Bloomberg BNA

Privacy and Security Law Report®

Reproduced with permission from Privacy & Security Law Report, 14 PVLR 2120, 11/23/15. Copyright © 2015 by The Bureau of National Affairs, Inc. (800-372-1033) http://www.bna.com

Data Security Standards

In the fast-changing data breach landscape, CEOs and boards need to understand the various data security yardsticks to measure their company against both to prepare effectively for cyberattacks and to understand what regulators and others will look to after the breach, the authors write.

Making Sense of a Morass: An Overview of the Different Standards U.S. Government Agencies and Other Entities Are Developing to Regulate Cybersecurity



By Richard H. Cunningham, Ryan T. Bergsieker and Reid Rector

Richard H. Cunningham, of counsel for Gibson Dunn & Crutcher LLP in Denver where he focuses on a wide range of antitrust and consumer protection matters, including government investigations, client counseling, and litigation.

Ryan T. Bergsieker, of counsel for Gibson in Denver, where his practice includes information security/data privacy counseling and litigation.

Reid Rector is an associate in Gibson's Litigation Department in Denver and is a member of the firm's Information Technology and Data Privacy practice group.

I. Introduction

Headlines abound about the latest data breaches at companies large and small. At this point, most business leaders and their counsel are aware of the threat of cyberattacks and have taken steps to prevent such attacks and plan for the aftermath in the event of a successful attack. But in this fast-changing landscape, very challenging questions remain about how counsel can help company leaders assess the adequacy of their businesses' cybersecurity efforts. Stated simply, how can in-house and outside counsel answer the questions chief executive officers and boards are asking: Are we doing enough? What yardsticks are we measuring ourselves against? How would our efforts be viewed by government regulators in hindsight after an attack?

Notwithstanding halting legislative efforts to create a more unified approach to cybersecurity enforcement, U.S. companies must operate for the time being in a

COPYRIGHT © 2015 BY THE BUREAU OF NATIONAL AFFAIRS, INC. ISSN 1538-3423

world of overlapping regulators. The Federal Trade Commission (FTC), state attorneys general, the Federal Communications Commission (FCC) and the Securities and Exchange Commission (SEC), among others, have each expressed through guidance or enforcement actions a clear intent to regulate cybersecurity practices. And even government agencies that do not play a direct enforcement role, such as the U.S. Department of Commerce's National Institute of Standards and Technology (NIST), have issued important guidance.

Each of these regulators brings a unique perspective and approach driven by its enforcement mission and statutory authority. For example, the FTC focuses on protecting consumers' personal information, and the FCC focuses on regulating the cybersecurity practices of telecommunications companies. This creates a patchwork quilt of legal standards and forces companies seeking to assess their cybersecurity compliance to evaluate two questions. First, which agencies might come knocking in the event of a successful hack or breach? And second, what does each of those regulators require in terms of security protocols?

This article seeks to provide an overview of the guidance and enforcement records of the federal and state agencies with broad jurisdiction that have currently ''put stakes in the ground'' as cybersecurity regulators. This index is not exhaustive (we omit foreign regulators and regulators with extremely narrow industry and/or issue jurisdiction), but our hope is that presenting a high-level overview of the activity of the primary regulators will assist companies working to navigate the matrix of enforcement risks and legal standards that apply to their organizations.

II. An Alphabet Soup of Regulators

Several prominent federal and state cybersecurity regulators' jurisdictions cut across industries.

Federal Trade Commission: The FTC is the most high-profile and active federal regulator of data security practices, having brought more than 50 enforcement actions since 2002.[1] Based on its statutory mission to regulate ''unfair or deceptive acts or practices in or affecting commerce,''[2] the FTC has asserted broad authority to regulate and enforce data security practices that affect consumers and has recently survived a high-profile court challenge to that authority.[3] In June 2015, the FTC issued updated guidance in the form of a 10-point plan, *Start with Security: A Guide for Business*.[4] The plan provides high-level priorities (factor data security ''into the decisionmaking in every department'') and specific suggestions (''insist on complex and unique passwords'').

The FTC guidance suggests that companies should plan ahead, minimize the data they store, and have robust systems and responses in place.

