In Focus: An Opinion on the Report on Securing and Growing the Digital Economy

By: Nir B. Kshetri

Kshetri, Nir. (2017)."In Focus: An Opinion on the Report on Securing and Growing the Digital Economy", IEEE Security & Privacy January/February, pp. 2-7. DOI: 10.1109/MSP.2017.10

Made available courtesy of Institute of Electrical and Electronics Engineers:
http://dx.doi.org/10.1109/MSP.2017.10

*****© 2017 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works.**

*****Note: This version of the document is not the copy of record. Figures may be missing from this format of the document. Footnotes and endnotes indicated with parentheses.**

Abstract:

On 1 December 2016, the US Commission on Enhancing National Cybersecurity (the Commission)—charged with developing recommendations to ensure the digital economy's growth and security—released the "Report on Securing and Growing the Digital Economy" (the Report).(1) The nonpartisan Commission was formed to develop the Report in response to challenges posed by cyberthreats. The Report focuses on areas such as the protection of critical infrastructure, the Internet of Things (IoT), cybersecurity R&D, public awareness and education to strengthen cybersecurity, governance issues, development of a cyber-ready workforce, identity management and authentication, cyberinsurance, international and global issues, and the role of small and medium-sized businesses (SMBs).

Keywords: cybersecurity | Internet of Things | blockchain | Dyn | information and communications technologies

Article:

On 1 December 2016, the US Commission on Enhancing National Cybersecurity (the Commission)—charged with developing recommendations to ensure the digital economy's growth and security—released the "Report on Securing and Growing the Digital Economy" (the Report).(1) The nonpartisan Commission was formed to develop the Report in response to challenges posed by cyberthreats. The Report focuses on areas such as the protection of critical infrastructure, the Internet of Things (IoT), cybersecurity R&D, public awareness and education to strengthen cybersecurity, governance issues, development of a cyber-ready workforce, identity management and authentication, cyberinsurance, international and global issues, and the role of small and medium-sized businesses (SMBs).

The Six Imperatives

The Report contains 16 recommendations and 53 related action items intended to strengthen US cybersecurity. The Commission also provides short-, medium-, and long-term time frames for each action item. The recommendations and action items are divided into six imperatives, which I discuss in further detail in the following sections.

Imperative 1

In Imperative 1: Protect, Defend, and Secure Today's Information Infrastructure and Digital Networks, the Report recognizes the importance of extensive and close cooperation between the government and the private sector to protect systems and networks.

The Report, emphasizing that cybersecurity problems will further intensify in the future, suggests that the federal government and private sector launch a multiyear joint initiative to deal with the growing challenge. Recommendation 1.1 states: "The private sector and the Administration should collaborate on a roadmap for improving the security of digital networks, in particular by achieving robustness against denial-of-service, spoofing, and other attacks on users and the nation's network infrastructure."

The Report also addresses the role of public–private partnership to prevent destruction and degradation of infrastructure and to mitigate cybersecurity risks. The Report points to the need to move from the current focus on cybersecurity incident response toward collaboration in all stages of operations. Primary emphasis must be placed on information exchange throughout the prevention and detection of incidents and the response to such incidents. For instance, government agencies might have actionable intelligence that helps companies manage their cyberrisks. As recommendation 1.2 notes, "As our cyber and physical worlds increasingly converge, the federal government should work closely with the private sector to define and implement a new model for how to defend and secure this infrastructure."

Strong identity management is a key emphasis of the Report. The Report raises potential concerns about our reliance on usernames and passwords as the most common form of identification and authentication. It contends that commercial adoption of large-scale identity management frameworks with stronger and more usable authentication is being hampered by the lack of uniform standards and users' preference for convenience. On the basis of such challenges, recommendation 1.3 states: "The next Administration should launch a national public–private initiative to achieve major security and privacy improvements by increasing the use of strong authentication to improve identity management."

