CIS® Center for Internet Security®

31 Tech Valley Drive
East Greenbush, NY 12061 USA
518.266.3460
www.cisecurity.org

Testimony of John Gilligan
Chief Executive Officer
Center for Internet Security
Hearing on Private Sector Data Breaches
Permanent Subcommittee on Investigations
Homeland Security & Government Affairs Committee
United States Senate
106 Dirksen Senate Office Building
Washington, DC
Thursday, March 7, 2019
10:00 a.m. ET

Chairman Portman, Ranking Member Carper, and members of the Subcommittee, thank you for inviting me today to this hearing. My name is John Gilligan, and I serve as the Chief Executive Officer of the nonprofit Center for Internet Security, Inc. (CIS). I have spent most of my career in service to the Federal government, including serving as the Chief Information Officer of both the U.S. Department of Energy, and the U.S. Air Force. I appreciate the opportunity today to share our thoughts on the current state of national cybersecurity, focusing on an area we know well: cyber defense. I look forward to offering our ideas on how we can collectively build on the progress being made in this important area of critical national security.

In short, we will: (1) introduce you to CIS and the Critical Security Controls; (2) identify general trends and root causes of recent cyber-attacks; and (3) explain how the CIS Critical Security Controls can help private—and public—sector organizations implement what we call "effective cyber defense". I will close with some recommendations.

About CIS and the CIS Critical Security Controls

Established in 2000 as a nonprofit organization, the Center for Internet Security's (CIS') primary mission is to advance cybersecurity readiness and response. CIS was instrumental in establishing the first guidelines for security hardening of commercial IT systems at a time when there was little online security leadership. Today, CIS works with the global security community using collaborative deliberation processes to define security best practices for use by government and private-sector entities. The approximately 200 professionals at CIS provide cyber expertise in three main program areas: (1) the Multi-State and more recently the Elections Infrastructure Information Sharing and Analysis Center, the MS-ISAC and EI-ISAC respectively; (2) the CIS Benchmarks; and (3) the CIS Critical Security Controls. I describe each briefly below.

MS-ISAC[1]. In 2010, the U.S. Department of Homeland Security (DHS), under the then-National Protection and Programs Directorate (NPPD), partnered with CIS to host the MS-ISAC, which has been designated by DHS as the focal point for cyber threat prevention, protection, response, and recovery for the nation's state, local, tribal, and territorial (SLTT) governments as well as all 79 Fusion Centers nationwide. MS-ISAC members include all 56 states and territories and more than 5,000 other SLTT government entities. MS-ISAC's 24x7 cybersecurity operations center provides: (1) cyber threat intelligence that enables MS-ISAC members to gain situational awareness and prevent incidents, consolidating and sharing threat intelligence information with the DHS National Cybersecurity and Communications Information Center (NCCIC); (2) early warning notifications containing specific incident and malware information that might affect them or their employees; (3) incident response support; and (4) various educational programs and other services. Furthermore, MS-ISAC provides around-the-clock network monitoring services with our so-called 'Albert' network monitoring devices for many SLTT networks, analyzing over one (1) trillion event logs per month. Albert is a cost-effective Intrusion Detection System (IDS) that uses open source software combined with the expertise of the MS-ISAC 24x7 Security Operations Center (SOC) to provide enhanced monitoring capabilities and notifications of malicious activity. In 2018, MS-ISAC analyzed, assessed, and reported on over 56,000 instances of malicious activity to over 4,000 MS-ISAC members.

EI-ISAC[2]. In 2018 CIS was tasked by DHS to stand up an information sharing and analysis center focused on the Nation's elections infrastructure. Leveraging the experience gained through the MS-ISAC, CIS established the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC). The EI-ISAC is now fully operational with all 50 states participating and over 1500 total members, including elections vendors. The EI-ISAC provides elections officials and their technical teams with regular updates on cyber threats, cyber event analysis, and cyber education materials. During the 2018 primaries and mid-term elections the EI-ISAC hosted the National Cyber Situational Awareness Room, an on-line collaboration forum to keep elections officials aware of cyber and non-cyber incidents and potential cyber threats. More than 600 elections officials participated in these forums. Moreover, CIS was processing data from 135 Albert sensors monitoring the networks, which supported on-line elections functions such as voter registration and election night reporting. The Albert sensors processed 10 petabytes of data during 2018, resulting in over three thousand actionable notifications to elections offices.

