Providers

Russia has said the purpose of the law is to protect citizens’ personal data, but skeptics view it as a threat to foreign social networks and a means for Russia to gain control over the internet and user data. However, other countries, such as Germany, have passed similar laws, requiring technology companies to store users’ information on local servers, without facing similar skepticism.

Some have speculated that LinkedIn was targeted as a means of sending a message to other companies. According to Roskomnadzor, other large U.S.-based online service providers have already started to move personal data storage to Russia in compliance with the law. In the aftermath of this court decision and subsequent ban, it is unclear whether other global technology companies will comply with the law or risk having their services banned in Russia. In light of these developments, companies that process the personal data of Russian citizens, and that consider Russia an important component of their business models, should evaluate their compliance with the data localization law.

Return to Table of Contents

(Attorney contacts appear on the next page.)
If you have any questions regarding the matters discussed in this newsletter, please contact the following attorneys or call your regular Skadden contact.

**Stuart D. Levi**
Partner / New York
212.735.2750
stuart.levi@skadden.com

**James R. Carroll**
Partner / Boston
617.573.4801
james.carroll@skadden.com

**Brian W. Duwe**
Partner / Chicago
312.407.0816
brian.duwe@skadden.com

**David C. Eisman**
Partner / Los Angeles
213.687.5381
david.eisman@skadden.com

**Patrick Fitzgerald**
Partner / Chicago
312.407.0508
patrick.fitzgerald@skadden.com

**Todd E. Freed**
Partner / New York
212.735.3714
todd.freed@skadden.com

**Marc S. Gerber**
Partner / Washington, D.C.
202.371.7233
marc.gerber@skadden.com

**Lisa Gilford**
Partner / Los Angeles
213.687.5130
lisa.gilford@skadden.com

**Richard J. Grossman**
Partner / New York
212.735.2116
richard.grossman@skadden.com

**Amy S. Park**
Partner / Palo Alto
650.470.4511
amy.park@skadden.com

**Timothy G. Reynolds**
Partner / New York
212.735.2316
timothy.reynolds@skadden.com

**Ivan A. Schlager**
Partner / Washington, D.C.
202.371.7810
ivan.schlager@skadden.com

**David E. Schwartz**
Partner / New York
212.735.2473
david.schwartz@skadden.com

**Michael Y. Scudder**
Partner / Chicago
312.407.0877
michael.scudder@skadden.com

**Jennifer L. Spaziano**
Partner / Washington, D.C.
202.371.7872
jen.spaziano@skadden.com

**Helena J. Derbyshire**
Of Counsel / London
44.20.7519.7086
helena.derbyshire@skadden.com

**Jessica N. Cohen**
Counsel / New York
212.735.2793
jessica.cohen@skadden.com

**Peter Luneau**
Counsel / New York
212.735.2917
peter.luneau@skadden.com

**James S. Talbot**
Counsel / New York
212.735.4133
james.talbot@skadden.com

**Joshua F. Gruenspecht**
Associate / Washington, D.C.
202.371.7316
joshua.gruenspecht@skadden.com
FCC Approves New Rules for Broadband Privacy

The FCC has approved new rules addressing how internet service providers must protect broadband users’ privacy.

The Federal Communications Commission (FCC) voted on October 27, 2016 to approve a proposal for rules to safeguard the privacy of broadband users. These rules require internet service providers (ISPs) to obtain explicit “opt-in” consent before collecting a wide range of what is deemed “sensitive information,” provide information to consumers about the data the ISP collects and allow consumers to opt out of most ISP collection of information.

Rules Requirements

The FCC has not yet published the final order describing the rules, but considering the commission’s initial notice of proposed rulemaking, FCC Chairman Tom Wheeler’s fact sheet outlining the ultimate proposed order in advance of the October meeting, and other FCC blog posts and related reporting, the broad outlines of the new rules are reasonably clear. Based on what has been made available to date, the new rules will require ISPs to:

- notify consumers about the types of information they are collecting. ISPs must provide this information when a customer signs up for service, and then update their customers if the privacy policy changes in significant ways. This information also must always be available on an ISP’s website or mobile app. The commission also has directed its Consumer Advisory Committee (CAC) to develop a standardized privacy notice format that, although voluntary, would provide a “safe harbor” for ISPs that choose to adopt it;
- specify how and for what purposes that information can be used and shared;
- identify the types of entities with which the ISP shares the information;
- most significantly, ISPs must offer affirmative opt-in consent for the collection and use of sensitive data. Opt-in consent refers to a paradigm where the default is that a consumer’s data may not be used unless the consumer checks a box, or otherwise...
manifests his or her explicit consent that his or her data may be used. While “sensitive” data includes categories that are traditionally considered sensitive, such as health and financial information and information concerning children, it also includes a number of categories that are the lynchpin of targeted advertising and a key revenue source for ISPs, including web browsing and app usage history. Many ISPs have expressed concern that obtaining opt-in consent for such data will hamper their ability to sell targeted advertising, resulting in higher prices for consumers. However, ISPs are prohibited from refusing to serve customers who do not consent to the use and sharing of their information for commercial purposes;

- take reasonable measures to protect consumer data from breaches and other vulnerabilities;
- notify consumers as soon as possible, but no later than 30 days, after reasonable determination of a breach, and notify the FCC, the FBI and the Secret Service of breaches affecting 5,000 or more customers no later than seven business days after reasonable determination of the breach. The FCC must be notified at the same time as customers if the breach affects fewer than 5,000 customers;
- disclose any plans that relate service price to privacy protections;
- allow consumers to “opt out” of using other personal data except as necessary for the provision of service, billing and certain other purposes; and
- adequately “de-identify” consumer data before sharing it as non-personal data.

Timing
The final effective dates of the rules will be announced with publication of the final order in the Federal Register. Based on information available to date, the various aspects of the order are to go into effect according to the following timeline:

- Data security requirements: 90 days after the order is published;
- Data breach notification requirements: six months after the order is published; and
- Notice and consent requirements: 12 months after the order is published, though small providers are expected to have an additional 12 months to come into compliance.

Rationale
Chairman Wheeler published a blog post on October 6, 2016, on the FCC’s website\(^1\) outlining his reasoning for proposing the new regulations. He emphasized that, prior to the passage of the new rules, there had been no regulations in place outlining how ISPs could use and share customers’ personal information even though parallel rules had been in place for decades requiring telephone companies to protect the information associated with phone calls and text messages.

“Our goal throughout the process has been straightforward: to give consumers the tools they need to make informed decisions about how ISPs use and share their data, and the confidence that ISPs are taking steps to keep that data secure, all while providing ISPs the flexibility they need to continue to innovate,” Wheeler wrote in the post.

Wheeler also wrote that the new rules are based on extensive feedback the FCC has received from consumer and public interest groups, fixed and mobile ISPs, advertisers, app and software developers, academics, other government actors including the FTC, and individual consumers.

FCC Jurisdiction and Scope of Rules
Broadband service providers have only recently become subject to FCC jurisdiction. Their status changed when the FCC reclassified broadband as a utility last year as part of new net neutrality regulations, a decision recently upheld by the U.S. Court of Appeals for the District of Columbia Circuit.\(^2\)

The new rules apply to information collected from consumers using broadband services, such as residential or mobile connections. The rules do not, however, apply to the privacy practices of websites or apps, over which the FTC has authority (even if the website or app is owned by a broadband provider).

Retreat From Initial Proposal
The new scaled-back rules were proposed after the FCC received strong negative feedback on an initial proposal by Chairman Wheeler. ISPs such as Verizon, AT&T and Comcast criticized the initial proposal for subjecting them to more stringent requirements than those imposed by the FTC, which apply to major web services such as Facebook, Twitter and Google. In particular, the ISPs objected to broad requirements under the initial proposal that required them to obtain affirmative consent for using nearly all consumer data. The more limited consent and opt-out obligations in the new rules reflect a concession to these industry concerns.

Next Steps
The final order from the FCC describing the rules are expected to be released by the FCC in the coming days. Once the rules have passed through internal executive branch review, they will

---

\(^1\) Available here.

\(^2\) Available here.
be published in the Federal Register, and unless challenged in court and subject to a stay, the rules can be expected to take effect soon thereafter based on the timeline above. We will be monitoring for publication by the FCC, and will provide updates as they develop.

Return to Table of Contents

FTC Releases Playbook for Data Breach Response and Notification

On October 25, 2016, the Federal Trade Commission (FTC) released a guidebook, together with a blog post and accompanying video, on how companies should respond to data breaches, including how they should notify affected consumers. The FTC also attached a model letter to be sent to individuals informing them of the data breach, which we expect will become the form that most companies under the jurisdiction of the FTC adopt.

Although the guidelines are nonbinding, companies should expect that the FTC will use them as a benchmark when determining if a company’s response to a data breach was so inadequate that it constituted unfair business practices under the FTC Act. Further, other agencies may use this guidance as a foundation for crafting their own data breach response guidelines. Finally, companies can expect that plaintiffs’ attorneys will highlight any disconnect between the guidelines and the company’s actions in responding to a data breach while trying to establish that the company acted negligently.

Response to Data Breach

In its guidance, the FTC addresses the key steps companies should take in response to a data breach, with specific recommendations for action at each step, beginning with the steps taken to secure operations and ending with providing required notices of the breach.

Secure Operations

Companies that suffer a data breach should move quickly to secure their operations. In order to achieve this, the FTC suggests companies should:

- secure systems and fix vulnerabilities that caused the breach;
- assemble a team of experts to conduct the breach response, including a forensics team and external legal counsel;
- secure physical areas potentially related to the breach, including by locking them and changing access codes;
- stop additional data loss by taking affected equipment offline immediately and updating credentials and passwords;
- remove improperly posted information from the web, both on sites the company controls and by making requests of the applicable third parties from third-party sites; and
- interview people who discovered the breach to gather information on the breach.

In taking these steps, the FTC advises not to turn off affected machines or otherwise destroy forensic evidence.

Fix Vulnerabilities

After securing systems against additional losses, companies should fix vulnerabilities that caused the breach. As part of this process, the FTC suggests companies should:

- if a service provider was involved, review its access privileges to company information and ensure it is taking steps to prevent further breaches;
- examine whether existing efforts to segment internal networks to contain damage have been effective;
- work with forensics experts to determine how the breach occurred and whether defensive measures such as encryption were enabled; and
- have a comprehensive communication plan for providing information to employees, customers, business partners and investors of the incident, but do not publicly share information that could put consumers at risk.