One of the Commission's recommendations for the next presidential administration is to "build on the success of the Cybersecurity Framework to reduce risk, both within and outside of critical infrastructure, by actively working to sustain and increase use of the Framework" (recommendation 1.4). The Cybersecurity Framework, also known as the "Framework for Improving Critical Infrastructure Cybersecurity" (called for by Executive Order 13636 in January 2013(2)) was released in February 2014. NIST coordinated this voluntary framework's development.

The Report also presents data on US SMBs and their contribution to the national economy and job creation, arguing that almost all rely on information and communications technologies (ICTs). Most SMBs, however, likely lack the skills and resources needed to take cybersecurity measures. For some SMBs, cybersecurity isn't the highest priority. A cybersecurity breach is likely to harm SMBs' business, customers, employees, and business partners. The Report explicitly acknowledges that the federal government needs to help SMBs strengthen their cybersecurity. Recommendation 1.5 states: "The next Administration should develop concrete efforts to support and strengthen the cybersecurity of [SMBs]."

Imperative 2

In Imperative 2: Innovate and Accelerate Investment for the Security and Growth of Digital Networks and the Digital Economy, the Report considers how the IoT is increasingly blurring the distinctions among critical infrastructure, regulated devices, and consumer products. The Report then explains how low consumer awareness of the IoT's security implications is associated with a higher likelihood that malicious actors will compromise such devices.

The Report also presents examples of IoT-based products, describing the criticalness of cybersecurity for various devices. A "one-sizefits- all" approach to the design and development of IoT-based products thus might be ill advised and likely ineffective in terms of meeting the privacy and security needs of different groups of people. Recommendation 2.1 notes: "The federal government and private sector partners must join forces rapidly and purposefully to improve the security of the [IoT]."

The lack of coordination and balance in current cybersecurity R&D efforts was also addressed. More emphasis is placed on developing reactive capabilities that identify, detect, and respond to threats and vulnerabilities and provide additional protection. The Report recommends that federal R&D cybersecurity funding for federal civilian agencies increase by $4 billion over the next 10 years. The Commission suggests that high priority be given to "efforts that will result in the use, integration, and deployment of affordable, inherently secure, privacy-protecting, usable, functional, resilient, recoverable, and defensible systems." Another recommendation for the federal government is to "make the development of usable, affordable, inherently secure, defensible, and resilient/recoverable systems its top priority for cybersecurity [R&D] as a part of the overall R&D agenda" (recommendation 2.2).

Imperative 3

In Imperative 3: Prepare Consumers to Thrive in a Digital Age, the Report stresses that manufacturers should create products and systems with built-in cybersecurity. The Report also suggests that manufacturers inform users about how their data and information are protected. A recommendation for ICT business leaders is to "work with consumer organizations and the Federal Trade Commission (FTC) to provide consumers with better information so that they can make informed decisions when purchasing and using connected products and services" (recommendation 3.1).

The Report discusses increasing research on human interaction so that designers and manufacturers better understand the process for creating secure and easy-to use products. A recommendation for the federal government is to "establish, strengthen, and broaden 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 the [IoT] and other connected technologies" (recommendation 3.2).

Imperative 4

In Imperative 4: Build Cybersecurity Workforce Capabilities, the Report presents data on the US's and global economy's shortage of cybersecurity professionals and recommends that current efforts be expanded to attract more workers. As recommendation 4.1 notes, "The nation should proactively address workforce gaps through capacity building, while simultaneously investing in innovations—such as automation, machine learning, and artificial intelligence—that will redistribute the future required workforce."

Imperative 5

In Imperative 5: Better Equip Government to Function Effectively and Securely in the Digital Age, the Report highlights two challenges faced by the federal government on the cybersecurity front. First, the fact that it's a major IT user makes it highly dependent on a reliable and secure cyberinfrastructure. Second, several federal agencies play key roles in protecting and defending the country from cyberattacks and in responding to catastrophic cyberincidents. The Report thus argues that cybersecurity must be accorded the same level of national security priority as counterterrorism and homeland protection.

The Report points out that certain aspects of the IT infrastructure are likely to perform better when managed as a shared resource. The first recommendation for the federal government is to "take advantage of its ability to share components of the [IT] infrastructure by consolidating basic network operations" (recommendation 5.1).

