Reprinted with Permission from *Law360*

National Cybersecurity Report: Top Business Takeaways

Law360, New York (December 14, 2016) –

Jonathan G. Cedarbaum

The recently released report of the nonpartisan Commission on Enhancing National Cybersecurity, established pursuant to an executive order issued by President Barack Obama in February, sets out more than 50 policy recommendations for the next administration.[1] With the Trump administration's appointments to many positions likely to shape its cybersecurity policies not yet determined and thus the direction of the new administration's cybersecurity initiatives unclear, it remains uncertain how influential the commission's recommendations will be. But the commission's 12 members, selected in part by congressional leaders and in part by the president and drawn from government, business, academia and the military, represent a knowledgeable and bipartisan group of advisers.[2] Their recommendations deserve careful consideration, and at least some are likely to be pursued by the Trump administration.

This article highlights a handful of the most important takeaways from the report for businesses, particularly ones that should be of interest to companies across the economy.

Cybersecurity Is Here To Stay

If you thought cybersecurity was a passing fad, think again. More and more aspects of our economic, social, cultural and political institutions and activities are becoming more dependent on networked devices every day. The security of our communications and actions using those devices and networks is thus becoming ever more essential to the efficient functioning of our economy and society. As the commission's report puts it:

> As the world becomes more immersed in and dependent on the information revolution, the pace of intrusions, disruptions, manipulations and thefts also quickens. Technological advancement is outpacing security and will continue to do so unless we change how we approach and implement cybersecurity strategies and practices.[3]

Customers — whether individual consumers or enterprises — and regulators will therefore be focusing with increasing urgency on how companies address data security in their products and services. Thus, as the commission notes, "[s]ecurity, privacy and trust must be primary considerations at the outset when new cyber-related technologies, products and services are conceived, rather than auxiliary issues to be taken into account after they are developed."[4] As the commission's report also emphasizes, that means that small- and medium-sized businesses in particular will need to pay greater attention to cybersecurity, and will require greater assistance in order to do so.[5]

Pay Attention to the NIST Cybersecurity Framework

Looking back 10 years from now, one of the most important legacies of the Obama administration may prove to be the set of voluntary cybersecurity standards and recommended assessment practices released by the National Institute of Standards and Technology in February 2014. Known formally as the Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0 and informally as the NIST cybersecurity framework, this guide has expanded its influence steadily from its initial release.[6] With its flexible, risk-based and process-oriented approach, the framework has proved adaptable to many industries. It has also gained admirers abroad, as indicated, for example, by the British Standards Institution's recent survey on developing a third-party certification process based on the NIST framework.[7]

As the commission's report emphasizes, businesses of all sizes and across different sectors should look to the NIST framework as a fundamental guide in improving their cybersecurity practices and reducing their cyber risk.[8]

Effective Public-Private Collaboration Is Crucial

Drawing on the experience of the development of the NIST framework — which incorporated extensive input from the private sector — the commission wisely calls for extensive collaboration between government and private sector contributors as a key to effective improvements in cybersecurity.[9] The commission recognizes that the proliferation of top-down regulatory requirements represents an obstacle to improvement in an area that requires response to rapid changes in technologies and risks. Thus, the commission sensibly urges regulatory agencies to "harmonize existing and future regulations with the NIST cybersecurity framework to focus on risk management — reducing industry's cost of complying with prescriptive or conflicting regulations that may not aid cybersecurity and may unintentionally discourage rather than incentivize innovation."[10]

Hopefully, regulators will heed the commission's cautionary statements. Unfortunately, not only do federal cyber standards continue to multiply in an uncoordinated fashion, but state governments have added to a mosaic that can become a drag on rather than a support for reduction of cyber risk.

The commission also wisely urges the federal government to, "extend additional incentives to companies that have implemented cyber risk management principles and demonstrate collaborative engagement."[11]

These are welcome messages for the business community, which should help spread them in its dealings with regulators. At the same time, for them to take hold, the private sector needs to articulate clearly and precisely the alternatives to further regulation that it seeks and how they will accomplish the common goal of improved cybersecurity, particularly for critical infrastructure systems. More intensive private sector collaboration efforts, such as the Financial Services Analysis and Resiliency Center, recently formed by a number of major financial institutions, may also provide alternatives to enhanced regulation.[12]

The Internet of Things is the Next Frontier

The “internet of things” (IoT) is the vast collection of devices used in all aspects of business and personal life that are connected to the internet and tied to physical activities, such as controlling a thermostat, driving a car or regulating a medical device. One of the commission report’s central themes is that the explosion of the IoT represents both an enormous opportunity for economic growth and a massive opening of new vulnerabilities to be exploited by malicious actors. That potential for exploitation has recently been demonstrated powerfully by a number of major distributed denial of service attacks using IoT devices as members of massive botnets, including the October attack on the domain name server company Dyn.[13]

In focusing on the IoT, the commission’s report follows a path taken by other government studies.[14] One earlier study predicted there could be as many as 50 billion devices connected to the internet by 2020, with IoT devices greatly outnumbering traditional computers.[15] But basic consensus security standards for IoT devices lags behind their development and adoption.

Companies involved in the development and marketing of IoT devices therefore should focus urgently on designing user-friendly security characteristics and promoting their use. Public-private collaborations on the development of IoT security standards and best practices — recommended not only by the commission but by other advisory bodies and the U.S. Department of Homeland Security — are on their way.