CIS Benchmarks. CIS is also the world's largest producer of authoritative, community-supported, and automatable security configuration benchmarks and guidance. The CIS Security Benchmarks (also known as "configuration guides" or "security checklists") provide highly detailed security setting recommendations for a large number of commercial IT products, such as operating systems, data base products and networking systems. These benchmarks are vital for any credible security program. The CIS Security Benchmarks are developed though a collaborative effort of public and private sector security experts. Over 200 consensus-based Security Benchmarks have been

[1] : Find out more information about the MS-ISAC here: https://msisac.cisecurity.org/. List of MS-ISAC services here: https://www.cisecurity.org/wp-content/uploads/2018/02/MS-ISAC-Services-Guide-eBook-2018-5-Jan.pdf

[2] A list of EI-ISAC services can be found here: https://www.cisecurity.org/ei-isac/ei-isac-services/

developed and are available in PDF format free to the general public on the CIS or NIST web sites. An automated benchmark format along with associated tools is also available through the purchase of a membership. CIS has also created a number of security configured cloud environments, called 'hardened images' that are based on the benchmarks that we are deploying in the Amazon, Google, and Microsoft cloud environments. These hardened images help ensure that cloud users can have confidence in the security provided within the cloud environment they select. The CIS hardened images are used worldwide by organizations ranging from small, nonprofit businesses to Fortune 500 companies.

The CIS Security Benchmarks are referenced in a number of recognized security standards and control frameworks, including:

- NIST Guide for Security-Focused Configuration Management of Information System
- Federal Risk and Authorization Management Program (FedRAMP) System Security Plan
- DHS Continuous Diagnostic Mitigation Program
- Payment Card Industry (PCI) Data Security Standard v3.1 (PCI) (April 2016)
- CIS Critical Security Controls

CIS Controls[3]. CIS' third program is most applicable to today's hearing topic. In 2015, CIS became the home of the CIS Critical Security Controls, previously known as the SANS Top 20, the set of internationally-recognized, prioritized actions that form the foundation of basic cyber hygiene or essential cyber defense. They are developed by an international consensus process and are available free on the CIS web site. The Critical Security Controls or just the CIS Controls have been assessed as preventing up to 90% of pervasive and dangerous cyber-attacks[4]. The CIS Controls act as a blueprint for system and network operators to improve cyber defense by identifying specific actions to be done in a priority order—achieving the goals set out by the NIST Cybersecurity Framework (CSF). Moreover, the CIS Critical Security Controls are specifically referenced in the NIST CSF as one of the tools to implement an effective cyber security program[5].

General Trends and Root Causes of Recent Cyber Attacks

In cybersecurity, there are no silver bullets. We must start with the basics. Fortunately, most methods of attacks are well known, as are basic defenses to these attacks. Basic cyber hygiene remains a critical solution to improving American cyber defenses, and the CIS Controls remain a clear, actionable, and free blueprint to implementation of what we call 'essential cyber defense'. Others use the term 'basic cyber

[3] Find out more information about the CIS Controls and download them for free here: https://www.cisecurity.org/critical-controls.cfm

[4] Up to 91% of all security breaches can be auto-detected when release, change and configuration management controls are implemented. IT Process Institute: https://www.sans.org/cyber-security-summit/archives/file/summit-archive-1533052750.pdf

[5] NIST Framework, Appendix A, page 20, and throughout the Framework Core (referred to as "CCS CSC"—Council on Cyber Security (the predecessor organization to CIS for managing the Controls) Critical Security Controls)

hygiene'. As noted above, deploying the top five CIS Critical Security Controls can reduce up to 90 percent of known pervasive and dangerous cyber-attacks.[6]

It is also important to note that good information technology (IT) operations (systems and network management) go hand-in-hand with good security. The foundation of good security is good IT management: knowing what you have, how it is configured, when things change, and what can change or bypass security settings. Security considerations begin with your IT operations infrastructure, not a separate security infrastructure. As CIO of the Air Force, I found that by implementing benchmark compatible operating system configurations and tools to ensure that the configurations were not modified resulted in improved security, better operational availability, and reduced costs. The cost reductions were the result of the need for fewer systems and network administrators. The CIO of the State of Arizona has documented similar cost reduction experiences.[7] The point here is that, contrary to common perception, better security can often cost less rather than better security resulting in increased costs.

Specific Examples of Breach Causes Tracked to the CIS Controls

Overall, 2018 brought the second-highest number of reported data breaches of any year on record. More than 6,500 publicly disclosed breaches and over 5 billion records exposed. We have seen more big data breaches, ransomware, and critical infrastructures hacked.[8] CIS has analyzed the data for breaches where the root cause has been made public and has found that in each case the root cause related to the failure to properly implement one or more of the CIS Controls. In essence, the root cause of these breaches is the failure to exercise basic cyber hygiene or essential cyber defense. Despite having the concept of the Controls around for a decade, we find that organizations are not implementing the basic hygiene/basic cyber defense.

Many organizations collect and retain large quantities of personally identifiable information (PII) about American citizens or other sensitive data. Any party that handles our PII has the responsibility to do their utmost to protect it. The CIS Controls establish the technical actions that must be implemented to provide basic security. In the Equifax breach, those include:

> CIS Control 2: Understand and control what software is running. (And be doubly certain if it is the software that handles or protects sensitive data.)
>
> CIS Control 3: Know what your critical software is and ensure that you have kept up to date on patches. (If there is a known vulnerability, patch it)
>
> CIS Control 6: Audit everything, centralize the audit records, and analyze them. (At a minimum, collect enough data so forensics experts can make full sense of it and help everyone else discover

[6] https://www.sans.org/cyber-security-summit/archives/file/summit-archive-1533052750.pdf
[7] http://www.govtech.com/blogs/lohrmann-on-cybersecurity/how-does-arizona-government-address-information-security.html

[8] https://pages.riskbasedsecurity.com/2018-ye-breach-quickview-report

and prevent similar attacks.)

CIS Control 9: Limit and control network ports, protocols and services (Operate critical services on separate devices. That makes it easier to see malicious actions. You can see if the attackers exfiltrated data? Did they open ports? Was there a host-based firewall?)

CIS Control 12: Defend the boundaries of your network. (Was traffic to and from the compromised devices being inspected? Did a server initiate an unexpected connection?)

CIS Control 14: Control access based on need to know. (Complexity is the cover used by attackers. Did Equifax segment its network so that critical business functions with user's data could be monitored more closely for anomalies?)

While NotPetya was world-wide in scope [Maersk, Merck, UK National Health System] even a sophisticated attack such as this one consists of numerous individual steps, many of which would have been detected, blocked, or prevented by a series of defensive actions that are found in a subset of the CIS Critical Security Controls. For example, there are CIS Controls that require visibility of all of the hardware and software on the network; removal of outdated, un-securable software; timely patching for known vulnerabilities; and separation of the network into sensitive and less-sensitive areas. There are also CIS Controls to ensure that plans are in place for recovery in case of a security breach. These critical security controls would have prevented, blocked, or managed the effects of the NotPetya attack at multiple cost-effective points.

In the recent Marriott case involving a data breach impacting approximately 500 million customers, a guest registration database from its Starwood properties had been compromised in 2014 — a full two years before Marriott purchased Starwood. Although the specific root causes of the attack have not been made public, based on analysis of other breaches the root causes will likely track to a failure to properly implement one or more of the CIS Controls. *Forbes* recently recommended that a thorough cybersecurity audit should be a part of any company's mergers and acquisitions due diligence process.[9] Our recommendation is that the CIS Controls be an element in this cyber due diligence process.