The FTC describes its flexible, situation-dependent standard as inquiring whether a company's practices are ''reasonable and appropriate in light of the sensitivity and volume of consumer information it holds, the size and complexity of its business, and the cost of available tools to improve security and reduce vulnerabilities.''[5] The FTC guidance suggests that companies should plan ahead, minimize the data they store, and have robust systems and responses in place. At just 14 pages, the FTC's guidance is a digestible starting point for any company assessing its cybersecurity efforts. The FTC also maintains a central website of potentially relevant materials,[6] including its guidance on data security in the ''internet of things''—i.e., connected devices, apps, sensors, and other services.[7]

Department of Justice (DOJ): Consistent with its law enforcement mission, the DOJ's emphasis to date has been on using its enforcement powers to bring cyber criminals to justice and to promote robust private sector cybersecurity practices through guidance and information sharing.[8] Notably, the DOJ ''view[s] corporations who are victims of a cyberattack as just that—victims . . .'' and the DOJ has ''encouraged other agencies to adopt a similar approach.''[9] In that vein, the DoJ issued ''best practices'' in April 2015 that focused on steps companies may take to plan for and respond to any cyberattack, but the DoJ has not initiated any enforcement actions against companies that have been victims of cyberattacks.[10] The DOJ's guidance is instructive nonetheless and includes a ''Preparedness Checklist'' that outlines recommended actions before, during, and after a cyberattack, with an emphasis on planning and having an ''actionable'' response plan in place. The DOJ's guidance also makes recommendations concerning collaboration with law enforcement and the appropriate time to report suspected incidents.

[1] Press Release, Fed. Trade Comm'n, *FTC Testifies on Data Security before Senate Banking Subcommittee* (Feb. 3, 2014), *available at* http://www.ftc.gov/news-events/press-releases/2014/02/ftc-testifies-data-security-senate-banking-subcommittee (last visited Oct. 26, 2015).

[2] 15 U.S.C. § 45(a)(1).

[3] *See, e.g.*, Fed. Trade Comm'n, *Commission Statement Marking the FTC's 50th Data Security Settlement* (Jan. 31, 2014); *see also FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015) (denying a challenge to the FTC's authority to regulate cybersecurity) (14 PVLR 1592, 9/7/15).

[4] Fed. Trade Comm'n, *Start with Security: A Guide for Business* (June 2015), *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf(14 PVLR 1236, 7/6/15).

[5] Fed. Trade Comm'n, *Commission Statement Marking the FTC's 50th Data Security Settlement* (Jan 31, 2014).

[6] Fed. Trade Comm'n, *Data Security*, *available at* https://www.ftc.gov/tips-advice/business-center/privacy-and-security/data-security (last visited June 24, 2015).

[7] Fed. Trade Comm'n, *Careful Connections: Building Security in the Internet of Things* (Jan. 2015), *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf0199-carefulconnections-buildingsecurityinternetofthings.pdf (14 PVLR 179, 2/2/15).

[8] *See* Press Release, Office of Pub. Affairs, U.S. Dep't of Justice, *Assistant Attorney General Leslie R. Caldwell Delivers Remarks at ''Cybersecurity + Law Enforcement: The Cutting Edge'' Symposium* (Oct. 16, 2015), *available at* http://www.justice.gov/opa/speech/assistant-attorney-general-leslie-r-caldwell-delivers-remarks-cybersecurity-law.

[9] *Id.*

[10] U.S. Dep't of Justice, *Best Practices for Victim Response and Reporting of Cyber Incidents* (Apr. 2015), *available at* http://src.bna.com/Tc

 COPYRIGHT © 2015 BY THE BUREAU OF NATIONAL AFFAIRS, INC. PVLR ISSN 1538-3423

State Attorneys General: State attorneys general play a significant role in policing cybersecurity issues. First, several states have enacted statutes or regulations that establish specific cybersecurity standards.[11] Second, state Attorneys General use state-level consumer protection laws to address data security issues based on theories similar to those applied by the FTC under Section 5 of the FTC Act. Finally, nearly every state has adopted breach notification laws that impose notification requirements on entities that have suffered a data breach, and state Attorneys General have brought enforcement actions pursuant to these provisions.

Office of Management and Budget (OMB): Companies that do business with the federal government are subject to an increasing number of regulations and requirements imposed by government contracts. In August 2015, the OMB published proposed guidance on ''Improving Cybersecurity Protections in Federal Acquisitions.''[12] If implemented, this guidance would have far-reaching consequences by placing cybersecurity-related requirements on all government contractors that handle controlled unclassified information (CUI). In its guidance, the OMB calls for the amendment of the Federal Acquisition Regulation (FAR) and actions by various agencies to incorporate the OMB's recommendations.[13]

Companies that do business with the federal government are subject to an increasing number of regulations and requirements imposed by government contracts.

