Bloomberg Law

Privacy and Security Law Report®

Reproduced with permission from Privacy & Security Law Report, Privacy and Security Law Report 16 PVLR 1555, 12/04/2017. Copyright © 2017 by The Bureau of National Affairs, Inc. (800-372-1033) http://www.bna.com

Cybersecurity Regulation

Federal government agencies can and should lead in an effort to create strong public-private partnerships to confront growing cybersecurity threats and protect sensitive and valuable information by incentivizing innovative cybersecurity solutions rather than imposing 'check-the-box' requirements currently being promoted, the authors write.

Cybersecurity

The Government's Role in Promoting and Leading Effective Cybersecurity

BY MARK KROTOSKI AND MARTIN HIRSCHPRUNG

Mark Krotoski is a litigation partner in the privacy and cybersecurity and antitrust practice groups of Morgan, Lewis & Bockius LLP in Palo Alto, Calif. He previously served as the national coordinator of the Computer Hacking and Intellectual Property Program in the Criminal Division of the Department of Justice and as an instructor on foreign economic espionage and trade secret cases and other law enforcement issues at the DOJ National Advocacy Center.

Martin Hirschprung is an associate at Morgan, Lewis & Bockius LLP in New York and a member of the investment management and privacy and cybersecurity practice groups.

Introduction

Data breaches have the power to inflict significant damage and consequences with the potential to bring a company, industry or government agency to its knees, or adversely harm those individuals whose information was compromised. Both the government and the private sector share responsibility in adopting effective cybersecurity practices. Both have been the victims of recent high profile, major cyberattacks.

Fundamentally, effective cybersecurity requires a tailored approach, recognizing the role of flexibility and innovation. There is simply no ''one size fits all'' solution.

The government can do much to encourage effective cybersecurity. Alternatively, the government can impede this objective by mandating costly, cumbersome, and unnecessarily complex regulatory standards. Regrettably, the recent trend highlights the government's increasing proclivity to adopt costly, inconsistent and unnecessarily complex regulatory standards that divert limited resources from tailored cybersecurity solutions. Many organizations today confront over-regulation on cybersecurity matters from multiple enforcers at the international, federal, and state levels.

This article highlights several recent cyberattacks, discusses cooperation efforts between the government and private sectors, provides an overview of the current U.S. regulatory landscape and then identifies key factors that we believe the government should consider to streamline and reduce the burden of cybersecurity regulations while still promoting effective cybersecurity.

Recent Cyberattacks Cyber criminals run the gamut of nation-state actors, terrorist groups, criminal groups, and lone hackers. They seek to steal information such as classified or sensitive government documents, personal and financial information, trade secrets, and confidential or proprietary information, and passwords to bank accounts, and emails.

Consider a few recent significant cyberattacks on government agencies along with critical reports and current steps to address vulnerabilities:

- In 2015, the U.S. Office of Personnel Management announced that it had been the target of a data breach involving 21.5 million records, described by federal officials as among the largest breaches of government data in the history of the U.S. Information targeted in the breach extended beyond personally identifiable information such as Social Security numbers and included detailed security-clearance-related background information.
- Last month, the SEC issued a statement confirming that it suffered an intrusion in 2016 that provided unauthorized access to the EDGAR test filing system.
- In 2016, numerous government agencies were victims of cyberattacks, including the FBI, Department of Homeland Security, NASA, and the IRS.
- Recent Government Accountability Office (GAO) reports continue to note the need for government agencies to strengthen cybersecurity.
- On May 11, President Donald Trump signed an executive order titled ''Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure,'' which mandates a cyber policy review across critical infrastructure sectors (communications, defense industrial base, financial, information technology, electric, transportation, health care, and others), as well as a focus on the federal government securing its own systems.

Recent large-scale data breaches have also occurred in the private sector:

- In September of 2017, Equifax Inc. announced a cybersecurity breach that compromised the names, social security numbers, addresses, birth dates, and, in some cases, driver's licenses of approximately 143 million U.S. residents.
- Earlier this year, DOJ filed criminal hacking and economic espionage charges alleging that two Russian Federal Security Service officers conspired with others to obtain ''unauthorized access to Yahoo's systems to steal information from about at least 500 million Yahoo accounts.''
- In 2014, DOJ charged five Chinese military officials with committing computer hacking, economic espionage and other offenses on U.S. companies in the U.S. nuclear power, metals, and solar products industries.