Notify Appropriate Parties

Companies will need to notify law enforcement as well as other affected businesses and consumers. In order to provide proper notifications, companies should:

- determine their legal requirements involving notice, including state data breach notification requirements;
- notify law enforcement, starting with the local police and then the FBI or Secret Service if local police are not familiar with these types of investigations;
- check whether health information was involved and Health Insurance Portability and Accountability Act (HIPAA) notification requirements are implicated;
Privacy & Cybersecurity Update

- if account information was affected, notify affected businesses such as credit card companies and banks so that they can monitor for fraudulent activity;
- if information stored on behalf of other companies was affected, notify the other companies;
- if names and Social Security numbers were affected, contact the major credit bureaus; and
- notify consumers so they can take steps to reduce the chance their information will be misused.

Recommendations and Form of Letter for Notice to Individuals

The FTC’s guidance includes a number of specific suggestions for how to manage and what to say in notifications to individuals affected by a data breach. In particular, the FTC suggests providing at least one year of free credit monitoring or other support if financial information or Social Security numbers were affected.

The FTC also attached a model letter to be sent to individuals, which calls on companies to provide information on:
- how the breach occurred;
- what information was taken;
- how thieves used the information (if known);
- what steps the company has taken to remedy the situation;
- what actions the company is taking to protect the individual, such as free credit monitoring; and
- how to reach relevant contacts in the company’s organization for more information.

The FTC also recommends telling consumers how to contact the FTC and local law enforcement about the misuse of their information.

Role in FTC Enforcement and Potential Litigation

The FTC guidance goes beyond existing state and federal requirements relating to data breach notification by describing the full process for responding to a breach. The FTC has been very active in policing cybersecurity matters on the basis of its general authority to police unfair business practices. Given the absence of specific standards, the FTC has looked to industry practices and its own guidance to determine whether companies have violated the law. It is likely that the commission will look to its data breach response guidance in evaluating companies in the future. In addition, plaintiffs’ attorneys are likely to look to the FTC’s guidance as a benchmark for evaluating whether companies have responded appropriately.

Grocer Not Entitled to Coverage Under Traditional Insurance Policy for Liabilities Stemming from Computer Hacking Incident

An Alabama federal court recently ruled in favor of an insurer in a coverage battle with its insured, a grocery store operator, holding that the insured was not entitled to coverage under its business insurance policy for litigation commenced against it stemming from a cyberattack on its computer systems that compromised its customers’ confidential data.

On October 25, 2016, the U.S. District Court for the Northern District of Alabama ruled in Camp’s Grocery, Inc. v. State Farm Fire & Cas. Co. that a grocery store operator could not look to its business insurance policy for third-party claims arising out of an alleged computer hacking incident that compromised its customers’ confidential data. That ruling adds to the growing number of decisions throughout the country finding that policyholders may not be covered for cyber losses under “traditional,” noncyber insurance policies due to electronic data-related exclusions and serves as a reminder to policyholders to evaluate the adequacy of their coverage for cyber losses.

Background and Language of Policy

In the case, three credit unions sued Camp’s Grocery, Inc., an Alabama-based Piggly Wiggly, LLC franchisee, alleging that the grocer’s failure to adequately safeguard its computer systems led to a computer hacking incident. The credit unions allege that the computer hack compromised confidential credit, debit and check card information of its customers, which in turn caused the credit unions to suffer losses on their cardholder accounts. These losses included the reissuance of cards, reimbursement of customers for fraud losses and administrative expenses associated with investigating, correcting and preventing fraud.

At the time of the hacking incident, Camp’s Grocery was insured by State Farm Fire & Casualty Company pursuant to a business insurance package policy. The coverage provided by the policy included first-party property coverage, third-party liability coverage and inland marine computer property coverage which insured, among other things, “accidental direct loss” to “electronic data” including certain data of Camp’s Grocery’s customers used in connection with its business operations. Notably, some of the coverages contained limitations on electronic data-related losses: The first-party property coverage expressly excluded “electronic data” from the definition of “covered

property,” while the third-party liability coverage was subject to an electronic data exclusion. Camp’s Grocery sought coverage under the policy’s third-party liability and inland marine computer property coverages, and insurance litigation ensued.

**Court’s Decision**

In granting summary judgment in favor of State Farm, the court concluded that the policy did not afford coverage to Camp’s Grocery for the underlying action. The court rebuffed Camp’s Grocery’s argument that it was entitled to coverage based on the inland marine computer property coverage for the credit unions’ claims against it. The court instead found that those provisions “unambiguously afforded first-party coverage only,” citing the fact that “there [was] no language ... whereby State Farm promise[d] to ‘defend’ or ‘indemnify’ the insured, whether in regard to claims involving computer equipment, electronic data, or anything else, for that matter.”

The court was equally unpersuaded by Camp’s Grocery’s argument that it was covered under the policy’s business liability coverage because the credit union’s alleged losses for replacement of customer debit and credit cards constituted covered “property damage.” While acknowledging that the business liability coverage insured Camp’s Grocery for third-party property damage claims, the court nevertheless found Camp’s Grocery’s argument to be flawed because the credit unions did not allege that the grocer’s actions resulted in physical damage to their customers’ credit and debit cards. Rather, the court found, the underlying action alleged the compromise of “intangible electronic data contained on the cards,” which did not constitute “property damage” under the policy and, in any event, fell within the policy’s electronic data exclusion.

**Key Takeaway**

As the court’s decision in *Camp’s Grocery* illustrates, traditional insurance policies, including seemingly comprehensive package policies, may not respond to cyber losses. With an increasing number of insurers expressly limiting coverage for cyber incidents under traditional policies through the inclusion of electronic data exclusions and the like, businesses of all types would be well advised to consider purchasing coverage specifically geared to cyber losses, to the extent not already in place, to avoid being left without coverage in the event of a cyber incident.

---

**National Highway Traffic Safety Administration Issues Voluntary Guidance for Automotive Cybersecurity**

On October 24, 2016, the National Highway Traffic Safety Administration (NHTSA) issued “Cybersecurity Best Practices for Modern Vehicles” (NHTSA Guidance), a 21-page document offering voluntary guidance for improving motor vehicle cybersecurity. The document arrives at a time of increased concerns about automotive cybersecurity for the industry and consumers, and may provide a future benchmark against which auto companies and their suppliers are measured.4

**Background**

In July 2015, two researchers successfully hacked and took over control of a Jeep Cherokee using a laptop located miles away. As a result of the hack, the NHTSA recalled nearly 1.5 million vehicles, marking the first time the agency used its enforcement authority due to a cybersecurity vulnerability. Since July 2015, private-sector and governmental stakeholders have created a range of security initiatives for the automotive industry. In the private sector, three key initiatives were introduced in 2016 alone. These include the SAE Cybersecurity Guidebook for Cyber-Physical Vehicle Systems, the Automotive Sharing and Analysis Center (Auto ISAC), and a cybersecurity best practices framework developed by two automotive trade associations.

**Purpose of NHTSA Guidance**

The NHTSA’s focus on cybersecurity reflects a priority of the U.S. Department of Transportation to protect consumers from malicious cyberattacks and unauthorized access. The NHTSA Guidance is based on public feedback received by the NHTSA, as well as the National Institute of Standards and Technology’s (NIST) Framework for Improving Critical Infrastructure Cybersecurity (NIST Framework). According to the NHTSA, the guidance was conceived as a “resource to supplement existing voluntary cybersecurity standards,” and has a dual purpose: First,

---

4 The NHTSA’s guidance is available [here](#).
to provide best practices to help protect against breaches and other security failures that can put motor vehicle safety at risk, and second, to provide a solid foundation for developing a risk-based approach to prevent cybersecurity issues in the automotive industry.

**General Cybersecurity Guidance**

The NHTSA Guidance offers two general cybersecurity principles:

*Layered Approach*

According to the NHTSA Guidance, and in accordance with the NIST Framework, the automotive industry should develop a layered approach to vehicle cybersecurity. This approach should:

- be built upon risk-based prioritized identification and protection of safety-critical vehicle control systems and personally identifiable information;
- provide for timely detection and rapid response to potential vehicle cybersecurity incidents in the field;
- design methods and measures to facilitate rapid recovery from incidents when they occur; and
- institutionalize methods for accelerated adoption of lessons learned across the industry through effective information sharing, such as through participation in Auto ISAC.

*Information Technology Security Controls*

The NHTSA Guidance suggests that the automotive industry review and adapt the standards and controls designed for information technology networks utilized by other industry sectors. These include ISO 27000 series standards and other best practices, such as the Center for Internet Security’s “Critical Security Controls for Effective Cyber Defense” (CIS CSC). Moreover, industry leaders should follow the CIS CSC recommendations, which include: performing cybersecurity gap assessment, developing implementation road maps, executing cybersecurity plans, integrating controls into vehicle systems and business operations, and reporting and monitoring progress through iterative cycles.

**Automotive Industry Cybersecurity Guidance**

Outside of the two general cybersecurity principles, the NHTSA Guidance describes seven recommendations on subjects ranging from product development to best practices on researching and validating cybersecurity measures. These principles include:

1. **Vehicle Development Process With Explicit Cybersecurity Considerations**

The safety of vehicle occupants and other road users should be a primary consideration when assessing risk. Companies can mitigate such risks by making cybersecurity a priority through:

- Designing systems free of unreasonable safety risks: Companies should develop an ongoing process to evaluate risks and should systematically conduct safety risk assessment steps for the full life cycle of the vehicle. Companies also should develop rapid detection and remediation capabilities.

- Considering privacy and cybersecurity risks throughout the entire life cycle of the vehicle: The life cycle of the vehicle includes conception, design, manufacture, sale, use, maintenance, resale, and decommissioning.

- Collecting and documenting information: The automotive industry should collect information on any potential attack and share such information with the Auto ISAC. Companies should fully document any subsequent actions, changes, design choices, and analyses.

2. **Leadership Priority on Product Cybersecurity**

The automotive industry should foster a culture that is prepared to handle cybersecurity challenges. Companies should facilitate a top-down emphasis on cybersecurity to demonstrate seriousness throughout their organizations. The NHTSA suggests that such corporate priorities can be created by:

- Allocating resources: Companies should allocate dedicated resources for research, investigations, and testing of cybersecurity measures.

- Establishing communication channels: Companies should facilitate seamless communication through organizational ranks related to product cybersecurity and should enable independent voices within the safety design process.

3. **Information Sharing**

The NHTSA was instrumental in the formation of Auto ISAC and encourages all members of the vehicle manufacturing industry to participate. The guidance document also encourages Auto ISAC to expand its membership to suppliers and other vehicle segments.

4. **Vulnerability Reporting/Disclosure Policy**

Companies should develop additional mechanisms for information sharing, such as a vulnerability reporting and disclosure program. Automotive industry members should consider creating their own vulnerability reporting and disclosure policies or adopting a version used in a different sector. These policies should provide external cybersecurity researchers with guidance on how to disclose issues to automotive industry companies and
should describe the relationship between the company and any cybersecurity researchers.