Leveraging the CIS Critical Security Controls to Reduce Cyber Attacks

The CIS Controls are especially effective because they are regularly updated by a global network of cyber experts based on actual attack data derived from a variety of public and private threat sources. The Controls help deal with what has sometimes been referred to as "the Fog of More,"—the confusion facing many organizations trying to sort through the many volumes of guidelines and frameworks as well as the constant barrage of marketing from cyber product companies. In essence, the Controls help organizations by cutting through the "fog" by providing a concise set of specific technical actions that track to the common attack patterns so individual organizations do not have to be capable of doing a sophisticated risk

[9] Forbes, March 1, 2019: https://www.forbes.com/sites/forbestechcouncil/2019/03/01/do-you-do-security-due-diligence-before-a-merger-or-acquisition/#5ae78a024535

assessment, the typical starting point of cyber risk frameworks such as the NIST CSF, as well as standards from the Payment Card Industry (PCI), the International Standards Organization (ISO), and the Institute of Electrical and Electronics Engineers (IEEE).

The *California Data Breach Report* (2016)[10], released by then-Attorney General Harris, established the world's first de facto minimum level of information security by warning that failing to implement all relevant Controls "constitutes a lack of reasonable security." Since then, other public organizations have followed California's lead. The State of Ohio also recently established the CIS Controls as the standard for cyber defense within the state.[11] The Republic of Paraguay has also mandated compliance with the Controls for government systems.[12] ETSI, the European Standards Organization, has adopted the CIS Controls as its standard for cybersecurity.[13] The Aerospace Industries Association (AIA) recently published their cybersecurity guidelines, which are based on the CIS Controls.[14] The Atlantic Council has also endorsed the Controls. [15]

We are encouraged that many organizations are catching on to the value of the CIS Controls. Security providers have also endorsed the Controls. Symantec, Verizon, and Tripwire have all identified the Controls as being the foundation for effective cyber defense. [16] [17] [18]

There is also a need to improve cybersecurity in the Federal government. CIS has been involved with knowledge sharing with the Government Accountability Office on aspects of the cybersecurity of elections infrastructure as well as discussions to improve the evaluation of the state of cybersecurity in the Federal government. We are also involved in discussions regarding the cloud computing policy of the U.S. Department of Defense.[19]

Possible Congressional Actions for Helping Prevent Future Cyber Breaches

As the U.S. Congress continues to consider the best ways to improve cybersecurity in the U.S., we respectfully offer our perspectives and our expertise to you as you determine how best to encourage the increased use of basic cyber hygiene and the adoption of voluntary best practices.

We start with the recognition that the NIST's Cybersecurity Framework is an excellent guidance document and serves as the top-level framework for addressing cyber security within the United States.

[10] Report here: https://oag.ca.gov/sites/all/files/agweb/pdfs/dbr/2016-data-breach-report.pdf) (see Recommendation 1).

[11] https://www.arentfox.com/perspectives/alerts/ohio-passes-first-safe-harbor-law-incentivizing-cybersecurity-controls

[12] http://www.cert.gov.py/index.php/guias-de-seguridad (Google will translate)

[13] http://www.etsi.org/deliver/etsi_tr/103300_103399/10330501/02.01.01_60/tr_10330501v020101p.pdf

[14] http://www.aia-aerospace.org/wp-content/uploads/2018/12/AIA-Cybersecurity-standard-onepager.pdf

[15] http://publications.atlanticcouncil.org/cyberrisks/risk-nexus-september-2015-overcome-by-cyber-risks.pdf

[16] https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf, pages 75-77

[17] Verizon's 2015 Data Breach Verizon DBIR 2015, page 55

[18] http://www.tripwire.com/state-of-security/featured/20-csc-list-post/

[19] Department of Defense Cloud Computing Security Requirements Guide, Version 1, Release 3, 6 March 2017. (search on 'CIS Benchmarks')

However, by design, the NIST Framework was developed at a general level and within the Framework it points to other, more detailed standards and best practices for specific implementation guidance (including the Critical Security Controls). While a logical construct, this approach has some unintended consequences. In particular, government and private sector organizations who wish to implement the NIST Framework must select for implementation from among very comprehensive lists of standards and best practices that are referenced in the Framework. As noted earlier, this contributes to the "fog of more"—organizations struggling to select the appropriate implementation guidance.

This same problem is magnified for organizations that are required to comply with multiple frameworks. Financial organizations are required to certify against the Payment Card Industry (PCI) framework. Organizations with international presence are often required to follow International Standards Organization (ISO) cybersecurity frameworks. These, and other frameworks have the same unintended consequence as the NIST Cybersecurity Framework. They are excellent high-level guidelines, but lack specificity regarding specifically what security controls should be implemented and in what priority. Working with state and local governments in operating the MS-ISAC, we see the enormous complexity resulting from the requirement to comply with frameworks specified by different Federal, State or domain policies. While the individual policies and regulations are well intended, they are contributing to much confusion and inefficiency in achieving the common goal of basic cyber defense.