Enhancing Public-Private Partnership Efforts The public and private sector reliance on technology and the internet is interdependent and directly affected by cyber threats domestically and abroad. Given this landscape, the question was framed by NSA Chief and Commander of the U.S. Cyber Command, Admiral Michael Rogers: ''The ultimate solution . . . is how do you bring this public-private partnership?''

The public and private sectors both stand to gain from working together on cybersecurity initiatives, as Professor Judith H. Germano has summarized. The private sector controls much of the critical infrastructure that is vulnerable to cyber-threats. Thus, many companies that own such infrastructure already have cybersecurity programs, giving them specific expertise and experience in dealing with potential threats. The public sector, conversely, is better positioned to investigate and prosecute cyber criminals. The source of a cyberattack is often difficult to identify, and government agencies are often better able to collect intelligence, collaborate with international law enforcement agencies, and gain access to critical information regarding potential threats.

An example of the collaborative approach is the NIST Cybersecurity Framework (NIST Framework). The NIST Framework is expressly based on an assessment of risk and designed to improve companies' technical, administrative, and physical protections to combat ever-changing cyber threats. Financial firms already have designed their cybersecurity programs to implement the NIST Framework and avail themselves of the Federal Financial Institutions Examination Council's Cybersecurity Assessment Tool and cybersecurity regulations under the Gramm-Leach-Bliley Act, which also adopt risk-based approaches.

The NIST Framework involved the participation of over 3,000 cybersecurity professionals from industry, academia, and government, representing the cybersecurity field's consensus on the most effective approach to improve cybersecurity. The NIST Framework establishes a voluntary and flexible framework that allows organizations to assess cyber risks and develop tailored responses. As of 2015, the framework is used by 30 percent of U.S. organizations. It is currently being updated based on feedback from industry groups, associations, nonprofits, government agencies, and international standards bodies as well as information NIST received from potential and current users.

The government has also sought to encourage information sharing about cyber threats. For example, the Cybersecurity Information Sharing Act (CISA) was enacted to make it easier for companies to share cyber threat information with the government and others. Although it does not require such information sharing, the Act creates a system for federal agencies to receive threat information from private companies. The DHS has also developed and implemented numerous information sharing programs. While helpful, these programs have not been widely adopted or used as hoped. One key reason is because some private companies do not want to cooperate with government entities, and do not trust that the government entities will protect their information and provide them with a safe harbor. The government needs to address this trust factor to encourage cooperation and collaboration. More importantly, government agencies should consider how to best incentivize effective cybersecurity in the private sector through its rules and regulations. *See generally* M. Krotoski, Views on Cyberthreat Information Sharing, Privacy & Security Law Report, 14 PVLR 687 (Apr. 20, 2015).

Overview of U.S. Regulatory Landscape A brief overview of the current cybersecurity regulatory landscape in the U.S. reveals several challenging issues that are at odds with the ideal goals of effective cybersecurity regulations and cooperation between the government and private entities. The U.S. legislative framework for

 COPYRIGHT © 2017 BY THE BUREAU OF NATIONAL AFFAIRS, INC. ISSN 1538-3423

data protection has incrementally become a patchwork quilt.

Unlike the EU and other jurisdictions, the U.S. does not have a dedicated data protection law, but instead regulates primarily by industry on a sector-by-sector basis. This state of affairs forces private companies to deal with inconsistent regulations, multiple enforcers, and varying standards. It is not uncommon for a company to be subject to multiple enforcers applying divergent cyber regulations to the same cyber incident. Additionally, there has been a discernable shift in recent regulations from a guidelines-based approach to a prescriptive one.

There are three main areas that are the subject of government regulation: (i) collection and use of nonpublic information; (ii) data security; and (iii) data breach notification.

Collection and Use of Nonpublic Information There are numerous sources of privacy law that dictate how firms may collect, use, or disclose non-public personal information, including laws and regulations developed at both the federal and state levels. These laws and regulations may be enforced by either federal or state authorities.

In the financial services context, for example, the Consumer Financial Protection Bureau and various financial services regulators (as well as state insurance regulators) have adopted standards pursuant to the Gramm-Leach-Bliley Act (GLB). Similarly, in the health-care arena, the Department of Health and Human Services is responsible for enforcement of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) against covered entities.

At the state level, attorneys general also have the ability to bring enforcement actions for unfair or deceptive trade practices, or to punish violations of specific state privacy laws.