Notably, the proposed guidance applies both to systems that contractors operate for the government and to contractors' own internal systems, and addresses requirements related to security controls, cybersecurity incident reporting, security assessments, security monitoring, and the role of agency due diligence.[14] The OMB guidance builds on proposed rules released in May 2015 by the National Archives and Records Administration (NARA), which is responsible for developing government-wide controls for CUI.[15] NARA also plans to release a single FAR clause for use in government contracts that will apply the requirements of its proposed rule to contractors.[16]

In addition to these cross-industry regulators, a host of regulators responsible for specific industries and/or sectors of the economy have established cybersecurity enforcement initiatives.

Federal Communications Commission: The FCC enforces the Federal Communications Act and has taken the position that it has jurisdiction to regulate data security practices at telecommunications companies under provisions of the Act that require companies to protect ''confidentiality of proprietary information'' (including customer information) and refrain from unjust and unreasonable practices.[17] The FCC has therefore weighed in with guidance specific to companies operating in the communications sector, including broadcast, cable, satellite, wireless, and wireline network service providers. In March 2015, an FCC-endorsed industry group, the Communications Security Reliability and Interoperability Council (CSRIC), issued a final report on *CyberSecurity Risk Management and Best Practices*.[18] That report creates voluntary mechanisms that communications companies can follow to ''give the [FCC] and the public assurance that communication providers are taking the necessary measures to manage cybersecurity risks.''[19] The report also identifies best practices and offers sector-specific advice on implementing the NIST Cybersecurity Framework (discussed below). The FCC has also taken several enforcement actions related to data privacy issues, securing settlements of up to $25 million from telecommunications companies that allegedly had lax data security practices.[20]

Securities and Exchange Commission: The SEC's recent efforts in this area have been focused on enforcing laws aimed at protecting customer information at companies in the financial industry (e.g., broker-dealers and advisers), and have not extended to all public companies that report to the SEC (though an expansion of the SEC's focus is not out of the question). In April 2014, the SEC's Office of Compliance Inspections and Examinations (OCIE) entered the fray when it released a list of questions it uses in cybersecurity investigations,[21] followed in February 2015 by a summary of findings and observations from its first industry assessment using those questions.[22] In September 2015, OCIE announced another round of investigations to ''further assess cybersecurity preparedness in the securities industry, including firms' ability to protect broker-dealer customer and investment adviser . . . [customer] information.''[23] Among companies that are subject to the SEC's jurisdiction in this space, the SEC's releases have

[11] *See, e.g.*, 201 Code Mass. Reg. 17.01 *et seq.* (Massachusetts' ''Standards for the Protection of Personal Information of Residents of the Commonwealth'').

[12] Office of Management and Budget, *Improving Cybersecurity Protections in Federal Acquisitions*, *available at* https://policy.cio.gov(14 PVLR 1516, 8/17/15) .

[13] *Id.*

[14] *Id.*

[15] *See* 80 Fed. Reg. 26501.

[16] *Id.*

[17] *See* 47 U.S.C. § § 201, 222.

[18] Commc'ns Security Reliability and Interoperability Council, *CyberSecurity Risk Management and Best Practices Working Group 4: Final Report* (Mar. 18, 2015), *available at* https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_WG4_Report_Final_March_18_2015.pdf (14 PVLR 504, 3/23/15).

[19] *Id.*

[20] Press Release, Fed. Commc'n Comm., *AT&T to Pay $25 Million To Settle Consumer Privacy Investigation* (Apr. 8, 2015), *available at* https://www.fcc.gov/document/att-pay-25m-settle-investigation-three-data-breaches-0 (14 PVLR 633, 4/13/15).

[21] Office of Compliance Inspections and Examinations, *OCIE Cybersecurity Initiative* , Nat'l Exam Program Risk Alert (Apr. 15, 2014), *available at* http://www.sec.gov/ocie/announcement/Cybersecurity-Risk-Alert—Appendix—-4.15.14.pdf .

[22] Office of Compliance Inspections and Examinations, *OCIE Cybersecurity Examination Sweep Summary*, Nat'l Exam Program Risk Alert (Feb. 3, 2015), *available at* http://www.sec.gov/about/offices/ocie/cybersecurity-examination-sweep-summary.pdf.

[23] Office of Compliance Inspections and Examinations, *OCIE's 2015 Cybersecurity Examination Initiative*, Nat'l Exam Program Risk Alert (Sept. 15, 2015), *available at* http://

shown that most of them have policies and procedures in place, but also that most have been affected by cybersecurity incidents. Like the other federal regulators, the SEC emphasizes comprehensive planning, preparedness, and adherence to industry best practices and technical standards. In a sign that the SEC is turning towards active enforcement of these guidelines, the SEC announced its first cybersecurity enforcement action in September 2015, a settlement with a St. Louis-based investment adviser for allegedly failing to establish required cybersecurity policies and procedures to protect customer information.[24]

Department of Defense (DOD): The DOD has an active cybersecurity risk management strategy for national security purposes, and the DOD's security priorities flow to contractors doing business with the Pentagon. In November 2013, for example, the DOD issued a final rule amending the Defense Federal Acquisition Regulations System to include new requirements related to cybersecurity incident reporting for government contractors.[25] The DOD updated those requirements in August 2015, when a new set of proposed data breach notification reporting rules became effective immediately, even as comments on the proposed rules were being collected.[26] The rule applies ''to all contractors with covered defense information transiting their information systems,'' which the DOD estimates may be 10,000 contractors.[27]

Department of Energy (DOE): On Jan. 8, 2015, the DOE released the *Energy Sector Cybersecurity Framework Implementation Guidance*.[28] Like the FCC, the DoE created its guidance in collaboration with industry participants, and the guidance provides sector-specific recommendations and guidance based on the NIST Cybersecurity Framework. The DOE also released guidance in April 2014 that provides strategies and suggested language to help the energy sector and technology suppliers improve cybersecurity protections during product design and manufacturing.[29]

Food and Drug Administration (FDA): The FDA has issued guidance relevant to medical device manufacturers and other entities subject to the FDA's purview. On Oct. 2, 2014, for example, the FDA released final guidance regarding cybersecurity measures in premarket submissions for medical devices.[30] The guidance outlines ''issues related to cybersecurity that manufacturers should consider in the design and development of their medical devices as well as in preparing premarket submissions for those devices.'' On May 28, 2015, the FDA released its ''Guidance for Industry—Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software,''[31] which elaborates the FDA's expectations about cybersecurity measures for medical devices.

III. Technical Standards and Guidance

In addition to guidance from federal and state agencies, several prominent entities have published technical guidance that companies may refer to when assessing the reasonableness of their cybersecurity preparedness.

National Institute of Standards and Technology: In February 2014, the NIST issued the *Framework for Improving Critical Infrastructure Cybersecurity*.[32]

At its core, the NIST Framework is a cybersecurity risk management tool designed to create a shared vocabulary about cybersecurity and help corporate decision-makers better manage cybersecurity exposure.

At its core, the Framework is a cybersecurity risk management tool designed to create a shared vocabulary about cybersecurity and help corporate decision-makers better manage cybersecurity exposure. The Framework provides a high-level view of companies' management of cybersecurity risks and options for potential enhancements. Government regulators are increasingly relying on the NIST Framework as the basis for their own guidance, with agencies like the DoE and the FCC expressly adapting the framework for their industry members. NIST also contributed to the creation of security guidelines for federal contractors when it released guidelines in June 2015 in NIST Special Publication 800-171[33]. These guidelines inform the NARA and OMB efforts discussed above.

Payment Card Industry Data Security Standard (PCI DSS): The PCI DSS specifies that any company that stores, processes, or transmits payment cardholder information must, as a condition of processing transactions, follow high-level requirements in six general ar-

www.sec.gov/ocie/announcement/ocie-2015-cybersecurity-examination-initiative.pdf.

[24] Press Release, SEC, ''SEC Charges Investment Adviser With Failing to Adopt Proper Cybersecurity Policies and Procedures Prior To Breach'' (Sept. 22, 2015), *available at* http://www.sec.gov/news/pressrelease/2015-202.html (14 PVLR 1749, 9/28/15).

[25] 48 C.F.R. § § 204, 212, 252 (2013).

[26] *See* 80 Fed. Reg. 51,739–51,748 (Aug. 26, 2015) (14 PVLR 1609, 9/7/15).

[27] *See Id.* at 51,740.

[28] Dep't of Energy, *Energy Sector Cybersecurity Framework Implementation Guidance* (Jan. 8, 2015), *available at* http://energy.gov/sites/prod/files/2015/01/f19/Energy%20Sector%20Cybersecurity%20Framework%20Implementation%20Guidance_FINAL_01-05-15.pdf.

[29] Dep't of Energy, *Cybersecurity Procurement Language for Energy Delivery*, *available at* http://energy.gov/oe/downloads/cybersecurity-procurement-language-energy-delivery-april-2014.