Recognizing that our multiple cybersecurity frameworks and duplicative policies have contributed to a real "fog of more" for U.S. organizations, we would recommend that Congress help move the Nation to a solution. Specifically, we recommend that NIST be chartered to develop a single implementation guideline that can be used to satisfy the requirements of the NIST Framework, PCI, ISO, IEEE, and others similar general frameworks. This implementation guideline, we believe, should provide clear guidance on what constitutes cyber hygiene (or essential cyber defense) and recommendations regarding the prioritization of implementation of security controls. We note that the United Kingdom and Australia have done exactly this with the Australian Signals Directorate's Essential Eight (controls) [20] and the United Kingdom National Cyber Security Center's Cyber Essentials. [21]

CIS recently parsed the Critical Security Controls into three 'Implementation Groups' to assist organizations in phasing the implementing the Controls. The Implementation Groups provide a step-by-step path to achieving effective defense against the most common cyber-attack patterns. Implementation Group 1 consists of 43 detailed, technical subcontrols that address the most frequent attacks and are relatively straightforward to implement. We would recommend that Implementation Group 1 or an equivalent be established as the National Cyber Baseline for all organizations who could assess their compliance. In this way, senior leaders in public and private organizations, Congress, and the American public can have an objective basis for measuring the ability of organizations to withstand expected cyber-attacks.

[20] https://acsc.gov.au/infosec/mitigationstrategies.htm
[21] https://www.cyberessentials.ncsc.gov.uk/2017/11/27/a-brief-history-of-cyber-essentials

Conclusion

We recognize that the cybersecurity problem is a hard one, and one that continues to evolve. However, we also know how to prevent the majority of cyber-attacks. The CIS Critical Security Controls is a proven example of a way to prevent these attacks. We encourage Congress to recognize the current “fog of more” that is inhibiting our progress in implementing effective cyber defense and to require that a technically oriented baseline for cyber defense be established and implemented. We offer the Critical Security Controls as a point of departure or a model for such an effort.

Attachments A: Biography of John Gilligan

John M. Gilligan
President and Chief Executive Officer
CIS (The Center for Internet Security, Inc.)

John Gilligan became the President and Chief Executive Officer of CIS (The Center for Internet Security, Inc.) in October of 2018. He served on CIS' Board of Directors from 2005 – 2018 and was Chairman of the Board from 2009 – 2018.

Gilligan has more than 25 years of managerial experience in leading large organizations with expertise in cybersecurity, business strategy, organizational innovation, and program implementation. He served as President and COO of the Schafer Corporation from May 2013 until May 2017. Prior to Schafer Corporation, he was the President of Gilligan Group, a Virginia based IT and cyber consulting firm. Before founding the Gilligan Group, Gilligan was a Senior Vice President and Director, Defense Sector, at SRA International, Inc.

Gilligan served as the Chief Information Officer for the United States Air Force and the U.S. Department of Energy. Gilligan's government experience includes working as the Program Executive Officer (PEO) for Command and Control Battle Management Operations for the United States Air Force. He was a member of the Cyber Security Commission (formed to advise the 44th President) and has served as an advisor to the Office of the Secretary of Defense on IT reform.

In addition to his work with CIS, Gilligan is currently on the boards of the Software Engineering Institute, Isobar Inc., and the Armed Forces Communications and Electronics Association. He currently co-chairs the Cyber Committee of the Armed Forces Communications and Electronics Association (AFCEA). Gilligan has also served as Chairman of the boards of directors for Cyber Griffin Inc., Schafer Corporation, and HDT Global Inc.

Gilligan's published work on cybersecurity includes CIS' A Handbook for Elections Infrastructure, The Economics of Cybersecurity Part I: A Practical Framework for Cybersecurity Investment and The Economics of Cybersecurity Part II: Extending the Cybersecurity Framework. The last two publications were coordinated via the AFCEA International's Cyber Committee.