Data Security GLB and HIPAA also have data security obligations. The Safeguards Rule implemented pursuant to GLB requires financial institutions to 'develop, implement, and maintain a comprehensive information security program' that contains administrative, technical, and physical safeguards designed to protect the security, confidentiality, and integrity of customer information. The Security Rule implemented pursuant to HIPAA sets forth specific steps that covered entities and their service providers must take to protect electronic public health information. Numerous federal agencies have also released regulations and guidance to covered entities regarding data security requirements. Several U.S. states also impose general information security standards on organizations that maintain personal information. The New York Department of Financial Services (DFS) has recently released rules for data security for entities under their remit. Many believe that the DFS' regulations adopted a highly prescriptive approach. *See, e.g.*, Law Flash, Urging NYDFS to Modify Proposed Cybersecurity Rules (Nov. 16, 2016).

The State of California requires organizations that own or license personal information about California residents to implement and maintain reasonable security procedures and practices to protect the information from unauthorized access, destruction, use, modification, or disclosure. In addition, organizations that disclose personal information to non-affiliated third parties must contractually require those entities to maintain reasonable security procedures.

Data Breach Notification At present, 52 jurisdictions in the U.S. (including 48 states and the District of Columbia, Guam, Puerto Rico, and the Virgin Islands) have enacted data breach notification laws that require data owners to notify affected individuals in the event of unauthorized access or acquisition of personal information, as that term is defined in each jurisdiction. In addition to notification of individuals, the laws in 20 states also require notice to a state regulator (typically the state attorney general). Although most state breach laws require notification only if there is a reasonable likelihood that the breach will result in harm to affected individuals, a number of jurisdictions do not employ such a harm threshold and require notification of any incident that meets their definition of a breach. Thus, the same incident may require notification in some jurisdictions but not others.

Other enforcers impose divergent notification standards. For example, the New York Department of Financial Services recently adopted this cumbersome notification double materiality standard: Notification not ''later than 72 hours from a determination that a Cybersecurity Event'' occurred for ''Cybersecurity Events that have a reasonable likelihood of materially harming any material part of the normal operation(s) of the Covered Entity.'' 23 NYCRR § 500.17(a)(2). Organizations subject to this rule often fall under the jurisdiction of other federal and state enforcers and will have to evaluate this notification standard along with others.

The numerous inconsistencies that apply based on these divergent state standards reinforce the need for streamlined standards, including a uniform national standard. As the inconsistencies multiply, the calls for federal pre-emption will correspondingly increase. *See, e.g.*, M. Krotoski, L. Wang, & J. Rosen, The Need to Repair the Complex, Cumbersome, Costly Data Breach Notification Maze, BNA's Privacy & Security Law Report, 15 PVLR 271 (Feb. 8, 2016) (noting the need for a uniform national standard to redress the myriad inconsistent standards that have resulted at the state level).

Issues One of the side effects of this ''patchwork'' of cybersecurity regulations is that it leads to inconsistent regulations, multiple enforcers and varying standards. Rather than promoting compliance, it becomes costly and burdensome. For example, while straight-forward notification standards have been adopted in nearly every state, the DFS' Cybersecurity Rules adopted an unnecessary and complicated ''double materiality standard'' based on ''a reasonable likelihood of *materially harming* any *material part* of the normal operation(s) of the Covered Entity.'' 23 NYCRR 500, 500.17 (March 1, 2017) (emphasis added). It remains unclear why an unduly complicated standard was drafted when pre-existing notification standards were available. Instead of harmonizing standards, another regulatory conflict was created. *See, e.g.*, California Data Breach Report (Feb. 2016) (recommending that ''State policy makers should collaborate in seeking to harmonize state breach laws on some key dimensions.'').

Companies operating in multiple jurisdictions regularly confront the challenge to comply with divergent standards. Additionally, a firm is often subject to a number of regulators applying each of its regulators' data security standards and different regulations that

are not be in sync with one other. For example, the DFS' Cybersecurity Rules are vastly different in substance and in approach from the guidance other agencies have issued for financial services providers. The DFS-covered entities thus have to develop a separate compliance program in order to comply with the new regulations. Some firms may also be subject to the concurrent enforcement jurisdiction of multiple agencies such as the Federal Trade Commission, the Securities and Exchange Commission, State Attorneys General, and the DOJ.

Factors that Government Should Consider on Cybersecurity Regulations It is time to clarify the proper role of government in cybersecurity regulation. We believe that the government can better incentivize and promote effective cybersecurity and that this can be best accomplished by reducing rather than increasing the regulatory burden on the private sector. This involves considering the following fundamental factors:

1. Does the government agency lead by example? Many government agencies mandate the collection of confidential, personal, and sensitive information that is stored by the government. Does the government agency, as an enforcer and leader on this issue, practice strong, effective cybersecurity? How many cyber incidents has the agency suffered and what were the circumstances? Would the government agency be able to comply with its own regulatory standards that it imposes on covered entities? Public confidence is weakened when the enforcer is unable to satisfy core cybersecurity practices or standards. The ability of the government agency to lead by example also addresses trust factor issues that the private sector may have with government collaboration.