The Report also covers the serious legacy IT problem facing government agencies, indicating a prevalence of older technologies with poorer security functionality. The Report explicitly acknowledges the central importance of modernizing government systems to increase security and performance. It notes the importance of implementing "improved standards, guidelines, and best practices, as well as a more agile and capable workforce." Recommendation 5.2 states: "The President and Congress should promote technology adoption and accelerate the pace at which technology is refreshed within the federal sector."

The Report also raises concerns that federal agencies' cybersecurity requirements are often viewed as a "checklist" that's separate from their core functions and capabilities. The Commission identified the importance of adopting a risk management approach that's guided by the US Office of Management and Budget's (OMB's) enterprise risk management program. Recommendation 5.3 notes: "Move federal agencies from a cybersecurity requirements management approach to one based on enterprise risk management (ERM)."

The Report also recommends that cybersecurity be accorded a top national security priority and relevant officials be sufficiently empowered. Overall, the Report concludes that more resources should be devoted and the government staffed and organized in a better way to carry out the mission. Another recommendation for the federal government is to "better match cybersecurity responsibilities with the structure of and positions in the Executive Office of the President" (recommendation 5.4).

The Report stresses that various government departments and agencies must clearly understand their roles and responsibilities to increase the nation's cybersecurity preparedness. The Report explains that such an understanding will lead to improved coordination and more efficient use of resources. Recommendation 5.5 notes: "Government at all levels must clarify its cybersecurity mission responsibilities across departments and agencies to protect and defend against, respond to and recover from cyber incidents."

Imperative 6

Finally, in Imperative 6: Ensure an Open, Fair, Competitive, and Secure Global Digital Economy, the Report raises concerns about how a "patchwork of technology requirements, regulations, policies, and laws" has hampered the free flow of information in the globally connected economy. The Report then emphasizes the importance of coordinated and effective international harmonization and cooperation to realize the Internet's full economic benefits. The Report recommends that the administration "encourage and actively coordinate with the international community in creating and harmonizing cybersecurity policies and practices and common international agreements on cybersecurity law and global norms of behavior" (recommendation 6.1).

A Critical Assessment

A main focus of the Report is the huge gap between the demand and supply of cybersecurity professionals. The Report describes some current successful efforts such as NSF support in building capacity in institutions of higher education through the CyberCorps, the Cybersecurity National Action Plan's (CNAP's) cybersecurity education and workforce initiatives, and NIST's National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework. The Report emphasizes the need for increased funding to further scale these and other successful initiatives to address the national cybersecurity workforce shortage. However, the Report is silent on stronger mechanisms such as special visa programs that could attract qualified cybersecurity professionals from other countries. For instance, organizations in Singapore are recruiting cybersecurity professionals from overseas.(3)

The Report examines the current state of consumers' "near-universal dependence" on ICTs and their lack of understanding of how to protect data and personal information. More important, the Report indicates that consumers are ill-equipped to select the technology products and services that best meet their cybersecurity and privacy needs. The Report recognizes that a main component of the US's cybersecurity strategy has been to raise consumers' cybersecurity awareness, citing many federal, private-sector, and nonprofit attempts that have been undertaken to increase awareness for many demographic groups. Despite good intentions, however, public-

and private-sector efforts have been largely unsuccessful. The Report explains that some of the public awareness campaigns have been carried out by technology-centered organizations rather than those with expertise in public messaging and behavioral change. No one disagrees that consumers' lack of cybersecurity orientation is a key issue that must be addressed. The Report, however, lacks details on the concrete steps, mechanisms, and processes required to raise consumers' cybersecurity awareness and knowledge.

The Report examines the current leadership and organizational structure for dealing with cybersecurity in the federal government. The Report indicates that the federal government's organizational structure and the amount of resources devoted to cybersecurity are insufficient to secure the US digital economy. It details some important steps the federal government has taken to improve national cybersecurity, such as appointing the first-ever Federal Chief Information Security Officer and establishing a privacy branch in the OMB Office of Information and Regulatory Affairs. Strong cybersecurity, however, requires a multipronged approach. The government must teach all its employees—including the 22 million federal, state, and local government employees and government contractors—about strong cybersecurity practices and ensure that they follow proper procedures.

The Report could have analyzed the use of new ICTs such as blockchain to enhance cybersecurity. Consider the October 2016 cyberattacks on the Domain Name System (DNS) provider Dyn. Dyn said that the attacks originated from "tens of millions of IP addresses" and was among the largest ever attacks.(4) According to Dyn, at least some of the malicious Internet traffic came from IoT devices, including webcams, baby monitors, home routers, and digital video recorders.(5) Because the attacks involved Mirai malware, Chinese camera manufacturer Hangzhou Xiongmai recalled its products sold in the US that were vulnerable to the Mirai malware.(6) The recall, however, applied only to devices sold under Xiongmai's name.(7) The recall also covered the first few batches of surveillance cameras made in 2014, which monitored rooms or shops for personal use.(8) The recall problem could have been resolved with blockchain technology, one of the most striking features of which is that it enables parties to store transactions in a secure, transparent, and publicly accessible way. These characteristics make it especially suitable for complex workflows such as those for technology production and supply chain. When an item changes ownership, blockchain can be used to register the time, location, price, parties involved, and other relevant information. The technology can also be used to track raw materials as they move through the supply chain, transform into circuit boards and electronic components, are integrated into products, and finally sold to customers. Blockchain can also be used to register updates, patches, and part replacements applied to any product or device throughout its lifetime. This would make it easier to track progress in addressing vulnerabilities and security problems and send warnings and notifications to product owners.(9)

The Report tries to capture the thinking of technology designers and manufacturers. It suggests that ease of use must be a key factor in product development. The Report also explains that products designed with increased privacy and security protections are often complex and difficult to use. Because cybersecurity is one of the most serious national security problems, it might be necessary to incorporate new regulatory requirements favoring more secure products.

The Commission provided suggestions and recommendations for the next administration, although it's not clear whether these recommendations will be adopted. First, there's widespread disagreement between the incoming and Obama administrations on many key issues. It remains to be seen whether the Republican Party and new administration agree that key cybersecurity programs initiated by the Obama administration, such as the Cybersecurity Framework, have indeed been successful. In January 2017, the Center for Strategic and International Studies' task force on cyberpolicy, chaired by influential Republican congressman Michael McCaul, released a comprehensive set of recommendations for the Trump administration to strengthen cybersecurity. The task force noted that the Obama administration has made "uneven progress" on cybersecurity.(10)

Concerns have been expressed about the vagueness of Donald Trump's cybersecurity proposals.(11) It's been reported that the new president has indicated a preference for snail mail over emails for important communication.(12) This would indeed be desirable if the goal were to ensure the digital economy's security—but it ignores its growth.

A recommendation for the new administration is to work more closely with the international community. The US has found it especially challenging to address cybersecurity issues with large, powerful nations such as China and Russia. These nations pose the most severe threats to the US because of their technologically advanced research and economic and military powers. Russia–US relations have been particularly controversial on the cyberfront in recent years. Allegations and counterallegations have been persistent themes in the dialogues and discourses between the US and Russia regarding cybersecurity. In early January 2017, a bipartisan group of senators began work on a bill to impose sanctions against Russia in response to two Russian intelligence agencies' alleged cyberattack on Democratic National Committee computers.(13) These same attackers are believed to have been behind the 2015 cyberattacks on the White House, the State Department, and the Joint Chiefs of Staff.(14) Trump has attempted to deviate from the previous administration's views toward Russia, appearing motivated and willing to work with Russia to improve the relationship diplomatically.(15)

The Report underscores cybersecurity's importance and provides several useful recommendations and suggestions. One critique is that it could have gone further. For instance, it didn't deal with new technologies such as blockchain that might be critical to enhancing cybersecurity. Furthermore, the Report didn't sufficiently emphasize strengthening the government's organizational capacity and culture from a cybersecurity standpoint. Cybersecurity's increasing criticalness means that organizations will require separate divisions, departments, or subunits (similar to R&D, production, and marketing) to deal with this issue.

Acknowledgments

I thank Jeffrey Voas of NIST for his comments and edits on earlier versions.

References

1. "Report on Securing and Growing the Digital Economy," Commission on Enhancing National Cybersecurity, NIST, 1 Dec. 2016; www.nist.gov/sites/default/files/documents/2016/12/02

/cybersecurity-commission-report-final-post.pdf.

2. B. Obama, “Improving Critical Infrastructure Cybersecurity,” Executive Order 13636, *Federal Register*, vol. 78, no. 33, 19 Feb. 2013, pp. 11737–11744.

3. A.S. Kalra, “Why HR Directors’ Concerns about Tech Security Aren’t Unfounded,” HumanResources, 29 Sept. 2016; www .humanresourcesonline.net/hrdirectors-concerns-tech-security-arent-unfounded.

4. “3rd Cyberattack ‘Has Been Resolved’ after Hours of Major Outages: Company,” *NBC New York*, 21 Oct. 2016; www.nbcnewyork.com/news/local/Major-Websites-Taken-Down-by-Internet-Attack-397905801.html.

5. N. Perlroth, “Hackers Used New Weapons to Disrupt Major Websites across US,” *New York Times*, 21 Oct. 2016; www.nytimes.com/2016/10/22/business/internet-problems-attack.html?_r=0.

6. J. Stavridis and D. Weinstein, “The Internet of Things Is a Cyberwar Nightmare,” Foreign Policy, 3 Nov. 2016; foreignpolicy.com/2016/11/03/the-internet-of-things-is-a-cyber-war-nightmare/?utm_source=Sailthru&utm_medium=email&utm_campaign=New%20Campaign&utm_term=Flashpoints.

7. “Chinese Firm Says It Did All It Could Before Cyberattack,” *Columbia Daily Tribune*, 25 Oct. 2016; www.columbiatribune.com/business/chinese-firm-says-it-did-all-it-could-before-cyberattack/article_288688d3-7306-5eaf-b4a2-bb17f721d9da.html.

8. “China’s Xiongmai to Recall up to 10,000 Webcams after US Hack,” Channel NewsAsia, 25 Oct. 2016; www.channelnewsasia.com/news/technology/china-s-xiongmai-to-recall-up-to-10-000-webcams-after-us-hack/3234756.html.

9. B. Dickson, “Blockchain Could Help Fix IoT Security after DDoS Attack,” Venture Beat, 2016; venturebeat.com/2016/10/29/blockchain-could-help-fix-iot-security-after-ddos-attack.

10. M. Chalfant, “Task Force Urges Trump to Develop Better Cyber Deterrent,” *Washington Free Beacon*, 5 Jan. 2017; freebeacon.com/national-security/task-force-urges-trump-develop-better-cyber-deterrent.

11. T. Greene, “The Trump Effect on Cybersecurity: Tough to Tell,” Network World, 8 Dec. 2016; www.networkworld.com/article/3148295/security/the-trump-effect-on-cybersecurity-tough-to-tell.html.

12. “No Computer Is Safe, Use Snail Mail: Donald Trump,” *Deccan Chronicle*, 1 Jan. 2017; www.deccanchronicle.com/world/america/010117/no-computer-is-safe-use-snail-mail-donald-trump.html.

13. T. Kopan, “Lawmakers Preparing Russia Sanctions Bill,” CNN, 3 Jan. 2017; edition.cnn.com/2017/01/03/politics/russia-sanctions-senate.

14. “After the NSA Hack: Cybersecurity in an Even More Vulnerable World,” The Conversation, 18 Aug. 2016; theconversation.com/after-the-nsa-hack-cybersecurity-in-an-even-more-vulnerable-world-64090.

15. K. Ruiz, “‘Only Stupid People Don’t Want a Relationship with Russia’: Donald Trump Calls for Closer Ties with Russia in Twitter Rant Despite Ongoing Hacking Scandal,” *Daily Mail*, 7 Jan. 2017; www.dailymail.co.uk/news/ar ticle-4097982/Donald-Trump-calls-closer-ties-Russia-latest-Twitter-rant.html.