Cybersecurity in the Federal Government: Failing to Maintain a Secure Cyber Infrastructure

by Christine Lino

EDITOR'S SUMMARY

Since the first cyber-attack in 1988, online viruses have proliferated through personal, organizational and government computers worldwide with devastating consequences. Concern was raised in 1999 regarding potential effects on the nation's poorly protected nuclear weapons, and further reports have highlighted flaws in the country's information infrastructure that put national security, public safety and personal privacy at risk. A 2014 report revealed the alarming frequency of attacks on government systems and agencies, gaps in awareness and response and minimal disclosure. Software protections are often nonexistent, ineffective or simply unused and insufficient to match rapidly advancing technology. Lack of leadership, expertise, funding, time and other resources adds to the challenge. Creation and implementation of cybersecurity policy standards have been thwarted by conflict over public and private sector roles, capabilities and inaction, and compliance with existing standards is negligible and ineffective. Joint pressure from the public and government will be needed for meaningful action.

KEYWORDS

data security
national security
public policy
privacy
government agencies
computer crime

Christine Lino is a graduate student at Drexel University College of Information Science and Technology, concentrating in digital libraries. She currently works for the Department of Defense and deals primarily with personnel and information security. She can be reached at crl38<at>drexel.edu.

The North Atlantic Treaty Organization (NATO) manages *The NATO Review*, a free online magazine containing opinion and analysis on current international security threats and challenges. Cybersecurity is highlighted on the *NATO Review*'s website and includes a timeline titled, "The History of Cyber Attacks," that outlines the most significant and detrimental cyber-attacks throughout the world in the past 20 years. According to the timeline, the first significant cyber-attack was launched in 1988 and spread across many computers within the United States. The attack, labeled the "Morris Worm," exploited vulnerabilities in the UNIX system Noun 1 and had the ability to self-replicate and subsequently slow down computers, rendering them useless [1]. A decade later, in May of 2000, the "ILOVEYOU" virus spread like wildfire via an email transmission that prompted users to open an attachment. The action of opening the attachment triggered attack code, automatically forwarding the email virus to all contacts in the user's email contact list. Prior to this incident viruses sent via spam were rare; however, the ILOVEYOU virus changed the playing field by demonstrating how malware can send itself through spam and prey on human psychology [2]. The National Infrastructure Protection Center (NIPC) within the Federal Bureau of Investigation (FBI) was tasked with coordinating efforts with the private sector to collect data pertaining to possible cyber threats as well as sharing the information effectively. However, although the NIPC learned of the ILOVEYOU virus at 5:45 a.m. Eastern Standard Time, an alert was not disseminated until 11 a.m., after many federal agencies were hit [3]. Almost 12 hours after the delayed notification, guidance regarding remedying the damage was finally released. According to Willemssen's statement on behalf of the General Accounting Office, deficiencies in dealing with these

cyber threats were caused by multiple factors, including insufficient understanding of risks, technical staff shortages, slow response rates, poor security program management, lack of adequate technical expertise and lack of supporting policy and funding [3].

"Science at Its Best, Security at Its Worst," a report by the President's Foreign Intelligence Advisory Board, was the main focus of discussion during a meeting of the U.S. House Committee on Commerce in 1999. This report raised concerns that the country's most sensitive nuclear weapon laboratories and secrets, housed at the Department of Energy, were poorly protected [4]. Despite the risk awareness raised by this report, a year later the chief information officer of the Department of Energy admitted to the U.S. House Subcommittee on Government Management, Information and Technology that many of the same technical vulnerabilities still existed. In his statement the CIO compared cybersecurity to rocket science, stating that cybersecurity was more complex and "much more difficult than rocket science." [5, p. 116] The CIO went on to detail the importance of receiving funding and support for cross-government security initiatives to serve as a foundation for improvements in cybersecurity. Furthermore, reports from the General Accounting Office were presented during a hearing before the U.S. Senate Committee on Governmental Affairs in 2000 and revealed that the "nation's underlying information infrastructure is riddled with vulnerabilities which represent severe flaws and risks to our national security, public safety and personal privacy." [6] While these hearings are only a few of many held by Congress focusing on cybersecurity throughout different government agencies, they collectively highlight the federal government's inability to adequately protect against and respond to potential cyber-attacks over the past decade.