2. Consider the regulatory costs of compliance when covered entities are already subject to multiple regulators. Regulators should consider the growing cost of cybersecurity, the limited resources that a company may have, and the necessity of tailored approaches for effective cybersecurity. Cybersecurity spending by the financial services industry has soared 67 percent since 2013. In 2016, security investments increased 11 percent from the year before. *See* PwC, ''Global State of Information Security Survey 2017: Financial Services.'' Overly detailed or new conflicting regulations impose costly compliance requirements, diverting resources towards compliance and away from investing in more robust cybersecurity efforts. Cybersecurity mandates should be streamlined and reduced, retaining flexibility for tailored cybersecurity solutions, and allowing limited resources to be targeted where they can have the most impact and promote security.

3. Reward companies adopting effective cybersecurity approaches by providing voluntary safe harbors and rules. **Punish the true bad actors—the hackers and thieves that perpetrate cyber attacks—through criminal and other enforcement actions.** When considering the uses of carrots and sticks, regulators should be aware of the efforts firm are already making. The interests of firms and of the regulators are squarely aligned regarding cybersecurity; cybersecurity remains a top priority for all industries. Each year, firms, regardless of their size, expend significant resources to safeguard consumer data and defend against cyber-crime. It is in the interest of all firms to train employees in cybersecurity best practices and retain experts to assist in further developing protective measures tailored to the specific needs of their firms.

4. Regulations should be voluntary, flexible (not ''one size fits all''), risk-based and evergreen and firms should be encouraged to adopt meaningful tailored cybersecurity enhancements as opposed to a mere ''check the box'' approach. Regulators should consider issuing guidance and voluntary standards as opposed to rules. Flexible and open standards—even those that are voluntarily adopted—enable firms to tailor and focus efforts on certain areas that are specific to the firms' particular needs and will have a greater impact on the prevention of cyber-attacks and protection of personally identifiable information.

Cybersecurity policies are most effective when they are tailored to a firm's unique cyber risks and vulnerable information. [The NIST Framework also expressly adopts a risk-based approach. The NIST Framework focuses on ''the likelihood that an event will occur and the resulting impact,'' and states that, by taking this information into account, ''organizations can prioritize cybersecurity activities, enabling organizations to make informed decisions about cybersecurity expenditures'' and develop methods to handle the unique risks faced by different firms by ''mitigating the risk, transferring the risk, avoiding the risk, or accepting the risk, depending on the potential impact to the delivery of critical services.''] An effective cybersecurity program, by its nature, cannot be a ''one size fits all'' or ''check the box'' program. Rather, the most effective cybersecurity programs take into consideration a host of factors related to the relevant business activities.

Previous supervision efforts, such as the Interagency Guidelines issued by the Agencies pursuant to the GLB, have applied a principles-based approach to cybersecurity. *See* 12 C.F.R. Part 364, Appendix B, Section II.A (requirement that a bank implement a comprehensive written information security program that includes administrative, technical, and physical safeguards appropriate to the size and complexity of the bank and the nature and scope of its activities); *id*. at Section III.C (requirement that a bank design its information security program to control identified risks commensurate with the sensitivity of the information as well as the complexity and scope of the bank's activities). A principles-based approach is flexible, permitting firms to tailor their cybersecurity programs to their unique needs, resulting in a more effective approach to cybersecurity. Many organizations have heterogeneous information technology environments that develop for a variety of reasons: mergers, legacy systems, customer demands and so forth.

Regulations that specify a particular technology or method of compliance may make demands that are impossible or inapposite. Conversely, flexible standards are often less vulnerable to obsolescence. Detailed specifications may decay quickly when technology changes rapidly, undercutting the efficacy of regulation, or forcing frequent updates to the detailed specifications. Penetration testing and other system vulnerability assessments are evolving on a continuous basis, making it impracticable to prescribe specific standards that do not run the risk of becoming quickly obsolete. Multi-factor authentication, for example, may be supplanted by other technological safeguards. The objective is to ensure data is secure. There are a variety of means today, and evolving over time, that may be more

 COPYRIGHT © 2017 BY THE BUREAU OF NATIONAL AFFAIRS, INC. PVLR ISSN 1538-3423

adept at protecting data. A rigid regulation will likely become quickly outmoded by superior methods.

