Skadden

Privacy & Cybersecurity Update

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*,[1] 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[2] 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[3] 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.

- 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 computer fraud provision of its 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 "@petrofacltd.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."

[4] No. 15-20499, 2016 WL 6090901 (5th Cir. Oct. 18, 2016).

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.

Return to Table of Contents

US Treasury's Federal Insurance Office Considers Big Data, Cyber Risk and Data Privacy in First Annual Report on the Protection of Insurance Consumers

Last month, the Federal Insurance Office of the U.S. Department of the Treasury released a first-of-its-kind "Report on Protection of Insurance Consumers and Access to Insurance," in which it weighed in on key consumer protection issues in the insurance industry, including the use of big data, cyber risk and data privacy.

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

[5] Available here.

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 emphasizes the need to close the regulatory gap with respect to big data vendors that provide pricing and rating tools to insurers, calling for state insurance regulators to exercise their authority over such vendors to prevent potential harm to consumers.

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.

Return to Table of Contents

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

Federal Communications Commission Chairman Tom Wheeler outlined a new regulatory program aimed at reducing the risk of cyberthreats posed by internet-of-things devices.

In a December 2, 2016, letter to Sen. Mark R. Warner, outgoing Federal Communications Commission (FCC) Chairman Tom Wheeler[6] confirmed that addressing internet-of-things (IoT) threats is an ongoing national imperative and such threats are being actively examined by the FCC. Chairman Wheeler further reiterated that concerns surrounding IoT threats and cybersecurity should not be delayed by the impending transition in Washington, D.C., however, he admitted that some immediate next steps have been postponed in light of the election.

Chairman Wheeler's letter was in response to Sen. Warner's October 25, 2016, letter, which raised concerns about the October 2016 Mirai botnet attack that led to the largest distributed denial of service (DDoS) attack recorded. By utilizing IoT devices such as cameras and digital video recorders (DVRs), attackers were able to temporarily disable internet sites including Twitter, Amazon, Tumblr, Reddit, Spotify and Netflix. In his letter, Sen. Warner, who co-founded the bipartisan Senate Cybersecurity Caucus and is the incoming vice chair of the Senate Intelligence Committee, questioned the role of private sector actors, such as internet service providers (ISPs), and the role of the FCC in regulating IoT 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

[6] Since releasing his letter, Chairman Wheeler has announced his resignation, which will take place on January 20, 2017.

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.

Return to Table of Contents

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.

Return to Table of Contents

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 / New York
212.735.4133
james.talbot@skadden.com

Joshua F. Gruenspecht
Associate / Washington, D.C.
202.371.7316
joshua.gruenspecht@skadden.com