Since 1988 cyber-attacks have perpetuated, and many challenges faced in cybersecurity during the turn of the century are still problematic. While technology capabilities have grown by leaps and bounds, security measures and protocols are failing to keep pace with the rapidly changing field, often being rendered obsolete faster than new hardware and software can be released. In 2014 Senator Tom Coburn, ranking member of the Committee on Homeland Security and Government Affairs, released a report [7] revealing startling statistics regarding the government's failure to bring cyber threats under control. The report indicated that government systems were the target of 48,000 detected cyber incidents, along with countless more undetected ones. Additionally, civilian agencies only detect four out of 10 cyber intrusions, and with reporting to the public being even worse, the majority of attacks are unknown to the public except on the rare occasions when hackers publicize their exploits. While many different agencies are subject to these cyber-attacks, the common thread among them is that the intrusions typically prey on common and fixable weaknesses. These inlets into the systems are frequently a result of out-of-date software and failure to install software patches or update programs. These controllable shortcomings pose great risk to the federal government and result in costly losses in manpower hours, personal data and classified or other protected information.

Policy, Legislation and the Government vs. Private Sector Debate

Over the years legislation has fallen short in mitigating the threat of cyber-attacks by failing to implement standards for prevention, protocol for reporting intrusions, consequences for non-compliance or adequate funding for necessary personnel and resources. The last piece of legislation to be passed was the Federal Information Security Management Act of 2002, also known as the E-Government Act [8]. Since 2002 many failed attempts were made to update cybersecurity policy, including in 2012 when the U.S. Senate failed to pass the Cybersecurity Act of 2012 [9].

This failure is frequently attributed to differing opinions regarding the roles of government and the private sector in cybersecurity program and policy regulation and oversight. One side of the debate about government involvement holds that the private sector has not adequately implemented measures to protect themselves against cyber threats, warranting government involvement [11]. A study conducted by Dell surveyed global IT leaders and found that most believe the government can help create strategies to protect against cybersecurity threats. In fact, nearly 90% of those surveyed believe government involvement in developing cyber

defense strategies is necessary and view the government's role in protecting organizations against threats as positive. Only 17% believe the government hindered operational effectiveness in regards to security [12].

Those who oppose government involvement in cybersecurity management argue that the federal government is not sufficiently equipped to develop and enforce cybersecurity policy and regulations [10]. From an enforcement perspective, the federal government struggles with ensuring its own agencies comply with federal policy, and confidence is minimal that federal legislation would succeed on a broader scale. Coburn says, "None of the other agencies want to listen to Homeland Security when they aren't taking care of their own systems. They aren't even doing the simple stuff." [11] In the same *The Washington Post* article, Coburn describes another underlying problem as the inability of federal agencies to "hire top-notch information technology workers, pay them enough and give them enough clout to enforce routine security practices." Adding insult to the lack of confidence held in the government's abilities to manage the issues, the U.S. government has spent at least $65 billion since 2006 to implement tools to secure computers and networks; however, there seems to be little to no compliance with standards and no decrease in the vulnerabilities that exist and cyber-attacks that continue to happen [7, 12]. Both Democrats and Republicans voted against the Cybersecurity Act of 2012, with a shared concern being that the regulatory approach of the Cybersecurity Act would be ineffective and potentially harmful [13].

Following the Senate's failure to pass the Cybersecurity Act of 2012, the Obama administration began drafting Executive Order 13636, modeled on the Cybersecurity Act [14]. Issued in February 2013, "Improving Critical Infrastructure Cybersecurity" states "repeated cyber intrusions into critical infrastructure demonstrate the need for improved cybersecurity. The cyber threat to critical infrastructure continues to grow and represents one of the most serious national security challenges we must confront." The order also asserts that it is the policy of the government to "maintain a cyber-environment that encourages efficiency, innovation and economic prosperity while promoting safety, security, business confidentiality, privacy and civil liberties."

When analyzing the list of agencies, it is clear that the risk is not only to the nation's infrastructure, but also to the nation's citizens whose personal information is left unlocked for hackers to steal and use as they choose.