The need for flexibility becomes all the more important when considering the wide diversity of firms in terms of size and nature of business that may be subject to a specific regulation. Each type of firm may gather and retain different types of protected data and, accordingly, the cybersecurity systems vary widely amongst these different types of businesses. For example, the cyber risks and types of data and transactions vary among investment companies, insurers, safe deposit companies, and charitable foundations. In addition, firms vary greatly in their size and sophistication of business activities.

5. Any mandatory requirements should be as simple and user-friendly for firms as possible and avoid unnecessary ambiguity and confusion. This would incentivize compliance and lower costs for firms. Imposing on firms a particular technology, system, control or approach may be unnecessarily burdensome and expensive, especially when infrastructures differ significantly, there are a range of alternatives, or the endpoint can be achieved without applying technology. Regulators must also keep in mind that while technology is crucial to any risk management discussion, it cannot be relied upon at the expense of other considerations, such as developing a mature cybersecurity culture and synchronizing third party vendor security. In addition, it is critical to consider the cost of complying with detailed standards and consider less costly alternatives before imposing regulations. While the full cost and impact of overly detailed regulations cannot be readily determined, they need to be assessed.

6. Any newly issued regulations should be harmonized with existing regulatory standards. Many companies are regulated by multiple federal and state agencies that impose distinct, and often conflicting, cybersecurity requirements.

Government officials and agencies have long recognized the need for coordination and convergence of cybersecurity regulatory activity. Government agencies should coordinate their cybersecurity efforts with other federal and state regulators to prevent inconsistent standards. **Former U.S. Treasury Secretary Jack Lew encouraged agencies ''to collaborate with the private sector to establish cyber security best practices and improve information sharing.'' Comptroller of the Currency Thomas J. Curry has underscored that ''[o]ne of the lessons we have learned in the bank regulatory community is that collaboration is vital, especially in dealing with highly complex, rapidly evolving challenges like cybersecurity.'' And former Deputy U.S. Treasury Secretary Sarah Bloom Raskin stressed the need to ''figure out ways [to] harmonize [cybersecurity standards]. We don't want to see emerge the development of multiple sets of standards, multiple guidances.''**

Harmonized guidance is the right approach because many firms and their subsidiaries are already subject to numerous cybersecurity regulations and requirements. For example, financial institutions are subject to a variety of regulatory bodies exercising overlapping jurisdiction—including but not limited to the CFTC, the SEC, the Federal Despoit Insurance Corp., the Federal Reserve, Federal Trade Commission, the Office of the Comptroller of the Currency, the Financial Industry Regulatory Authority, and the NFA—that have each promulgated regulations or guidance. See, e.g., CFTC Systems Safeguards, supra fn. 7; CFTC System Safeguards Testing Requirements for Derivative Clearing Organizations, 81 Fed Reg. 64,322 (Sept. 19, 2016); SEC Office of Compliance Inspections and Examinations (OCIE), National Exam Program, Examination Priorities for 2016; OCIE National Exam Program Risk Alert, OCIE's 2015 Cybersecurity Exam Initiative, Volume IV, Issue 8 (September 15, 2015); FTC, Start with Security: A Guide for Business (Lessons Learned from FTC Cases); FTC, Protecting Personal Information: A Guide for Business; NFA, Interpretive Notice to NFA Compliance Rules 2-9, 2-36 and 2-49 Information Systems Security Programs (effective March 1, 2016); FINRA Report on Cybersecurity Practices (February 2015); FINRA 2016 Regulatory and Examination Priorities Letter (January 5, 2016); Interagency Guidelines, supra n.4.

Multiple states are also becoming increasingly involved in the area of cybersecurity. State policy makers should collaborate to harmonize state data breach notification laws on some key dimensions (as noted above). Such an effort could reduce the compliance burden for companies, while preserving innovation, maintaining consumer protections and retaining jurisdictional expertise.

Conclusion Rather than incentivizing innovative cybersecurity solutions and fostering innovative approaches, the expanding regulatory patch quilt is promoting a culture of ''check the box'' compliance and diverting limited resources that can and should be dedicated to effective cybersecurity. Given the need for a strong government and private sector partnership to confront the cyber threat, government agencies should focus on fostering cooperation between government and the private sector and safeguarding our sensitive and valuable information. The government can and should lead appropriately and carefully on this important issue which impacts our national and economic security. The failure to do so will compromise rather than enhance our nation's cybersecurity.

By Mark L. Krotoski and Martin Hirschprung

To contact the editor responsible for this story: Donald Aplin at daplin@bna.com