5. Vulnerability/Exploit/Incident Response Process

The automotive industry should have a process for responding to incidents, vulnerabilities and exploits. This process should:
- cover impact assessment, containment, recovery and remediation actions;
- outline roles for each responsible group and specify requirements for internal and external coordination;
- ensure rapid response without sole dependence on any single individual;
- define metrics used to assess effectiveness of response process;
- document details of each identified and reported vulnerability, exploit or incident, and report them to the Auto ISAC, US-Cert and to the industrial control systems CERT, at the discretion of the company; and
- run periodic response capabilities exercises to test effectiveness of disclosure policy operations and internal response processes.

6. Self-Auditing

The NHTSA recommends that the automotive industry participate in self-auditing by:
- documenting details related to the cybersecurity process, which may include risk assessments, penetration results and organizational decisions;
- retaining documents through the expected life span of the associated product; and
- regularly revising documents such as cybersecurity requirements as new information, data and research become available.

7. Fundamental Vehicle Cybersecurity Protections

The NHTSA has issued recommendations informed through its own internal research. These recommendations are offered to help companies secure automotive computing systems and include: limiting developer/debugging access in production devices, protecting control keys, limiting diagnostic features, employing good security coding practices, and limiting use of network services to essential functionality.

Additional Cybersecurity Recommendations

The NHTSA Guidance concludes with three additional recommendations for the automotive industry. First, the NHTSA recommends that the automotive industry participate in cybersecurity education activities for its current workforce, but also future workforce and nontechnical individuals. Second, the guidance document encourages companies to consider aftermarket devices and equipment that may be brought into cars and connected with vehicle systems. Finally, the NHTSA recommends that implemented cybersecurity protections should not unduly restrict access by authorized third-party service repairers.

Key Takeaways and Next Steps

The NHTSA is accepting public comments on the NHTSA Guidance until November 23, 2016, after which it may revise its guidance or seek to address other related topics. Whatever the final result, the NHTSA Guidance — or its successors — will likely become a benchmark against which the automotive industry’s cybersecurity efforts are measured.

Return to Table of Contents

District Courts Dismiss Data Breach Suits Where No Actual Harm Was Alleged

In re Barnes & Noble Pin Pad Litigation, an Illinois district court dismissed a class action complaint for failure to allege cognizable damages, even though the plaintiffs had established “substantial risk of harm” for Article III standing purposes. In Kamal v. J. Crew Group, Inc., a New Jersey district court dismissed a class action complaint for failure to establish Article III standing where no actual harm,

In re Barnes & Noble Pin Pad Litigation

On October 3, 2016, the U.S. District Court for the Northern District of Illinois dismissed a class action complaint asserting common law and statutory claims based on a data breach at Barnes & Noble retail stores, holding that the complaint failed to plead cognizable damages even though the plaintiffs sufficiently pleaded Article III standing based on allegations they faced a substantial risk of harm. This decision makes clear that alleging substantial risk of harm to establish Article III standing is not, in itself, sufficient to survive a motion to dismiss.

Background and Claims

In September 2012, certain individuals tampered with PIN pad terminals used to process credit and debit card payments in 63 Barnes & Noble retail stores across nine states. Weeks after learning of this potential data breach, Barnes & Noble publicly announced that the individuals may have stolen customer credit and debit card information. The plaintiffs were customers of the 63 stores during the time when the data breach occurred.
On March 25, 2013, the plaintiffs filed a complaint asserting causes of action for: (1) breach of contract; (2) violation of the Illinois Consumer Fraud and Deceptive Business Practices Act; (3) invasion of privacy; (4) violation of the California Security Breach Notification Act; and (5) violation of California’s Unfair Competition Act. Barnes & Noble moved to dismiss the complaint for lack of standing and failure to state a claim under Federal Rules of Civil Procedure 12(b)(1) and 12(b)(6). The court granted the motion to dismiss for failure to establish Article III standing.

On September 24, 2013, the plaintiffs filed an amended complaint asserting the same causes of action and alleging six additional paragraphs of factual allegations. Barnes & Noble moved to dismiss the amended complaint, again for lack of standing and failure to state a claim.

The Court’s Decision

The court dismissed the amended complaint, but this time for failure to state a claim.

The court first addressed the issue of Article III standing, holding that the plaintiffs met their burden to plead injury in fact pursuant to the 7th Circuit’s holding in Remijas v. Neiman Marcus Group. In discussing Remijas, the court noted that the 7th Circuit held that allegations that hackers had targeted the plaintiffs’ credit card information made it “plausible to infer that the plaintiffs have shown a substantial risk of harm,” and that allegations of lost time and monetary cost to the Remijas plaintiffs to protect against future identity theft were sufficient to demonstrate a “substantial risk of harm.” Based on Remijas, the court held that the plaintiffs’ allegations that their personal identifying information had been taken from Barnes & Noble stores and used for unauthorized purposes, and that the plaintiffs had devoted time and money to preventing improper use of their personal identifying information were sufficient to establish Article III standing.

Next, the court addressed whether the amended complaint stated a plausible claim for relief. Regarding the breach of implied contract and statutory claims, the court held that the amended complaint failed to state a claim because it failed to plead any economic or out-of-pocket damages caused by the data breach. The court cited other cases holding that the loss of value of personal information cannot serve as damages in a breach of contract cause of action. The court also held that one of the plaintiffs’ allegations of damages for subscribing to an identity protection monitoring service was insufficient to state a claim because he had previously subscribed to that service and did not allege the data breach was the cause of his decision to subscribe. With respect to the California Security Breach Notification Act claim, the court further noted that there were no allegations that the six-week delay in reporting the data breach caused any injury.

Regarding the invasion of privacy claim, the court held that the plaintiffs failed to allege a public disclosure of any of the plaintiffs’ personal identifying information, a requirement for stating a claim. The court held that the information’s accessibility by those who sold it and those who potentially purchased it was not sufficient to serve as a public disclosure. Moreover, the court noted that the stolen personal identifying information would not qualify as highly offensive to a reasonable person, an additional requirement to stating a claim.

Kamal v. J. Crew Group, Inc.

On October 20, 2016, the U.S. District Court for the District of New Jersey dismissed a class action complaint asserting a single cause of action for violation of the Fair and Accurate Credit Transactions Act (FACTA) based on the allegation that printing more than the last five digits of a customer’s credit card number on receipts violated the statute. The court held that the complaint failed to establish Article III standing because no actual injury was alleged and the allegations of possible future harm, in contrast to “certainly impending” future harm, were not sufficiently “concrete” to qualify as an injury in fact.

Background and Claims

The defendants are a group of clothing stores and manufacturers known as J. Crew and parent company Chino’s Holdings, Inc. The plaintiff alleged that in December 2014 and January 2015, he visited several of the defendants’ stores and made purchases with a credit card. The plaintiff alleged that the receipts he was given contained the first six and last four digits of his credit card number. The plaintiff filed this action on behalf of customers, who, like the plaintiff, received receipts from the defendants that displayed more than the last five digits of their credit card numbers.

The complaint alleged a single cause of action for violating FACTA. The court denied a motion to dismiss under Rule 12(b)(6), holding that the plaintiff stated a claim for the willful violation of FACTA’s credit card number truncation provision. The court then stayed the matter while Spokeo Inc. v. Robins was pending in the U.S. Supreme Court. Following the Spokeo decision and supplemental briefing, the court addressed whether the plaintiff had Article III standing.

---

5 794 F.3d 688 (7th Cir. 2015).
**Privacy & Cybersecurity Update**

**The Court’s Decision**

The court cited *Spokeo* for the propositions that (1) an “injury in fact” must be “concrete” in order to establish Article III standing; (2) although “injury in fact” may be “intangible,” it must be “actual or imminent, not conjectural or hypothetical”; and (3) allegations of future harm must “entail a degree of risk sufficient to meet the concreteness requirement.”

The court held that the plaintiff’s allegations of printing 10, rather than five, credit card digits on a sales receipt were insufficient to establish Article III standing. The court reasoned that no allegations established (1) a sufficiently “actual or imminent” risk of future harm; (2) that anyone had accessed, attempted to access or will access the plaintiff’s credit card information; (3) that any of the plaintiff’s credit card information had been disclosed to third parties; or (4) any actual harm to the plaintiff’s credit or identity. Instead, the court found that the allegations were more akin to an increased risk of a data breach sometime in the future, which the court held was not sufficiently “concrete” to qualify as an “injury in fact.”

Accordingly, the court granted the motion to dismiss pursuant to Rule 12(b)(1) for failure to establish Article III standing.

**Key Takeaways**

The decisions make clear that while some circuits have lowered the bar for establishing Article III standing in the wake of *Spokeo*, courts will still closely analyze pleadings to determine whether plaintiffs have pleaded cognizable damages sufficient to establish Article III standing and sufficient to state a claim. As these cases show, establishing Article III standing does not guarantee sufficient damages to state a claim and stating a claim does not guarantee sufficient injury in fact to establish Article III standing.

**Federal Banking Regulators Make Sweeping Cybersecurity Proposal for Large Banks and Related Critical Institutions**

The Federal Reserve, Office of the Comptroller of the Currency and the Federal Deposit Insurance Corporation issued a joint advanced notice of proposed rule-making (ANPR) requesting comments on a sweeping set of cybersecurity rules for the nation’s largest banks, as well as certain critical service providers. The ANPR does not propose specific rules, but is rather a discussion of the types of rules the agencies are considering, and an invitation for comments on specific aspects of those rules. As described in the ANPR, these rules would impose specific cybersecurity governance and operational procedural requirements on these institutions, which would be intended to ensure continuity of the U.S. financial system in the event of a cyberattack.

Overall, the agencies are considering applying the new rules to entities with total consolidated assets of $50 billion or more — as well as certain of their service providers — based on the risk an attack on these institutions would pose to the institutions themselves, other financial institutions and the U.S. financial sector overall. Each agency would apply the rules to entities within its own jurisdiction, and to those entities’ service providers.

Furthermore, because an attack on one part of a financial institution could affect other parts, the rules would apply on an enterprisewide basis.

**Needs to Address**

The ANPR’s proposed rules would require covered entities to meet enhanced cyber risk management standards, which would focus on their need to:

- demonstrate effective cyber risk governance;
- continuously monitor and manage their cyber risk within the risk appetite and tolerance levels approved by their boards of directors;
- establish and implement strategies for cyber resilience and business continuity in the event of a disruption;
- establish protocols for secure, immutable, transferable storage of critical records;
- maintain continuing situational awareness of their operational status and cybersecurity posture on an enterprisewide basis; and

- (for “sector-critical systems” only) substantially mitigate the risk of a disruption due to a cyber event to their sector-critical systems.