Failure to develop and put in place these security improvements risks not only empowering malicious actors but also bringing new liability on companies that do not pay enough attention to the security of these devices. The commission calls for the U.S. Department of Justice to, “lead an interagency study with the U.S. Departments of Commerce and Homeland Security and work with the Federal Trade Commission, the Consumer Product Safety Commission, and interested private-sector parties to assess the current state of the law with regard to liability for harm caused by faulty IoT devices and provide recommendations within 180 days.”[16] Whether that particular interagency effort gets off the ground or not, a debate over liability for cybersecurity lapses in IoT devices — whether driven by policymakers or litigants — is on the horizon, as one of the commissioners has separately emphasized in an interesting recent blog post.[17]

The Human Element in Data Security Is Critical

Another major theme of the commission’s report is the centrality of human factors in influencing data security vulnerabilities and solutions. This has several implications for businesses.

First, as the commission emphasizes, the country needs a greatly expanded workforce of people skilled in developing and putting in place cybersecurity tools.[18] Second, cybersecurity methods need to take into account not only technical effectiveness but also ease of adoption. “Because human behavior and technology are intertwined and vital to cybersecurity,” the report explains, “technologies and products should make the secure action easy to do and the less secure action more difficult to do.”[19] Third, training and organizational culture can make the difference between success and failure in a company's cybersecurity. "Effective cybersecurity," the commission observes, "depends on consumer and workforce awareness, education and engagement in protecting their digital experience," which must be "a continuous process."[20]

—By Jonathan G. Cedarbaum, WilmerHale

Jonathan G. Cedarbaum is a partner in WilmerHale's Washington, D.C. office who specializes in false claims acts and cybersecurity, privacy and communications.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of the firm, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

[1] Commission on Enhancing National Cybersecurity: Report on Securing and Growing the Digital Economy (Dec. 1, 2016) ("Commission Report"), available at https://www.nist.gov/cybercommission.

[2] The commission's chair and vice chair were Tom Donilon, former national security adviser to President Obama, and Samuel J. Palmisano, retired chairman and CEO of IBM. The other members were: General (Ret.) Keith B. Alexander, founder and CEO of IronNet Cybersecurity; former director of the National Security Agency and former founding commander of U.S. Cyber Command; Ana I. Antón, professor and chairwoman of the School of Interactive Computing, Georgia Institute of Technology; Ajay Banga, president and CEO, MasterCard; Steven Chabinsky, global chairman of data, privacy and cybersecurity, White & Case; Patrick Gallagher, chancellor, University of Pittsburgh; former director, National Institute of Standards and Technology; Peter Lee, corporate vice president, Microsoft Research; Herbert Lin, senior research scholar for cyber policy and security, Stanford University; Heather Murren, founder, Nevada Cancer Institute; former managing director, Global Consumer Products Research, Merrill Lynch; Joseph Sullivan, chief security officer, Uber; and Maggie Wilderotter, chairman and CEO, The Grand Reserve Inn, former executive chairman, Frontier Communications.

[3] Commission Report at 1.

[4] Id. at 5.

[5] See Commission Recommendation 1.5.

[6] The Cybersecurity Framework and related materials developed by NIST are available here: https://www.nist.gov/cyberframework.

[7] The BSI's request for information can be found here: http://pages.bsigroup.com/l/73472/2016-08-11/61k6wf.

[8] See Commission Recommendations 1.4 and 5.3 and Action Items 1.2.3, 1.5.1, and 6.1.5.

[9] See Commission Recommendations 1.2, 1.3, and 2.1 and Action Item 1.4.1.

[10] Commission Report at 20.

[11] Id. at 21. See also id. at 5 ("Incentives should always be preferred over regulation, which should be considered only when the risks to public safety and security are material and the market cannot adequately mitigate these risks.").

[12] See FS-ISAC Announces The Formation Of The Financial Systemic Analysis & Resilience Center (FSARC) (Oct. 24, 2016), available at http://www.prnewswire.com/news-releases/fs-isac-announces-the-formation-of-the-financial-systemic-analysis--resilience-center-fsarc-300349678.html.

[13] See, e.g., James Scott and Drew Spaniel, Rise of the Machines: The Dyn Attack Was Just a Practice Run, Institute for Critical Infrastructure Technology (2016), available at http://icitech.org/icit-publication-the-rise-of-the-machines-the-dyn-attack-was-just-a-practice-run/.

[14] Department of Homeland Security, Strategic Principles for Securing the Internet of Things Version 1.0 (Nov. 15, 2016), available at https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf; FTC Staff Report, Internet of Things: Privacy and Security in a Connected World (Jan. 2015), available at https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf; The President's National Security Telecommunications Advisory Committee, NSTAC Report to the President on the Internet of Things (2014), available at https://www.dhs.gov/sites/default/files/publications/IoT%20Final%20Draft%20Report%2011-2014.pdf;

[15] NSTAC Report at ES-2, 1, 4.

[16] Commission Action Item 2.1.3.

[17] Herb Lin, Regarding the Report of the Presidential Commission on Enhancing National Cybersecurity (Dec. 6, 2016), available at https://www.lawfareblog.com/regarding-report-presidential-commission-enhancing-national-cybersecurity%E2%80%A6.

[18] See Commission Imperative 4.

[19] Commission Report at 5.

[20] Id.