[30] FDA, *Content of Premarket Submissions for Management of Cybersecurity in Medical Devices* (Oct. 2, 2014), *available at* http://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm356190.pdf (13 PVLR 1725, 10/6/14).

[31] FDA, *Guidance for Industry —Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software* (May 28, 2015), *available at* http://www.fda.gov/RegulatoryInformation/Guidances/ucm077812.htm .

[32] *See* National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity* (Feb. 12, 2014), *available at* http://www.nist.gov/cyberframework/ (13 PVLR 281, 2/17/14).

[33] *available at* http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171.pdf (14 PVLR 1190, 6/29/15).

 COPYRIGHT © 2015 BY THE BUREAU OF NATIONAL AFFAIRS, INC. PVLR ISSN 1538-3423

eas of information security: (1) building and maintaining a secure network and system; (2) protecting cardholder data; (3) maintaining a vulnerability management program; (4) implementing strong access control measures and regularly monitoring and testing networks; and (5) maintaining an Information Security Policy. Beyond the high-level requirements, the standard specifies more detailed requirements and testing procedures to validate compliance.

ISO 27001 Standard: The International Organization for Standardization and the International Electrotechnical Commission publishes this information security management framework, which sets forth a set of high-level organizational policies, procedures, and technical standards that a company may wish to follow, based on the specific risks it faces, to analyze and manage its security risks. ISO 27001 provides a checklist for a company's management to consider regarding how to set, execute, implement, and validate the effectiveness of the company's information security policy.[34]

ISO 27002 Standard: This standard suggests guidelines and general principles for initiating, implementing, maintaining, and improving information security management within an organization. The standard outlines hundreds of potential security controls and control mechanisms for a company's use after a formal risk assessment. Specifically, the ISO 27002 standard suggests guidance to a company on how to manage employees, organizational assets, suppliers, network security, physical security, and security incident response.[35]

IV. Key Takeaways

Several conclusions may be drawn from the record of enforcement actions, agency guidance, and third-party guidance:

- **For the foreseeable future, it will be complicated**. Unless Congress unexpectedly enacts comprehensive legislation, most companies will be subject to the jurisdiction of multiple overlapping regulators for the foreseeable future. This means that companies need to stay up-to-date on the rapidly evolving guidance from those regulators and also may need to anticipate overlapping investigations in the event of a cyberattack.
- **Standards are evolving and tightening**. As reflected by the sheer volume and cadence of guidance and enforcement from the FTC, SEC, FCC, and others, agencies are rapidly developing detailed positions regarding what practices are reasonable and unreasonable, and are willing to bring enforcement actions when companies do not adhere to those practices. Moreover, the clear trend—especially in the vanguard cases brought by the FTC—is moving from prosecuting egregious violations toward challenging practices that fall into more of a gray area in terms of their reasonableness, and that may have been a result of inattention rather than intentional misconduct.
- **Standards are not identical**. There is considerable variation in the standards to which companies may turn for guidance. Some are more technical; others, more focused on reasonableness standards that are, as yet, not highly refined through case-by-case adjudication. Together, the available guidance provides useful information for companies to consider, but it is essential for a company's legal department to work hand-in-hand with its information security department to determine whether particular standards are applicable to a company's activities and how those standards can be measured against the company's systems.
- **Planning is paramount**. If there is one hallmark of all of these standards, it is the emphasis on robust and comprehensive planning and implementation. An appropriate, well-developed, and thoroughly implemented plan is a must-have for every company.
- **Breach response matters**. Even with robust plans and practices in place, the worst can still happen. And in that case, a company's response is important. Several state Attorneys General have brought enforcement actions against companies for failing to comply with state breach notification statutes. Many agencies require notification within a specified time after a breach in which government information has been exfiltrated. Enforcement premised on the reasonableness of a company's post-breach response may be a logical extension of enforcers' current approach.
- **There is an increasing emphasis on data minimization**. The FTC and others are increasingly counseling companies not to collect information they do not need to run their business. A logical follow-on to this guidance are enforcement actions in cases where the hacked company's data security practices were otherwise reasonable, but the company did not have a demonstrable need in the first instance to obtain and retain the stolen personal information.

[34] *See generally* http://www.iso.org/iso/home/standards/management-standards/iso27001.htm (last visited July 14, 2015).

[35] *See generally* http://www.iso.org/iso/catalogue_detail?csnumber=54533 (last visited July 15, 2015).