---

6 The text of the ANPR is available [here](#).

---

9 Skadden, Arps, Slate, Meagher & Flom LLP and Affiliates
Five Categories of Standards
The standards proposed in the ANPR are organized into five general categories, and the ANPR goes into substantial detail (with specific questions) on each. We have summarized the key elements of the standards below.

1. Cyberrisk Governance
The ANPR describes a key aspect of cyberrisk governance as developing and maintaining a formal cyberrisk management strategy that is integrated into the overall strategic plans and risk governance structures of covered entities, as well as a supporting framework of policies and procedures to implement the strategy.

As part of this governance process, the agencies are considering a number of requirements, including the following:
- the covered entity’s board of directors must approve the overall strategy and hold senior management responsible for implementing policies consistent with the strategy;
- the entity must establish its cyberrisk tolerances to be consistent with the entity’s overall risk appetite and strategy, and manage risk appropriately;
- the entity must identify and assess cyberrisks;
- the entity’s board of directors must have adequate expertise in cybersecurity, or maintain access to resources or staff with such expertise, so it can provide a credible challenge to management on these issues;
- senior leaders with responsibility for cyberrisk oversight must have direct, independent access to the board and must independently inform the board of cyberrisk exposures;
- the entity must implement enterprisewide reporting structures and expectations for risk management; and
- the entity must include in its risk management framework mechanisms for identifying and responding to cyber incidents.

2. Cyberrisk Management
Having established overall risk strategies and tolerances, the ANPR describes specific proposals the agencies are considering for implementing, managing and monitoring these strategies, broken down into three separate functions: business units, independent risk management and audit.

Business Units. As described in the ANPR, business units would be responsible for assessing, on an ongoing basis, the cyberrisks associated with their activities and all of their assets (including workforce, data, technology and facilities) and report those risks to senior management. In addition, business units would have to comply with policies and procedures necessary to adhere to the entity’s overall risk management framework. In order to fulfill these duties, the business units should maintain — or have access to — resources and staff with the skill sets needed to assess and address cyberrisks.

Independent Risk Management. The ANPR suggests that covered entities would have to integrate cyberrisk management into their overall independent risk management function. This function would report to the entity’s chief risk officer and board of directors regarding implementation of the entity’s risk management framework throughout the organization. Risk management would analyze cyberrisk at the enterprise level and report to the CEO and board of directors if its assessment of cyberrisk differed from that of the business units. In addition, the ANPR suggests that companies may have to, at a holding company level, quantitatively measure the completeness, effectiveness and timeliness with which they reduce their aggregate cyberrisk and report this analysis to the appropriate level. (One of the questions on which the ANPR seeks input is how to develop a methodology to quantitatively measure these factors.)

In order to achieve these goals, the risk management function must have the appropriate independence, stature, authority, resources and board access to ensure that the entity’s operations are consistent with its cyberrisk framework.

Audit. Finally, the ANPR proposes that cyberrisk be added to an entity’s existing audit function. Entities should incorporate an assessment of cyberrisk management into their overall audit plan. This plan should include risk assessments of the entire security lifecycle, including penetration testing and vulnerability assessments as appropriate based on the entity’s size and complexity.

3. Internal Dependency Management
The ANPR explains the agencies’ proposals for entities to assess and manage the cyberrisks associated with their internal assets (such as their workforce, data, technology and facilities) throughout their lifecycles. These risks would include, for example, insider threats, data transmission errors and the use of legacy systems acquired through a merger. The agencies would expect entities to continuously assess and improve their effectiveness in mitigating these risks on an enterprise-wide basis.

As part of the standards in this area, the ANPR suggests a number of requirements, including requiring entities to:
- have current and complete awareness of all internal assets and business functions, including an inventory of all business assets that is prioritized based on their criticality to the business function they support, the entity’s mission and the financial sector;
- map the interconnections between these assets so as to understand how events impacting some assets could affect others;
- have controls in place to address the cyberrisks posed by their internal assets; and
- periodically conduct tests of back-ups to business assets to achieve resilience.

4. External Dependency Management

Parallel to assessing an entity’s internal dependencies, the ANPR also describes how the agencies believe entities should manage risk associated with external dependencies. These external dependencies include, for example, vendors, suppliers, customers, utilities and other external organizations and service providers which the entities depend on, or that interact with important systems. Entities should identify these dependencies and understand the interconnections between the entity and these external parties.

As part of the external dependency management strategy, the agencies are considering requiring entities to establish effective policies, plans and procedures to identify and manage, in real time, the cyberrisks associated with these external dependencies, especially those that connect to sector-critical systems and operations.

As with the internal dependency management, the agencies make a number of proposals for standards in this area, including requiring entities to:
- maintain current, accurate and complete awareness of all external dependencies, and prioritize them based on their criticality to the business function they support, the entity’s mission and the financial sector;
- map these dependencies and business functions, and be aware of how these external dependencies connect with each other; and
- review and analyze the risks associated with these external relationships, and periodically test alternative solutions in case an external partner fails to perform as expected.

5. Incident Response, Cyber Resilience and Situational Awareness

Standards within the incident response, cyber resilience and situational awareness category would be designed to ensure that entities plan for, respond to, contain and rapidly recover from disruptions caused by cyber incidents. The ANPR describes a number of specific proposed requirements in this area, including:
- entities must maintain situational awareness of changes in the operating environment so that they can reliably predict, analyze and respond to those changes;
- entities must have in place cyber resilience and incident response programs that include escalation procedures, containment procedures and communications strategies;
- the entity’s cyber resilience and incident response program must include feedback processes to enable lessons learned in one attack to be applied back to the programs for the future;
- entities must establish protocols for secure, immutable offline storage of critical records, including daily transaction information, in order to preserve critical records in the event of a cyberattack; and
- entities must have plans in place to transition business to another entity or service provider within prescribed time-frames, in order to preserve critical records in the event of a cyberattack.

Higher Standards for Sector-Critical Systems

The ANPR suggests that different standards might apply to “sector-critical systems.” While asking for guidance on how to define such systems more specifically, the agencies describe these as “systems of covered entities that are critical to the functioning of the financial sector,” suggesting that entities will have a mix of sector-critical and other systems, and thus must have different policies for both.

Specifically, the ANPR proposes two specific requirements with respect to these sector-critical systems:
- entities should implement the “most effective, commercially available controls” to protect these systems from cyberrisks. This requirement suggests that entities and vendors may end up engaging in a rapid “race to the top” as security and other technologies improve.
- entities will have to design their processes to target a two-hour recovery time for these systems.

Interaction with Existing Policies and Guidance

The ANPR makes clear that the proposed rules are not intended to supersede existing policies and guidance applicable to these institutions. These existing policies and guidance include, for example:
- the Federal Financial Institutions Examination Council’s (FFIEC) “IT Handbooks,” which provide cybersecurity guidance for examiners reviewing financial institutions and their service providers;
- the Gramm-Leach-Bliley Act’s safeguarding requirements providing general requirements for financial institutions for cybersecurity practices related to customer financial data;
- the NIST’s Cybersecurity Framework, a voluntary framework for assessing and addressing cybersecurity risks across many industry sectors; and
- the FFIEC’s Cybersecurity Assessment Tool, a voluntary self-assessment tool.

Rather than supplant these existing regimes, the new rules, as envisioned by the agencies, would supplement them by thus imposing higher standards on the largest institutions and the critical service providers.

**Key Takeaways and Next Steps**

Although the ANPR is not a specific proposal for cybersecurity rules, it clearly reflects the issues of concern to these three key federal regulators and what they see as best practices to address them. These rules, if enacted, would reflect the first set of specific enterprise-wide requirements imposed by federal regulators on cybersecurity matters. This move follows closely on the heels of the New York Department of Financial Services’ proposed cybersecurity rules for the financial sector, suggesting a growing trend towards greater specificity on cybersecurity matters.7

Answers to the ANPR’s questions are due January 17, 2017, suggesting that any specific policy proposals from these agencies will not be released until sometime later that year. We will closely monitor these developments and provide updates in this newsletter as the situation evolves.

**European High Court Rules that IP Addresses Can Be ‘Personal Data’**

The European Court of Justice has ruled that dynamic IP addresses can be “personal data” under the EU Data Protection Directive, even if the person storing the IP address does not have the information necessary to associate that data with a particular data subject.

On October 19, 2016, Europe’s highest court, the European Court of Justice (ECJ), ruled that dynamic IP addresses can qualify as “personal data” under the EU Data Protection Directive, even if additional information from other data sources was required to identify the individual associated with such IP addresses. The decision in Breyer v. Federal Republic of Germany confirms what many pundits had asserted: that dynamic IP addresses were covered under the directive. While at least some IP addresses already were going to be deemed personal data under the new General Data Protection Regulation (GDPR) going into effect in 2018, the court’s decision will have an immediate and significant impact on website and other internet service operators as well as on pseudonymization practices, and it suggests that the GDPR will be interpreted to apply to dynamic IP addresses as well.8

**Static Versus Dynamic IP Addresses**

The EU Data Protection Directive defines “personal data” as “any information relating to an identified or identifiable natural person.” Static IP addresses — those that remain constant over time — were long believed to constitute personal data because they could be used to consistently identify a specific machine connected to the internet, and thus the user of that machine. With respect to dynamic IP addresses — which change every time the user reconnects to the internet — there was more ambiguity. While parties (such as internet service providers) held enough information to associate a specific dynamic IP address with a specific user at a specific time, many believed that if a party only held the IP address and did not have the other data necessary to associate that IP address with an individual, the IP address was not personal data under EU law.

**Background of the Case**

Patrick Breyer, a German privacy activist and member of Germany’s Pirate Party, sought to stop the German government from registering and storing his dynamic IP address when he visited its web pages, claiming that such practices were a violation of data protection laws. Many websites operated by the German government store certain visitors’ information, including IP addresses, search terms and access dates for purposes of preventing cyberattacks and identifying attackers.

Breyer argued that his IP address should be treated as personal data under the EU Data Protection Directive, which applies special protections to such information and which would prevent the German government from storing such IP addresses. The German government argued that dynamic IP addresses could not be considered personal data because an individual could not be identified by an IP address without obtaining additional information from a third party, such as the individual’s internet service

---

7 For a discussion of the New York Department of Financial Services proposal, see our September 15, 2016, supplement to the monthly Privacy & Cybersecurity Update, available here.

8 A copy of the decision is available here.
provider. The case was referred by the German federal court to the ECJ to settle that question.

ECJ Ruling
The ECJ ruled that data may be deemed “identifiable” even if such information alone is not sufficient to identify the individual and additional means are required to do so. If a website operator could employ legal means, such as a request from a governmental authority, to require the internet service provider to provide additional information that could then be used together with the dynamic IP address to identify the individual, then the IP address in question should be considered personal data.

Effect of Ruling
The ECJ’s ruling effectively broadens the definition of personal data used in the EU Data Protection Directive. Websites and other internet-enabled service operators routinely collect IP addresses from users, so now they will have to consider how they must reform their activities to comply with the Data Protection Directive’s limits on the collection, use and storage of this data.

The ruling also may impact the scope of the GDPR, which goes into effect in May 2018. The GDPR generally uses a similar definition of personal data to that used in the Data Protection Directive, but expressly includes “online identifiers,” a term that is generally believed to at least include static IP addresses. There was some question, however, whether dynamic IP addresses were within GDPR’s scope, for the same reason as there was doubt under the directive. The ECJ’s ruling with respect to the directive suggests it will apply the same standard under the GDPR.

Finally, the Breyer decision may also have implications for the practice of pseudonymization of personal data, which the GDPR suggests as a means to ensure data security and the lawfulness of data processing, or to enable research. The GDPR defines pseudonymization as “the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.” The information held by the internet service provider in Breyer was kept separate from the website operator’s information and was subject to technical and organizational measures to defeat attribution. These measures were seemingly in compliance with the GDPR definition but was nevertheless held to identify the individual in question. The ECJ’s decision suggests that such pseudonymization will not be sufficient to escape the scope of the law’s personal data definition.

Future Remains Uncertain
It remains to be seen whether the ECJ will take the same view under GDPR as it did under the Data Protection Directive, though it seems likely. The GDPR has not yet gone into effect, so there have yet been no cases posing the question. In the meantime, website operators will need to carefully examine their practices with respect to the collection and use of dynamic IP addresses now that those practices are more clearly subject to the directive.

G7 Cybersecurity Risk Experts Establish Framework Outlining Eight Elements of Cybersecurity for the Financial Sector

The G7 Cyber Expert Group has announced a framework to help public and private financial entities address cyberrisks. The framework adds to a growing body of recent guidance and proposed regulation in this area.

On October 11, 2016, the G7 Cyber Expert Group, comprised of representatives from the United States, Canada, France, Germany, Italy, Japan and the United Kingdom, announced a voluntary framework to help financial institutions address cyberrisks. The G7 framework comes amid moves by U.S. state regulators (such as New York’s Department of Financial Services)9 and federal regulators (such as the recent announcement by the Federal Reserve, FDIC and Office of the Comptroller of the Currency)10 to address cyberrisk issues, and reflects policymakers’ growing emphasis on cyber as a key issue to be addressed.

The G7 framework identifies eight elements as critical to assess and confront cyberrisks, and is intended to provide high-level guidance to help public and private financial entities address risks based on their risk profile and other binding legal and regulatory requirements. They also are intended to allow entities to engage in an evolving process of risk assessment and to encourage re-evaluation of responses, strategy and policies.

The eight elements identified in the G7 framework are set forth below. Each describes a specific action that public and private financial entities should take:

9For a discussion of the New York Department of Financial Services proposal, see our September 15, 2016, supplement to the monthly Privacy & Cybersecurity Update, available here.
10The Federal Reserve, FDIC and Office of the Comptroller of the Currency announcement is discussed elsewhere in this issue.
- Element 1 – Cybersecurity Strategy and Framework: Implement a cybersecurity strategy that is tailored to the entity’s risk profile and is informed by international, national and industry standards and guidelines;

- Element 2 – Governance: Establish defined roles for personnel overseeing the cybersecurity strategy to foster accountability and communication, as well as to help establish proper resource allocation and access to decision-makers;

- Element 3 – Risk and Control Assessment: Evaluate the cyberrisks and the entity’s existing controls to protect against such risk, as well as prioritizing the importance of the risk and identifying any relationships between the various risks;

- Element 4 – Monitoring: Establish a monitoring process that can detect cyber incidents and evaluate the effectiveness of the system quickly and on an ongoing basis. Such monitoring can be enhanced if it is performed by individuals who are independent from those personnel responsible for managing the cybersecurity program;

- Element 5 – Response: Implement incident response policies to allow the entity to timely assess a cyber incident, contain it, notify stakeholders and coordinate any joint response.

- Element 6 – Recovery: Achieve operational stability after a cyber incident and focus on returning critical economic and other functions while allowing for continued remediation.

- Element 7 – Information Sharing: Gather and share reliable cybersecurity information with internal and external stakeholders, both inside and outside of the financial sector, to increase the breadth of understanding of cyberrisks and ability of all entities to respond to such risks.

- Element 8 – Continuous Learning: Review and revise the cybersecurity framework regularly in order to identify and solve any issues, as well as to incorporate any lessons learned from any incidents.

The framework itself does not create any binding obligations. It simply sets forth guiding principles that financial institutions should take into account when establishing their cybersecurity framework and programs. Despite the high-level nature of the elements set forth in the framework, it is clear that companies need to thoroughly assess their own risk profile and cybersecurity preparedness on an individual basis in order to bolster the security of the international financial system.

---

**Federal Regulators Issue Guidance on Use of Cloud Computing Under HIPAA; Cloud Service Providers are Deemed ‘Business Associates’**

On October 6, 2016, the U.S. Department of Health and Human Services (HHS) issued new guidance on how to use cloud computing technology and also comply with HIPAA obligations relating to privacy, security and breach notification. The guidance made it clear that the use of cloud service providers (CSPs) is permissible under HIPAA, provided that certain conditions are met. Specifically, the guidance clarifies that CSPs are considered “business associates” under HIPAA, even if the CSPs only have access to encrypted health information (and not the decryption key). The guidance also specifies that CSPs subcontracted by business associates also would be deemed to be business associates for the purposes of HIPAA.

**HIPAA and Business Associates**

HIPAA’s regulations apply to health plans, health care providers and other entities that are involved in the health service industry, as well as business associates that perform services for those entities. Among its many requirements, HIPAA includes specific obligations with respect to the collection and use of protected health information (PHI). Business associates must enter into business associate agreements (BAAs) with the applicable covered entity, which set out the permitted uses and disclosures of PHI and contractually obligate the business associate to appropriately safeguard any PHI.

**Application to Cloud Service Providers**

Under the new HHS guidance, CSPs that provide services to covered entities (or to other business associates) are business associates under HIPAA. As business associates, the CSPs, in conjunction with the covered entities, must conduct risk analyses to identify particular threats and vulnerabilities to the confidentiality, integrity and availability of PHI passing through
their systems. According to the guidance, these risk assessments should include a review of the nature and structure of the cloud services being provided, such as whether the services are private or public cloud offerings.

In addition to their contractual obligations under the BAA, as a business associate CSPs must also comply with specific requirements of HIPAA. These include: (1) implementing appropriate internal controls to limit access to information systems that maintain PHI under the HIPAA Security Rule in order to protect the availability, confidentiality and integrity of the PHI; (2) only using the PHI as permitted by the HIPAA Privacy Rule; and (3) appropriately notifying customers of any breaches of PHI as required by HIPAA. These obligations apply even where a CSP only has access to encrypted PHI and does not have the ability to decrypt such information. However, if the information has been “de-identified” in accordance with the HIPAA Privacy Rule (which requires the removal of various types of information) then the CSP would not be deemed a business associate, and the associated restrictions and requirements would not apply.

Key Takeaways

In light of the new HHS guidance, HIPAA-regulated entities should reassess their use of cloud-based services and enter into BAAs where appropriate. CSPs also should ensure compliance with HIPAA in all circumstances where they are processing PHI. In addition, HIPAA-regulated entities and business associates (including CSPs) should ensure that they are appropriately conducting risk analyses and risk management in order to identify and manage risks associated with the use of cloud services.

New Study Indicates that Consumers May Not Benefit From More Cybersecurity Awareness

A NIST study suggests that efforts to give consumers more information and control over their security profile is driving consumers to engage in poor security practices. The study may push policymakers to fundamentally reform their approach to security matters.

A recent study from NIST suggests that a consistent thread in privacy and cybersecurity laws and guidance may be having the opposite effect than what was intended. The study, which was published in the September-October 2016 edition of the trade publication “IT Professional,” found that the push to provide consumers with more information on security risks and impose rigid security requirements actually drives consumers to engage in poor security practices rather than improve their habits. Coming from such an influential source as NIST, these results may drive policymakers to fundamentally rethink how they require companies to communicate with consumers on security issues.

Security Fatigue

According to NIST, the study found that a majority of ordinary computer users experience decision fatigue regarding online security. The individuals in the study ranged in age from 20 to 60, worked in a variety of jobs, and lived in urban, suburban and rural areas. The interviewers asked participants about their professional and personal computer habits and their use of computer security, security terminology, security icons and tools.

In the interviews, many participants expressed feeling bombarded by the breadth of security protocols involved in their daily computer use, such as software updates and requirements to change passwords. Instead of facilitating safe online behavior, these initiatives have led to feelings of hopelessness, risk minimization and decision avoidance, behaviors NIST calls “security fatigue.” The study found that warnings to stay alert and adopt safe online behavior overwhelmed the majority of typical consumer users. As a result, users avoided making decisions or based their decisions on immediate motivations and failed to follow security guidelines. Most subjects expressed frustration with understanding the complexity of various privacy policies and trying to remember different usernames and passwords, as well as needing to gain access to their personal accounts through additional security measures.

Assessing and Minimizing Risk

In addition to feelings of information and warning overload, interviewees also doubted that they would be the target of a cyberattack. Many participants felt they were not high-profile enough for someone to want to steal their information, stating they did not work for the government or a financial company. They also noted that they did not personally know anyone who had been the subject of a cyberattack.

Some participants also were skeptical of their ability to protect themselves online, referencing the fact that large corporations had expended tremendous sums of money on security and still suffered from computer hacks. Others felt it was the responsibility of larger companies, whether it be banks or online stores, to protect consumer data. These perceptions contribute to users’ decisions as to whether to incorporate or disregard recommended security practices.
Moving Forward

NIST plans to interview employees in the technology field to assess their perceptions and thought processes compared to ordinary users. They will interview individuals with a range of responsibility, including cybersecurity professionals and midlevel employees with duties to protect personally identifiable information.

Key Takeaways

Cybersecurity risks are spreading as more users store sensitive information online through online banking, healthcare portals and other services. The NIST study suggests that to encourage users to adopt safe online habits and make informed decisions, service providers should limit the volume of decisions users need to make, streamline the process for choosing the right security action and create opportunities for consistent decision making.

NIST has historically been a key policy influencer in the U.S. government’s efforts to provide guidance on cybersecurity. As a result, the NIST study’s conclusions that current practices have been counterproductive are likely to carry significant weight. As policymakers continue to examine best practices for protecting consumer privacy and security, they are likely to take NIST’s findings into account and may fundamentally rethink their strategies on these issues.
Cyrus Amir-Mokri

My introduction to cybersecurity took place while I was in government, serving at Treasury as assistant secretary for financial institutions. In my time there, cybersecurity became a significant operational risk, and it was important to create a robust information-sharing and technical assistance program, sponsored by the government, to assist the financial institutions. We took a “whole of government” approach to coordinate the work of Treasury with Homeland Security and the law enforcement intelligence community.

My involvement in cybersecurity on the government side continued through the end of my tenure at Treasury in April 2014. Since rejoining Skadden, I’ve been fortunate to work with people like Stuart, Lisa and Mike to further develop Skadden’s cybersecurity practice.

Lisa Gilford

Since I’m in Los Angeles, my practice has a particular emphasis on class actions in California arising under state consumer laws and statutes. Historically, I represented a number of telecommunications companies and litigated cases arising under the Telephone Consumer Protection Act and the California Invasion of Privacy Act. Over time, that has morphed into the cybersecurity area, as cases now tend to focus on data loss from security breaches.

California continues to be a hot jurisdiction for these types of matters, so I’m increasingly called upon to help clients assess litigation risk arising from the statutes and from cybersecurity threats. I’ve also had a number of cybersecurity issues arise in the context of large-scale product litigation, where information exchanged securely in the litigation is stolen. I’ve been working on how to retrieve that information and keep it more secure.

Stuart Levi

My work in cybersecurity originated through Skadden’s privacy practice, which dates back to the first dot-com boom. Companies were starting to wrestle with a number of issues involving the unprecedented amounts of data they were collecting online, including what they were allowed to do with it, what their privacy policies should say and their ability to move data around the world. U.S. companies also were struggling with how to run a global business when certain countries and regions, particularly the EU, had far more stringent privacy regimes.

Over the last few years we have added a robust cybersecurity practice. It started with clients who experienced inadvertent data loss, such as data that was accidentally sent by their vendor to another customer. Then they began to experience actual cyberattacks, such as data breaches and denial-of-service attacks. Today, there’s a steady drumbeat of these issues.

Michael Scudder

I first began to work in cybersecurity on the policy side, when I served as the general counsel of the National Security Council in the George W. Bush administration. There were the beginnings of a heightened focus and policy initiatives in the cyber area at that time.

When I joined Skadden in 2009, I wanted cybersecurity to be part of my practice, though not to the exclusion of other areas. I focus on the law enforcement and government-interfacing side of cyber matters. I was a federal prosecutor in the Southern District of New York before working in Washington and have a lot of experience interfacing with the law enforcement community. I still have all of my security clearances from working for President Bush, and I’ve had a number of matters where I’ve worked in the classified space for clients.
Lawdragon recently had the opportunity to talk to some of the top minds in cybersecurity at Skadden. The four lawyers reflect the range of practitioners addressing one of today's most pressing topics: threats to vast computer networks and repositories of digital information with the potential to significantly impact enterprises of all sizes and across all industries.

**Lawdragon:** Let's start by looking at some of the trends you see in cybersecurity today.

**Amir-Mokri:** In terms of where the threat is coming from, the trend over the last year or two has been that cyberattacks are perpetrated by either state actors or their proxies, or criminal gangs that may or may not be related to proxies of state actors. In many ways, we deal with a very murky world, but the reality is that attempted intrusions occur all the time.

I was speaking to a chief risk officer at a major financial institution about a year and a half ago. He said they were facing about 5,000 to 6,000 attempted intrusions each day. That may not be 5,000 or 6,000 different people, but it's still a staggering amount of attempts to get in.

What intruders want to do once they do get in is a different issue: anything from simple spying to exfiltration of data to compromise of data. What people worry about most is destruction, irretrievable destruction — we haven't seen a heck of a lot of that yet, but it's something to watch for.

**Levi:** Another trend, from a U.S. regulatory perspective, is that the Federal Trade Commission, using its authority under Section 5, has been increasingly aggressive in pursuing companies for cybersecurity violations. In some cases, they are going after businesses that have arguably misled consumers by overstating the cybersecurity protection they offer. Companies find this frustrating because there is no set standard. It's not like the FTC can pull out a document and say, “You are required to take seven steps. You took four. Clearly you misled consumers who would have thought you took all seven.” In the view of many companies, the FTC is making it up as they go along. It also can be troubling when the FTC goes after a company that has experienced a cybersecurity incident and asserts that the company has engaged in unfair practices. Again, without a set standard, it's difficult for companies to know what level of protection they must offer.

**Scudder:** There is a clear trend of companies properly viewing cyber risk as an enterprise risk — one requiring the attention of not just IT departments but also executive suites and boardrooms. While the right risk management recipe differs from company to company, companies continue to crave the identification of best practices. The challenge, of course, is that best practices in the cybersecurity area evolve as fast as they are identified, making the management of cyber risk all the more difficult. One key to staying ahead is developing the most complete understanding possible of the threats facing an organization. On this front, we'll continue to see many companies more proactively foster relationships with law enforcement and, in many instances, the intelligence community all in an effort to enhance the government’s sharing of relevant cyber threat information affecting industry. The trend of enhanced and more robust public-private partnerships, in other words, is one I see continuing with increased energy.

**LD:** There's a murkiness that is now affecting every company and government, and individuals as well, and regulatory agencies are racing to keep up. There are no evolved standards. Lawyering on cybersecurity issues must be fascinating because you're working with and creating law constantly.
LEVI: That’s right. Every company is vulnerable to attack, regardless of whether they are a financial service institution or a manufacturing business or a professional services firm. All too often, companies think that if they don’t have consumers’ personal information, their risk is low. They forget about theft of confidential business information, denial-of-service attacks and other cyber incidents that might impact them. These attacks are not limited to large companies. Clients of every size and in every industry are getting hit.

GILFORD: One of the major trends I see, and this is probably not a surprise given my background as a product liability lawyer, is the convergence of cybersecurity and product liability law. There are so many devices and products that are now connected to the Internet that are not computers or storage devices, and they’re involved in cybersecurity cases and regulation because of their susceptibility to hacking.

There was a recent case against a number of hotels because someone demonstrated how easy it is to engineer access through key cards to rooms. The automobile industry has been hit with a class action regarding the vulnerability of electronic control systems on cars to hacking. We will see plaintiffs’ lawyers try increasingly to make hackability the equivalent to liability. It will hit industries we hadn’t previously viewed as being subject to cybersecurity threats and issues.

AMIR-MOKRI: Another trend is various regulatory agencies coming out either with sets of cybersecurity expectations or guidelines. That’s beyond what’s going on in terms of attacks and attack vectors and actors. The independent federal agencies and self-regulatory organizations like FINRA (the Financial Industry Regulatory Authority) and others have been issuing guidelines of expected conduct, though none are necessarily raised to the level of hard-and-fast regulatory requirements by which conduct would be assessed.

There’s one partial exception — the SEC’s Regulation SCI (Systems Compliance and Integrity), which is really a systems-integrity regulation that goes beyond cybersecurity. With the 2014 release of the Department of Commerce’s “Framework for Improving Critical Infrastructure Cybersecurity” and follow-up by various regulatory agencies, people are beginning to get a sense of what the expectations are around governance, cyber hygiene, participation in information-sharing mechanisms and crisis management when an event occurs. That includes communication with government agencies.

The financial sector is probably further along than many other sectors in this respect. I think the Department of Commerce’s publication is a trendsetter. What remains to be seen is whether adherence to these practices will serve as defenses to claims of liability. Certainly, in a world where conduct is measured by due care or other such standards, these evolving guidelines and pronouncements by regulatory agencies are going to play a role.

LD: It also looks as though the product liability and class action bars have unlimited potential to create a new cause of action against companies — whether it’s security class actions or product liability — with data as the resource, and lack of disclosure of the risks in their management of that resource. Perhaps you could offer some insight on the scale of what you see regarding the growth of claims in that area.

GILFORD: The FTC recently came out with guidelines on the responsibilities of companies that have products connected to the Internet and may be susceptible to breaches. That created a playbook for plaintiffs’ lawyers, and I’ve seen the plaintiffs’
As the regulatory environment is a combination of all the issues, it really does create a "who to sue next" for the plaintiffs' bar.

LEVI: The interesting counterbalance is that, for the most part, the plaintiffs' bar has not been particularly successful in these cases. A big reason is that they've had tremendous difficulty establishing "standing" to bring lawsuits, since consumers are generally not injured by these attacks.

For example, in the Target breach, which many consider to be among the worst data breaches in the last few years, very few consumers were impacted financially. Despite all the fear and concern, consumers didn't suffer identity theft, and while many experienced fraudulent charges, these typically got wiped off their accounts.

Now, when they want to bring a class action suit against Target, they are presented with the very real and difficult challenge of showing the court how they were injured. Plaintiffs have tried a variety of approaches to overcome this hurdle, but with only limited success. For example, they might assert that they are concerned about the possibility of future identity theft. This "what if" argument is difficult to sustain, although the Seventh Circuit was recently persuaded by it. In other cases, consumers might argue that they were injured because they spent money on identity theft protection, but many companies now offer that service for free after a data breach.

The net result is that, even in data breaches impacting millions of people, class action lawyers are finding limited financial damage. This means that these cases are settling for relatively low amounts, which might make them unattractive to plaintiffs' lawyers as time goes on. It's not as lucrative as I think they were hoping when this wave of data breaches first hit. It will be interesting to see if interest in data breach class actions wanes over time.

GILFORD: As the regulatory environment changes and the statutory basis for certain claims changes, the courts are adopting a broader view of what constitutes standing or the right to sue and what may constitute damage.

As this evolves, you may see plaintiffs' lawyers getting some traction based on the regulatory environment and the theory that products aren't as safe as promised and are worth less than what the consumer believed them to be when they purchased them. This may morph and the idea of a security threat constituting some basis for liability may develop over time. While the plaintiffs' lawyers haven't been doing well in these cases so far, I'm not sure that's going to remain the case much longer.

Given this environment, our clients — no matter what industry they're in — would be wise to think about the way they're disclosing information about products and, frankly, the way they're designing them.

AMIR-MOKRI: The concept of loss and damage is important. When you think about some of the debit card/credit card theft situations, the fact is that the financial services industry has become very good at doing two things in this regard: Once a compromise has occurred, they shut down the affected accounts; and the second is fraud detection. Even before the consumer knows there's a breach, they detect unusual activity very well and they shut down the ability to transact.

Part of the loss minimization in these fact patterns is the result of the relevant entities and institutions already working on damage mitigation.

Lisa's point is very important — not just in the financial services industry, but also in other industries: People should think about what could possibly go wrong if there were a breach and ways to mitigate potential damage if something bad happens. Hopefully, the fact patterns will not be worse than what we've seen happen thus far in the financial services industry; even though there has been some loss, it has not been catastrophic.

LEVI: In addition to counseling companies in the midst of a data security incident, a significant piece of our practice is advising companies how to best prepare to deal with an attack on the enterprise-wide level. We also advise clients on how to find "smoking guns," such as badly worded statements or policies that were not followed that could be used against them in the event of litigation.

The biggest change in the environment is that clients are much more attuned to the need to be prepared. A year or 18 months ago, most of our clients would say, "Preparedness is interesting; it's probably something we should be thinking about at some point." Now, they are much more actively engaging and, in almost an urgent sort of way, wanting to do something about this.

LD: To what do you attribute this urgency for preparedness? Have some of the high-profile attacks raised client awareness? Or is it that the firm and others have effectively raised awareness that this is really something clients need to get front and center on? Is it government regulation? A variety of factors could have caused this to come to the fore.

AMIR-MOKRI: It's a combination of all of the above. The spectacular-type events tend to grab everyone's attention. Then the fallout is not just litigation in state or federal court but also congressional investigations, regulatory investigations, reputational risk.
Every journalist is going to be interested in what happened and how it happened. Senior managers who are concerned about the share performance of their company, if it’s a public company, or just the company’s reputation generally, are going to be focused on this if they aren’t already.

Over the past couple of years, senior management and boards have become particularly conscious of the cyber threat. President Obama’s executive order on this subject was issued in February 2013. Headline-grabbing incidents and regulators have made this more top of mind in the last couple of years. Directors and other participants have identified it as one of their top priorities.

Boards are wondering, “What exactly do we need to do? We have our governance structure put together. Now what should we worry about?” People are becoming a little more systematic in their thinking and a little more intent on getting it wherever they need it to be in order to be prepared.

SCUDDER: A lot of companies have realized they’re not exempt from the risk, that it’s not a risk that is only going to present itself in acute ways in particular industries. It’s not limited to retail, financial services or energy. We’re seeing a lot of companies that operate in industries where their intuition may tell them, “Sure, it’s a risk, but it’s one that’s manageable and not all that acute.” Then they’re surprised when they have an incident.

For example, a manufacturing company in the Midwest had a particular intrusion about accessing corporate funds, a big company that in complete good faith viewed cybersecurity as a secondary-level risk. A lot of those kinds of institutions are realizing that it’s an enterprise risk.

LEVI: You’ll see every so often — and Sony is the best example of this — an incident that shakes up an entire industry. That hack had a profound impact. It wasn’t that North Korea was the alleged perpetrator; it was that the attack happened within the entertainment world. These companies are traditionally focused on piracy of their creative works, but outside of their IT groups for the most part had not focused on broader issues of cybersecurity.

Now we see tremendous focus on cybersecurity by the entertainment industry. They realize how much personal information is floating around — very sensitive personal information that could have a profound reputational impact on a company if it were released. Every so often you’ll have an incident like the one involving Sony, which makes an industry suddenly hyperfocused on this issue.

LD: Is there a basic playbook for what you tell a company, a general counsel or a CEO they need to have in place from a defense perspective?

LEVI: We urge clients to have a cybersecurity incident response plan. We tell them it’s gone from a “nice to have” to a baseline requirement. Indeed, today, if you don’t have a plan, you are quickly becoming an outlier.

We provide clients with a template to help them think through the key issues. We also get involved in tabletop exercises and walk clients through different scenarios. This ranges from figuring out who should be sitting at the table and making decisions if a major attack occurs to what your legal obligations and responsibilities are.

I’ll give you an example of something that gives clients pause. We recommend that they diligence their third-party agreements to see if they’re obliged to disclose a cyberattack to business partners, vendors and customers. Inevitably the client says, “Oh, we don’t have time to do that now.” We tell them, “You can either do it now or in the midst of an attack when there are a lot of other things you’re worried about.” They realize they really do need to think about these issues and plan.

Clients that have an incident response plan and have tabletop tested it are much more adept at responding to an incident than those that spend the first 48 hours arguing internally over whose area this falls into, who’s making the decisions, who should be at the table and which stakeholders are involved. All those questions represent time that’s lost in an environment in which you need to move quickly, and it increases the chance of a misstep.

SCUDDER: There is no set playbook, but there are certain practices and resources companies need to have in place from a defense perspective. When we’re asked to evaluate incident response plans, we invariably find that the plans are too narrow because they fail to address scenarios that may in fact befall a company. Incident response needs to be viewed broadly —
companies need to consider not only operating continuity and information and system safeguarding, but also communications with consumers and other constituents as well as regulators and law enforcement. It’s often prudent to map out how communications will flow up the chain within a company during or in immediate response to an incident. This will help organizations avoid certain pitfalls, such as when a company puts together an incident response plan that is very U.S. resource-centric, and a serious intrusion occurs in Europe — basic things like different time zones can slow down a response and the mobilization of resources.

**LD:** Lisa, from a litigator’s perspective, is it fair to say you prefer to defend companies with an incident response plan?

**GILFORD:** That’s certainly fair to say. Companies find that when they have an adequate response in place, it goes a long way toward defeating claims and eliminating or minimizing damages. Companies are in much better stead defending against class actions if they have quick notification response plans when cyberattacks occur.

**LD:** Do you also recommend cyber insurance now?

**LEVI:** We have insurance lawyers at Skadden who’ve been advising clients fairly regularly on cyber insurance plans so they understand what’s covered and what’s not. Also, as companies have incidents, we review their policies and advise on whether they have a claim and how they should approach their insurance provider. That’s clearly a large and growing area.

**LD:** Is it your estimation that basically all companies need some level of cyber insurance?

**AMIR-MOKRI:** As good as your defenses are, the reality is that someone at some point is going to penetrate. The questions are, “What is the harm that is done and what is the damage that’s done?”

The issue with cyber insurance is that some insurance companies find it very difficult to price it because of the lack of experience. I imagine as the insurance industry builds a bank of experience, this will become easier. We have to wait and see.

**LD:** It sounds as though your advice broadly to clients is that they look at an incident not as a matter of if, but when. Two of the areas that we could untangle a bit are how you advise clients to prepare to address the incident publicly, and with the media, since it’s going to come out one way or the other, and what the obligations are in terms of public reporting, government notification and how you advise your clients to handle them.

**AMIR-MOKRI:** It’s important to think about what the incident response plan really does and how it fits into the damages scenario. The idea behind it is, once there is an incident, knowing how to mobilize everyone to do everything that needs to get done. Where it becomes very important is in mitigation.

If you have a plan, you can take action to cut off certain activities or operations to minimize the amount of damage that’s already going to be occurring. Those first 24, 48, 72 hours can make a huge difference because things happen so rapidly in information technology. If you find out immediately what’s going on and you’re able to shut it down, it could make a very, very substantial difference between something manageable and something that gets out of control.

A certain amount of damage will already be done. That’s the definition of an incident, but the importance of incident response plans is that they can sometimes mean the difference between catastrophic and not.

**LEVI:** A lot of our clients will get a PR agency involved with the media piece. After an attack, we look very carefully at clients’ communications. We urge them not to say things very definitively because they run the risk of painting themselves into a corner. These situations are much more in flux than even they realize. Statements need to be phrased very carefully.

**GILFORD:** It’s very important that a client’s incident response plan take into account jurisdiction-specific rules that guide data breach notification requirements. The California Legislature, for example, has been very active in this area, and data breach notification rules in the state seem to be amended on a yearly basis. It’s critical that incident response plans be kept up to date. In terms of broader notification of an incident to the public through the media, as Stuart mentioned, litigation is frequently on the horizon for a company that has experienced a breach, and careful vetting of media statements is crucial.

**SCUDDER:** Companies often have a very real and urgent need to communicate with their customer base. They’re inclined to plant their feet on facts before all the facts are out and they’re aware of the full scope of the incident, and before they’ve decided as an institution what measures they’re going to take to mitigate losses that may appear to exist in the initial phases. So often, clients say, “We have to go in this particular direction” before they’ve got their arms around the situation. We’ve even seen it before the incident is complete.

As far as the government goes, most companies in regulated industries will want to think through whether to self-report the incident to the regulatory authority that has jurisdiction over them. They’ll also want to consider reporting the incident to law enforcement.

We don’t advise clients to reflexively report or not report an incident. Sometimes that surprises people. There are a lot of occasions in which you would choose to report an incident to law enforcement in the very earliest phases. There are other times when you may not. You’ve got to run through a calculus about what is in the company’s best interest at a particular point in time. You can always defer reporting. You can always choose to not report it and allow the government to come to you, and hope things work out fine. So much depends on your capacity to deal with law enforcement at a particular moment in time and what information you feel comfortable providing on a voluntary basis.

Often clients will say, “Why wouldn’t you just instantly pick up the phone and let the government know? How does that harm you?” It may set you back some operationally.

**AMIR-MOKRI:** It’s a complicated question. You have many different stakeholders. Before reaching out, you have to think about the nature and quality of the information you have and assess what that information
really means, how certain it is, how helpful it is and what its implications are.

There are certain statutes to follow. For example, security-breach statutes create an obligation to self-report if customer information gets compromised. Hopefully Congress will act, and we’ll have a uniform standard across the board. At least that will bring certainty as to how people should act in these situations.

SCUDDER: That’s a really important point because a lot of institutions will be very reluctant to invite the FBI in, precisely because of their concern that the FBI is going to want to figuratively turn the place upside down — be disruptive and assign blame.

We had a client in the Midwest that had an intrusion resulting in the wire transfer of money out of the company. It was all wired to the individuals that perpetrated the hack itself. After talking to us, the company decided to get the FBI in there right away. The FBI actually knew exactly how the intrusion happened, where the vulnerability was in the company’s system. There are instances where the government can add value. That’s an essential part of the public-private partnership that you’ve heard the government talk so much about in the cyber area.

LD: Mike, when you’re talking about the “Do we or do we not self-report?” situation, what would be the reasons on the “don’t report” side of the table? Or to you, is it just a clear, “You need to get law enforcement in on this?”

SCUDDER: In the case of the intrusion at the Midwest company resulting in the wire transfer, the situation was one where we thought, on balance, that it should be reported. In other cases, it becomes a question of when. You have to look at how the incident occurred. There’s obviously a problem if somebody is able to infiltrate the system and send a fictitious email that results in a wire transfer going out of the company. You could say, “We need to figure out as an institution how it happened and put a plug in it because the moment we invite in law enforcement, they’ll only look at it from the standpoint of investigating a crime. We don’t have the bandwidth and capacity to simultaneously attend responsibly to law enforcement and deal with the technical decisions that obviously need to be made.”

The company in this particular situation thought they might benefit from the perspective of law enforcement because it looked like something this company would not have been the only one to experience. They turned out to be right.

LD: It strikes me that among the factors on the side of reporting is if you’re in a more regulated environment, like financial institutions, or if it is the kind of intrusion that has the potential to be more systemic or is the first in a series. For instance, with this company, Mike, where they arranged one transfer, if you hadn’t gotten on it early, there could have been more transfers.

SCUDDER: Exactly. Stuart and I were involved in a situation where there was a little more hesitancy in informing the government right away because the intrusion was so disruptive to company operations. In the early chapters of the incident, the company was much more focused on what was actually happening at the time and getting their arms around it.

LEVI: The incident Mike’s talking about also goes to the concern that the FBI would have the mindset, “While we’re here, let’s see
if there are any crimes you might have committed.” Also there was a fear that the FBI would walk in and say, “Everybody get up from your desks. We’re going to put agents at all the computers and start looking at everything you’re doing.” We tried to convince them that it wasn’t going to work that way.

The other hesitancy — which was interesting, and I think they’ll admit they were very wrong about this — came from it being a technology-intensive company. Their view was, “What could the FBI possibly tell us that our very smart technologists and internal cybersecurity people can’t figure out on their own?” After we convinced the client to inform the government, the FBI said, “We’ve seen this exact attack before. Here’s what they’re after. Here’s what’s going to happen next. Here’s their profile,” which of course the company’s guys couldn’t know. It’s not what they do for a living. They were surprised at the utility of the information and the breadth of knowledge the FBI and law enforcement can bring.

**LD:** It’s striking how narrow a company’s perspective can become when under attack — all the company can see is that it’s being attacked. One of the benefits of bringing in outside lawyers and, in appropriate circumstances, law enforcement, is to gain a more objective view — a longer lens than any individual company has on its own.

**AMIR-MOKRI:** That’s a very important point. That’s the perspective of government: to look at the system and at everyone, then say, “Eight other companies were affected by the same thing.” When you’re in a company, as much as you strive to be aware of what’s going on with others, you just don’t have the same vantage point.

**AMIR-MOKRI:** A lot of recent cases involve allegations of breach of fiduciary duty. Senior managers and boards of directors have to worry about the fiduciary duty of care, which is, “Are you conducting the affairs of the corporation in a reasonable way?” Boards are trying to think through a lot of issues in terms of how to set up a governance structure.

We also discuss whether a client’s primary focus is rapid response or preparedness. How do you conduct the day-to-day affairs of the corporation in a way that’s sensitive to information security needs? When should issues be escalated? What’s the chain of command? Who’s responsible? It’s important to tighten up all of the corporation’s governance and practices around those kinds of fundamental issues. Taking stock of information security is going to be an essential feature of the company’s operations.

When I was at Treasury, we worked with some of the trade associations on these questions. On one occasion, SIFMA (the Securities Industry and Financial Markets Association) took the lead in a simulation of what would happen to the market if there was a cyberattack on it and how market participants would react.

**LD:** That perspective is also critical, I would think, to the board of directors. You advise the CEO and the in-house lawyer and technology leaders, but you may also advise the board. What’s most important about your guidance in that area?

**AMIR-MOKRI:** A lot of recent cases
the guts of what’s going on, but the business people have to make the ultimate decision. Does the company continue functioning? If so, how does it function? What message has to be delivered? What are the big business decisions that have to be made?

Every company needs to be aware of these questions because the answers determine the design of their governance structure with regard to information security. Once a company has its governance structure set up, it needs to ask questions such as, “What specifically as a board member do I need to know about how we’re doing in terms of information security? What kinds of experts should we be consulting?” These are all evolving issues people are trying to understand better.

Information security is very technical and can get so complex. It’s imperative to be able to translate technical language into a medium that is readily understood by business decision-makers, to give them the knowledge they need to make good decisions.

**LD:** When you focus on what you report, does the board need to be notified of everything?

**LEVI:** That’s a great question and one clients ask us a lot. Not everything needs to be reported.

You don’t need to report run-of-the-mill incidents, such as a small attack that was thwarted. You should report the major reputational-impact-type attacks that could have a material impact on the company. You don’t want to call the board every time, but you should call them when an incident rises to a certain level of importance.

It’s a challenge. Even if you don’t tell the board immediately, you might discuss it at the next meeting. You might say, “Over the last quarter, we dealt with the following couple of issues. Here are the steps we’re taking to try to stop that from happening in the future.”

**LD:** Lisa, do you have a read on what the board should be told from the perspective of defending corporations in class actions? Is there a certain level of reporting to the board that is helpful or unhelpful?

**GILFORD:** I get involved when there are litigation updates that might be significant to report to boards. In terms of the initial breach and what risks may flow from it, including the risk of litigation, what Stuart and Cyrus have outlined is absolutely where the company needs to be. As they mentioned, it’s not a one-size-fits-all construct. It really does involve assessing the situation and getting a good sense of what rises to the level of board reporting and when to report it.

**LD:** If a company does self-report, is there a sense that that will result in enforcement agencies looking at it more favorably?

**AMIR-MOKRI:** As a general matter, many enforcement agencies say, “If you self-report, we will look more favorably because it shows that your compliance and other systems are working.” I don’t think anyone has made a particular pronouncement in the cyber area, but as a general rule self-reporting is better received than not.

In terms of self-reporting, there’s also a more general point to be made. I’m thinking about financial services, which is obviously my orientation. When you have a safety-and-soundness relationship with your regulator, there are two ways to view the relationship. One is adversarial, broadly speaking. The other is a partnership of sorts, where you’re trying to use the regulator to help you think through the situation and have an open line of communication to ensure the best results for the company and the system.

Each fact pattern is going to merit its own analysis. On balance, I consider sharing with your regulator a good idea. Again, you have to think about the specific situation, what the implications are, how significant the incident is and when the time is right. All those questions are very important.

**LD:** Shall we turn to the future? What is your sense in the near term about how much cybersecurity threats and this practice area are going to grow and in what ways — the predictable and some that folks might not foresee? And then, a bit further down the road, do you think cybersecurity is going to be an area that dominates litigation? Or is it something that will be managed and just one more area of corporate risk?

**LEVI:** It’s hard to say. A lot will depend on the regulatory/legislative point of view, what is enacted or not enacted. That could create a whole slew of new issues.

We’re advising a number of companies that have done virtually no work in this area or have done some but only skinned the surface. As cybersecurity issues and our clients’ businesses evolve, we’ll need to work with them to update their systems of policies, procedures and governance.

Some clients are more on top of cybersecurity issues than others, but then they say, “We did something in 2012 and haven’t really gone back to look at it.” They realize as they look at it now that none of it makes sense because they reorganized their business or their risk profile has changed.

**AMIR-MOKRI:** There are two, probably three, vectors to consider when thinking about what might happen in the future. One is, “What are the legal standards and what are the liability rules?” Stuart is exactly right. We have to wait and see how these develop, in court cases and statutes. Congress has been trying to pass a cyber bill since 2011. It’ll happen at some point and will provide more information as to what we should expect purely in terms of litigation liability. That’s one vector, and it will settle in the next couple of years.

Another is, “How will technology evolve?” This is one of those secular trends that we’re not going to stop. Information security is here to stay. If anything, as Lisa suggested earlier, it’s going to permeate more and more of our daily activities. The ways in which hacking or disturbances might occur and who could be liable for it may be spectacularly complex and unpredictable. Many people may be affected by it in the future in ways we can’t necessarily foresee today.

The third piece is, “How do businesses organize themselves?” You set yourself up one way today and you might be immune to certain kinds of attacks. To become more efficient tomorrow, you’re going to have to reorganize. Some national institutions are doing this. It used to be that their credit card business and their debit retail business and their commercial bank, for example, were all separate. Some of them are considering linking them up a bit more. Now they have to think about their IT environment a lot differently.
That’s true not just for financial institutions but for any company that wants to use technology to become more efficient. Once you organize yourself in a way to become more efficient, that usually results in different parts speaking to each other. You have to think about your information security architecture differently.

**Gilford:** Cyrus has perfectly organized the landscape. To expand a bit on the litigation front, litigation is a notoriously unwieldy and time-consuming way to work out policy issues. I don’t see that slowing down. As I predicted earlier, we may see a rise in cases at the convergence of product liability and cybersecurity as physical objects in our day-to-day lives are increasingly driven by connection to the Internet and are susceptible to hacking and security threats. I don’t see that slowing down. It will result in litigation that will take some time to work its way through the courts.

As I mentioned before, in California, we see an update or amendment to privacy statutes almost yearly that affects all companies doing business in the state. Our clients need to be aware of those changes. For example, California recently legislated the manner in which some companies that provide credit protection services to persons affected by a breach must go about providing those services. If that is something a company decides to do as part of a response plan, it should be aware of jurisdiction-specific requirements.

Those kinds of laws, their meaning and their scope are issues that will be litigated beyond any kind of harm to a particular plaintiff or set of consumers; cases will revolve only around the laws’ meaning and application to companies. Oftentimes, the parameters of those aspects of laws get worked out in the courts. It takes time to develop a body of law and an understanding about what the legislative environment is for companies.

The way companies organize themselves and design their products with an eye toward mitigating cybersecurity risks will be an expanding area of focus that will require input by lawyers and others knowledgeable about the legal risks in particular areas.

**LD:** Mike, what do you see in the future, particularly from your governmental purview?

**Scudder:** I would make a nonlegal point, which is implicit in what everyone is saying here. If I were sitting with a company, and they were looking into the future — knowing that cybersecurity risks exist today and will tomorrow — I would tell them to double down on their investment in security, both regarding product development and more broadly. Companies should focus on having the right skill set and capacity in their boardrooms and executive suites to deal with these risks, and they should recruit talent that’s able to manage this for their institutions going forward. You’ve got to stay a step ahead. That is the challenge.

**Amir-Mokri:** Cybersecurity issues cut across borders. As we think about legislation domestically in the United States, we also should consider working with a number of major international parties, and not just with our partners. I would include China in this broader group because they have a similar stake in maintaining a resilient Internet that is free of malicious attacks.

With information security and IT talent growing significantly in many different areas of the world, we shouldn’t assume that nonstate actors will be incapable, as they’ve already shown that they are capable, of causing serious damage. It’s incumbent on states that have an interest in the current world order — the U.S., Western Europe, China, Russia, India, etc. — to come up with protocols and ways to work with each other to manage this issue. Protecting cyberspace is our shared responsibility.