The order seeks to address a variety of cyber threats by expanding programs for information sharing and collaboration, establishing a process for identifying high priority infrastructure, requiring the National Institute of Standards and Technology (NIST) to create a cybersecurity framework of standards and best practices, and requiring agencies to determine adequacy and ability to address risks [15]. The importance of information sharing with private sector entities within the United States is paramount as it provides support and allows those entities to use the information from the federal government as a tool to better protect and defend their systems against similar cyber threats. To this end, the order directs the secretary of homeland security and the director of national intelligence to oversee timely production of unclassified reports for the private sector following individual cyber-attacks [14]. Not only does the executive order recognize the need to share information with the private sector, but it also reiterates the importance of creating and expanding programs that bring subject matter experts from the private sector into the federal service. The purpose of incorporating subject matter experts is to collaborate on identifying "content, structure, and types of information most useful to critical infrastructure owners and operators in reducing and mitigating cyber risks." [14]

A year after the release of Executive Order 13636, Coburn released the previously mentioned report that shed light on the actual and potential impact of significant breaches in cybersecurity on U.S. infrastructure. Such high-risk breaches have risked data pertaining to the nation's weakest dams, plans for nuclear plants and blueprints for the technology undergirding the New York

CONTENTS | TOP OF ARTICLE | < PREVIOUS PAGE | NEXT PAGE > | NEXT ARTICLE >

Stock Exchange [7]. Multiple agencies, including the Departments of Homeland Security, Justice, Defense, State, Labor, Energy, Commerce, NASA, EPA, the Office of Personnel Management and others, were cited as offenders that fail to secure data pertaining to the safety and security of the nation. When analyzing the list of agencies, it is clear that the risk is not only to the nation's infrastructure, but also to the nation's citizens whose personal information is left unlocked for hackers to steal and use as they choose.

One of the most disturbing findings of Coburn's report is that the Department of Homeland Security was tasked in 2010 by the Obama administration to lead efforts to secure computers across the federal government, yet research revealed that, like many other agencies, the department still experiences similar shortcomings in updating and maintaining a secure infrastructure. Furthermore, it was determined that the Department of Homeland Security rated below the government-wide average for compliance with properly using anti-virus software and other security measures, including security awareness trainings. Another startling example includes shortcomings found at the Nuclear Regulatory Commission, which maintains sensitive data on nuclear facilities, design and plans for all nuclear reactors and waste storage facilities, and information on design and process of nuclear material transports. Coburn's report detailed issues including perceived ineptitude of NRC technology experts, sensitive data stored on unsecured shared drives, failure to report security breaches and inability to keep track of computers.

The Way Ahead

Following Coburn's report publication, NIST issued "Framework for Improving Critical Infrastructure Cybersecurity," as directed by Executive Order 13636 [16]. The purpose of the framework is to create "a set of industry standards and best practices to help organizations manage cybersecurity risks." [16. p. 1] The government and private sector collaborated on creating this guidance, consisting of the "Framework Core, Profile, and Implementation Tiers" to address and manage cybersecurity risk in a cost-effective way. The framework also includes parameters for organizations and agencies to follow in developing procedures for protecting the privacy and civil liberties of U.S. citizens while carrying out cybersecurity activities. The private sector and NIST recognize that there is no one-size-fits-all approach and therefore the framework will be a living document that will continue to be improved and updated, based on feedback, evolving threats and new solutions. The framework is also generic and not industry- or country-specific, allowing organizations of different types and countries to adopt the framework to strengthen their own cybersecurity efforts.

According to a 2013 Congressional Research Service report [15], cybersecurity threats and consequences to U.S. infrastructure and high-value assets continue to be a concern in our nation. However, risks have long been known and largely swept aside as agencies continue to fail to comply with basic information security practices. There is no shortage of information available from government and private and public resources that have researched and reported on the existing and potential cybersecurity threats, yet much of the public, including those directly affected, are inadequately informed. While the number of hearings, research reports and failed legislation is plentiful, laws and best practices are lacking and not enforced sufficiently. Collaboration between private and government sectors and professionals may increase the likelihood of passing future legislation on the topic and may convince many agencies to commit the necessary time, personnel and resources to properly securing our nation's infrastructure against the risk of cyber threats. ■

Resources on next page

Resources Mentioned in the Article

[1] The history of cyber attacks – A timeline. (2013). *NATO Review Magazine*. Retrieved from www.nato.int/docu/review/2013/Cyber/timeline/EN/index.htm

[2] Ward, M. (May 4, 2010). A decade on from the ILOVEYOU bug. *BBC News*. Retrieved from www.bbc.com/news/10095957

[3] H.R. 4246: *Cyber Security Information Act of 2000*. Hearings before the Subcommittee on Government Management, Information, and Technology of the House Committee on Government Reform, 107th Cong. (2000) (comments by Joel C. Willemsen). Retrieved from www.gpo.gov/fdsys/pkg/GAOREPORTS-T-AIMD-00-229/pdf/GAOREPORTS-T-AIMD-00-229.pdf

[4] *The Rudman report: Science at its best, security at its worst.* Hearing before the House Committee on Commerce, 106th Cong. (1999). Retrieved from www.gpo.gov/fdsys/pkg/CHRG-106hhrg58514/pdf/CHRG-106hhrg58514.pdf

[5] *Computer security report card.* Hearing before the Subcommittee on Government Management, Information, and Technology of the House Committee on Government Reform. 106th Cong. (2000). Retrieved from www.gpo.gov/fdsys/pkg/CHRG-106hhrg74495/pdf/CHRG-106hhrg74495.pdf

[6] *Cyber attack: Is the government safe?* Hearing before the Senate Committee on Governmental Affairs, 106th Cong. (2000). Retrieved from www.gpo.gov/fdsys/pkg/CHRG-106shrg63639/pdf/CHRG-106shrg63639.pdf

[7] *The federal government's track record on cybersecurity and critical infrastructure.* (February 4, 2014). A report prepared by the U.S. Senate, Committee on Homeland Security and Government Affairs, Minority Staff, Sen. Tom Coburn Ranking Member. Retrieved from www.coburn.senate.gov/public/index.cfm?a=Files.Serve&File_id=f1d97a51-aca9-499f-a516-28eb872748c0

[8] E-Government Act of 2002, Pub. L. no. 107-347, 112 Stat 2681-749. (2002). Retrieved from www.gpo.gov/fdsys/pkg/PLAW-107publ347/content-detail.html

[9] Cybersecurity Act of 2012, S. 2105, 112th Congress (2012) Retrieved from http://beta.congress.gov/112/bills/s2105/BILLS-112s2105pcs.pdf

[10] Rosenzweig, P. (May 24, 2012). *The alarming trend of cybersecurity breaches and failures in the U.S. government.* The Heritage Foundation. Retrieved from www.heritage.org/research/reports/2012/05/the-alarming-trend-of-cybersecurity-breaches-and-failures-in-the-us-government

[11] Timberg, C., & Rein, L. (February 4, 2014). Senate cybersecurity report finds agencies often fail to take basic preventive measures. *The Washington Post.* Retrieved from www.washingtonpost.com/business/technology/senate-cybersecurity-report-finds-agencies-often-fail-to-take-basic-preventive-measures/2014/02/03/493390c2-8ab6-11e3-833c-33098f9e5267_story.html

[12] Malykhina, E. (February 26, 2014). Government cybersecurity guidance wanted by private sector. *InformationWeek.* Retrieved from www.informationweek.com/government/cybersecurity/government-cybersecurity-guidance-wanted-by-private-sector/d/d-id/1113999

[13] Rosenzweig, P. (November 13, 2012). The alarming trend of cybersecurity breaches and failures in the U.S. government continues. The Heritage Foundation. Retrieved from www.heritage.org/research/reports/2012/11/cybersecurity-breaches-and-failures-in-the-us-government-continue

[14] Exec. Order No. 13636: Improving critical infrastructure cybersecurity (2013). Retrieved from www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

[15] Fischer, E. A., Liu, E. C., Rollins, J. & Theohary, C. A. (March 1, 2013). The 2013 cybersecurity Executive Order: Overview and considerations for Congress. (CRS Report No. R42984). Washington, DC: U.S. Library of Congress, Congressional Research Service. Retrieved from http://fpc.state.gov/documents/organization/206157.pdf

[16] National Institute of Standards and Technology. (February 12, 2014). *Framework for improving critical infrastructure cybersecurity.* U.S. Department of Commerce. Retrieved from www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf