Government Business Council

FORCEPOINT
POWERED BY Raytheon

Security in the Golden Age of Cybercrime

An Exploration of Network Cybersecurity in the Federal Government

The American public remains skeptical about the federal government's cybersecurity capabilities: according to a 2016 survey by the Pew Research Center, less than half of all respondents were somewhat or very confident in the ability of the government to protect its data.[1]

The unprecedented scale and intricacy of today's threat environment — combined with a vast set of network solutions — make it more difficult for IT professionals to overcome security obstacles. Successfully managing more robust adversaries will require deftness, creativity, and flexibility; a goal made more challenging by a cumbersome regulatory environment.

> "Not having a cloud strategy creates a significant risk that organizations may deploy systems and expose Federal tax information with no assurance that the systems meet Federal guidelines."

Still, resourceful actions by some agencies demonstrate that the federal government might effectively meet future threats. To shed more light on the matter, Government Business Council (GBC) looked into the top five network security issues currently facing federal IT managers.

Issue #1: Navigating the Cyber Minefield

Today's cyber threat landscape includes state-led hacks, ransomware, insider threats, distributed denial-of-service (DDoS) attacks, and social engineering. These components link conventional financial criminals and nefarious computer experts in new, unpredictable ways.[2] [3]

The removal of many of the barriers that previously thwarted cybercriminals (e.g., the difficulty of inter-actor coordination) and the growth of incentives that bring new actors into the digital larceny underworld (e.g., the promise of remarkable compensation) have propped up a robust marketplace for cybercrime. The Justice Department's Computer Crime and Intellectual Property Section (CCIPS) reports that more than 4,000 daily ransomware attacks took place in 2016 — a three-fold increase compared to 2015. Another study finds that approximately 18 million new malware samples were captured in Q3 2016.[4] [5]

State sponsored attacks are a worrisome threat as well. Flashpoints like the BadRabbit/NotPetya Ransomware attack in October 2017, which experts have attributed to Russian actors, have caused disruption in both government and industry functions that few experts predicted.[6] [7] Along with these threats, the success of perpetrators in targeting and breaching vital systems is forcing federal IT security professionals to reevaluate critical infrastructures and their susceptibility to new adversaries.[8] [9]

Issue #2: Protecting Cloud Assets

Agencies are migrating applications to the cloud at an increasing rate as pressure mounts to consolidate and optimize existing data centers.[10] Cloud capabilities have tremendous promise for enhancing agencies' business operations, but the transition from on-premise data management to cloud-enabled third-party services has created functional and security-related challenges for federal IT managers.[11] [12]

These security-related challenges can take many forms — application or service compliance and performance monitoring, integration of enterprise application capabilities, and configuration management are a few key examples.[13] Equally diverse are the ways in which these challenges can impact IT modernization and even organizational mission success — a recent report published by the Treasury Inspector General for Tax Administration (TIGTA) describes how the Internal Revenue Service (IRS) has been undermined by its own cloud shortcomings: "Not having a documented enterprise-wide cloud strategy creates a significant risk that organizations […] may potentially expose Federal tax information [as well as] miss the opportunity to deliver public value by increasing operational efficiency and responding faster to constituent needs."[14] The report also describes some of the chief causes for these missed opportunities, citing the failure of the IRS to utilize the FedRAMP protocols to "conduct risk assessments, perform security authorizations, and grant Authorities to Operate for cloud services."[15]

The recent American Technology Council report "Report to the President on Federal IT Modernization" outlines some other cloud-specific challenges: "[Agencies must prioritize] consolidating and improving acquisition of network services so that management of security services for networks are… managed to high standards."[16] By improving acquisition and implementation, the report argues, agencies can "provide centralized capabilities that replace or augment existing agency-specific technology to improve both visibility and security."[17]

Forcepoint's Perspective

Sponsored Content

As many federal IT managers know, network security is not a niche technological issue – it is a key mission objective inextricably tied to national security. Recent attacks have ravaged agencies and exposed troubling vulnerabilities. Sometimes, it can seem like cybercriminals are winning the digital tug-of-war.

Through decades of private and public sector experience – and through original research conducted at Forcepoint Security Labs – we have fine-tuned a human-centric approach to cybersecurity. As the highest ranked for security effectiveness in NSS Labs' 2017 NGFW and NGIPS Tests, and as one of just two Visionaries in Gartner's 2017 Enterprise Network Firewall Magic Quadrant, we understand what it takes to protect the most vulnerable operations at our nation's most critical organizations.

Forcepoint NGFW – our scalable and centrally managed next-generation firewall – is at the forefront of network security technology. Combined with Forcepoint Security Management Center and our integrated application level proxy, Forcepoint NGFW currently serves as the foundation to many agencies' cyber defenses, and is the key to efficient and effective threat prevention.

Solutions that are centered on point product-based approaches and pay little mind to evolving data needs continue to miss the mark: the biggest opportunities for compromising federal networks lie at the human point. This is why Forcepoint couples its advanced intrusion detection and prevention with multi-ISP connectivity, and employs a security strategy based on insights into user behavior.

All of our tools – starting with NGFW and extending through the entire suite – are built with an understanding of the organizations' user rhythms and the flow of their enterprise data. Without this key knowledge, cyber defense is an uphill battle.

Ensuring the security of cloud-based applications has been a top priority of the federal government, and there has been early success in efforts to secure data, applications, and systems. Still, the ongoing efforts of government-wide entities show there is work to be done – individual agencies will be pivotal in shaping their network security destinies when it comes to new technologies.

Issue #3: Security in the IoT Era

Like cloud applications, the devices making up the Internet of Things (IoT) — sensors, drones, smart meters, etc. — present their own set of challenges.[18] In a May 2017 report, the Government Accountability Office (GAO) outlined security risks associated with the proliferation of IoT devices in federal agencies, raising concerns about the collection of information previously left unquantified, and calling out the hundreds of thousands of weakly-secured IoT devices that were "accessed and hacked" in 2016.[19] Protecting a network from penetration requires a toolkit that harmonizes with operating systems, device specifications, and policies designed to reduce human error.[20]

Given that many of the vulnerabilities plaguing IoT devices stem just as commonly from misuse as they do from technical flaws, a modern or 'next-gen' network security plan should also consider cyber hygiene, and not just within the context of insider threats. In May 2017, the Department of Homeland Security (DHS) Science & Technology Directorate presented an important lesson for maintaining security in a dynamic device environment: "Federal government mobile device users may be targeted with additional threats simply because they are public-sector employees." DHS emphasized that the response will require "active participation by the Federal government in key mobile-related standards bodies and industry associations."[21]

IoT devices present opportunities to many federal agencies by broadening the government's ability to deliver services and dedicate resources to mission-critical functions, and the collection of information from previously inaccessible sources.[22] [23] However, these opportunities also introduce larger and more complex security threats. A 2017 Government Accountability Office (GAO) report published a list of some, enumerating vulnerabilities like supply chain threats, upgrade deficiencies, and the risk of unauthorized communication with IoT devices.[24]

The federal government is still grappling with the nascent development of IoT security; legislators are deliberately approaching today's security frontier, having recently submitted a bill that introduces a number of best practices borrowed from other device and application contexts (e.g., functional patchability and modifiable passwords).[25] [26] And the recently introduced Internet of Things (IoT) Cybersecurity Improvement Act of 2017 makes needed progress, but the timeline for achieving tangible milestones remains unclear.[27]

Issue #4: Choosing the Right Tool

Some of the challenges IT managers face are internal, though they are impacted by external developments like the growing number of endpoints and opportunities for a federal network to be breached. One example is the procurement of network security tools and services — typically just the first step in a longer process, but a step that has become increasingly complicated in recent years.

Part of the challenge is the sheer quantity of options — today's managers are reaping the benefit of unprecedented technological innovation, but are also dealing with expansive 'shopping lists', seemingly countless vendors, and greater diversity in network security features. According to the Council on Foreign Relations (CFR), technological innovation is making information and communications technology supply chains more complex, which subsequently bogs down the acquisition of cybersecurity tools intended to protect these supply chains.[28] To mitigate existing and potential future damage from these complications, CFR recommends following the example of NIST to "support the development and voluntary adoption of industry-driven standards."[29] Taking note of the development in both security technology and threat nuance, the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) at DHS has prepared a strategic plan for federal government and critical infrastructure providers to adequately defend against cyber threats, laying out the importance of "specific countermeasures implemented in layers to create an aggregated, risk-based security posture" as the overarching strategy.[30]

Another hurdle managers are expected to overcome is the age-old but pernicious issue of staffing. Federal organizations today have a greater range of IT support options — maintaining a robust in-house team, acquiring support through vendor services, or leveraging government-provided assistance like the consulting services provided by ICS-CERT — but must also deal with the corollary decisions — preserving as much internal IT control as possible,[31] maximizing cost savings in order to free up organizational human capital,[32] [33] and complying with federal regulations.[34] In short, federal leaders are looking for tools that are relatively easy and cost-effective to maintain within the bounds of adequate cybersecurity.

As agencies adapt to meet the security challenges posed by growing device diversity and cybercriminal determination, they are increasingly looking to each other for lessons. In response, organizations like the U.S. Digital Service (USDS) are offering guidance in procurement, implementation, and upkeep of network security solutions. A 2016 USDS report to Congress outlines the process for "transforming federal IT procurement," citing team culture, investment in human capital, and a "shift from process to product" as pivotal in addressing the inability of government procurement cycles to "keep pace with fast-changing technology and user needs."[35]

Issue #5: Balancing Agility and Compliance

The policy framework underpinning federal cybersecurity is a complicated web of legislation, executive orders, and administrative guidelines. The various threats agencies face point to the need for a strategic framework to guide federal government network security, but they also indicate the importance of a balance between the needs of today and the demands of long-term effectiveness.

A framework with these features could be constructed from a number of existing foundations — the giants in the room include the Federal Information Security Modernization Act (FISMA), Modernizing Government Technology (MGT) Act, and Binding Operational Directive 18-01 from DHS.[36] [37] [38] These measures aim to keep government nimble in its preparation for and response to cyber threats regardless of threat origin. The DHS Directive, in particular, offers a vision for the future of network security governance: by formalizing and enforcing established cyber hygiene practices, the Department hopes to prevent phishing and spam, and to positively impact user security in general.[39]

While these policies have certainly progressed, their relatively slow rollout — combined with the acceleration of threat complexity — have somewhat dulled the effectiveness of the DHS directive and similar efforts. In addition to the procurement-centered issues described in a USDA report to Congress, the federal government has struggled to adequately ensure email authentication, web app firewalls, and even the physical security of facilities.[40] [41] And even when the policies have been produced with greater timeliness, agencies have responded slowly: a recent effort to form and implement an election task force at DHS has run into staffing issues and budgetary roadblocks.[42]

The federal government is learning from the rocky roll-out of a network security policy framework, and is implementing lessons with a quickening pace. A number of agencies are investing resources towards the improvement of network security capabilities. The 2017 White House budget proposes $1.5 billion in funding for the DHS to "protect federal networks and critical infrastructure from cyberattacks" and an additional $61 million increase to assist the FBI and Justice Department efforts to "combat criminals and terrorists' use of encrypted communication tools."[43] [44] Collectively, these budgetary commitments address the discrepancy between government-wide security modernization efforts and the resources available to IT managers expected to deliver measurable outcomes.

Looking Ahead at Network Security

While IT networks have added greater functionality and accessibility, they place added pressure on government organizations to secure their network security systems. Managers have many solutions available to them, but run into technical, human capital, and regulatory barriers during implementation.

As threats continue to escalate in scale and complexity, enterprise-level solutions designed to support a cloud-based IT environment will be crucial. It will be equally important to keep an eye towards wrangling IoT devices, crafting effective policy at the agency-specific and government-wide levels, and generally keeping apprised of major changes in cybersecurity best practice.

Sources

1 “Americans and Cybersecurity”, Pew Research Center. Published January 2017. http://www.pewinternet.org/2017/01/26/americans-and-cybersecurity/

2 “Ransomware attack reveals bitcoin as an accessory to cybercrime: Don Pittis”, CBC News. Published May 2017. http://www.cbc.ca/news/business/ransomware-bitcoin-threat-cyberattack-1.4115344

3 “Digital gold: why hackers love Bitcoin”, The Guardian. Published May 2017. https://www.theguardian.com/technology/2017/may/15/digital-gold-why-hackers-love-bitcoin-ransomware

4 How to Protect Your Networks from Ransomware”, United States Department of Justice, Computer Crime and Intellectual Property Section (CCIPS). Published June 2016. https://www.justice.gov/criminal-ccips/file/872771/download

5 “6 Must-Know Cybersecurity Statistics for 2017 | Barkly Blog”, Barkly Blog. Published January 2017. https://blog.barkly.com/cyber-security-statistics-2017

6 “New Ransomware Linked to NotPetya Sweeps Russia and Ukraine”, Wired Magazine, October 2017. https://www.wired.com/story/badrabbit-ransomware-notpetya-russia-ukraine/

7 “Alert (TA17-164A): HIDDEN COBRA – North Korea’s DDoS Botnet Infrastructure”, United States Computer Emergency Readiness Team (US-CERT). Published June 2017. https://www.us-cert.gov/ncas/alerts/TA17-164A

8 *Ibid.*

9 “Alert (TA17-293A): Advanced Persistent Threat Activity Targeting Energy and Other Critical Infrastructure Sectors”, United States Computer Emergency Readiness Team (US-CERT). Published October 2017. https://www.us-cert.gov/ncas/alerts/TA17-293A

10 “GAO: Optimize Data Centers or Lose Them”, Nextgov. Published March 2017. http://www.nextgov.com/cloud-computing/2017/03/gao-optimize-data-centers-or-lose-them/136416/

11 “Mitigating government’s risks in a cloud-based world”, GCN. Published June 2017. https://gcn.com/articles/2017/06/26/mitigating-cloud-risk.aspx

12 “Making the Leap: Exploring the Push for Cloud Adoption”, Government Business Council, Government Executive. Published September 2017. http://www.govexec.com/insights/reports/making-leap-exploring-push-cloud-adoption/141248/?oref=insights-river

13 “Department of Homeland Security (DHS), OCIO Architecture, Development, and Platform Technical Services (ADaPTS)”, Federal Business Opportunities (FedBizOpps.gov). Published August 2017. https://www.fbo.gov/index?s=opportunity&mode=form&id=31174249466827eff15c7196a854a974&tab=core&_cview=0

14 “The Internal Revenue Service Does Not Have a Cloud Strategy and Did Not Adhere to Federal Policy When Deploying a Cloud Service”. Treasury Inspector General for Tax Administration, United States Department of the Treasury. Published August 2017. https://www.treasury.gov/tigta/auditreports/2017reports/201720032fr.pdf

15 *Ibid.*

16 “Report to the President on Federal IT Modernization”, American Technology Council. Published August 2017. https://itmodernization.cio.gov/report/executive-summary/

17 *Ibid.*

18 “Greater Oversight Needed for the Federal Government’s Use of the ‘Internet of Things’”, The Heritage Foundation. Published September 2017. http://www.heritage.org/node/756452/print-display

19 “Internet of Things: Status and implications of an increasingly connected world”, United States Government Accountability Office (GAO), May 2017. http://www.gao.gov/assets/690/684590.pdf

20 “Network Security: Top 5 Fundamentals”, IT Manager Daily. Published 2017. http://www.itmanagerdaily.com/network-security-fundamentals/

21 “News Release: DHS Delivers Study on Government Mobile Device Security to Congress”, United States Department of Homeland Security. Published May 2017. https://www.dhs.gov/science-and-technology/news/2017/05/04/news-release-dhs-delivers-study-government-mobile-device

22 “Greater Oversight Needed for the Federal Government’s Use of the ‘Internet of Things’”, The Heritage Foundation. Published September 2017. http://www.heritage.org/node/756452/print-display

23 “How Is the Federal Government Using the Internet of Things?”, Information Technology & Innovation Foundation. Published July 2016. https://itif.org/publications/2016/07/25/how-federal-government-using-internet-things

24 “Internet of Things: Enhanced Assessments and Guidance are Needed to Address Security Risks in DOD”, United States Government Accountability Office. Published July 2017. http://www.gao.gov/assets/690/686296.pdf

25 “Senators Introduce Bipartisan Legislation to Improve Cybersecurity of ‘Internet-of-Things’ (IoT) Devices”, Office of US Senator Mark R.Warner. Published August 2017. https://www.warner.senate.gov/public/index.cfm/2017/8/enators-introduce-bipartisan-legislation-to-improve-cybersecurity-of-internet-of-things-iot-devices

26 “Spime Watch: The Fact Sheet for the Internet of Things Cybersecurity Improvement Act of 2017”, Wired Magazine. Published August 2017. https://www.wired.com/beyond-the-beyond/2017/08/spime-watch-fact-sheet-internet-things-cybersecurity-improvement-act-2017/

27 “A First Legislative Step in the IoT Security Battle”, Lawfare Blog. Published August 2017. https://www.lawfareblog.com/first-legislative-step-iot-security-battle

28 “Improving Supply-Chain Policy for U.S. Government Procurement of Technology”, Council on Foreign Relations. October 2015. https://www.cfr.org/report/improving-supply-chain-policy-us-government-procurement-technology

29 *Ibid.*

30 “Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies”, United States Department of Homeland Security. Published September 2016. https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf

31 “Best Practices for Federal Agency Adoption of Commercial Cloud Solutions”, PSC Technology Council. Published December 2015. http://www.pscouncil.org/Downloads/documents/PSC-Cloud-WEB%20-%2012-10-15.pdf

32 “From Awareness to Action: A Cybersecurity Agenda for the 45th President”, Center for Strategic & International Studies. Published January 2017. https://csis-prod.s3.amazonaws.com/s3fs-public/publication/170110_Lewis_CyberRecommendationsNextAdministration_Web.pdf

33 “Actions Needed to Strengthen U.S. Capabilities”, United States Government Accountability Office. Published February 2017. https://www.gao.gov/products/GAO-17-440T

34 “National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework”, National Institute of Standards and Technology”. Published August 2017. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf

35 “2016 Report to Congress: Transforming Federal IT Procurement”, The U.S. Digital Service. Published 2016. https://www.usds.gov/report-to-congress/2016/procurement/

[36] "Federal Information Security Modernization Act", United States Department of Homeland Security. Published November 2017. https://www.dhs.gov/fisma

[37] "MGT Act passes Senate as amendment to NDAA", FedScoop. Published September 2017. https://www.fedscoop.com/mgt-act-passes-senate-attached-ndaa/

[38] "DHS orders federal agencies to bolster cybersecurity with HTTPS, email authentication", TechRepublic. Published October 2017. http://www.techrepublic.com/article/dhs-orders-federal-agencies-to-bolster-cybersecurity-with-https-email-authentication/

[39] "Binding Operational Directive 18-1: Enhance Email and Web Security, United States Department of Homeland Security." Published October 2017. https://cyber.dhs.gov/

[40] "Report: Most Government Sites Fail Security Audit", Nextgov. Published June 2017. http://www.nextgov.com/cio-briefing/2017/06/report-most-government-sites-fail-security-audit/138867/

[41] "NIST's Physical Security Falls Short, Undercover Audit Finds", Nextgov. Published October 2017. http://www.nextgov.com/cybersecurity/2017/10/nists-physical-security-falls-short-undercover-audit-finds/141696/

[42] "DHS Forms Election Security Task Force", Nextgov. Published October 2017. http://www.nextgov.com/cybersecurity/2017/10/dhs-forms-election-security-task-force/141497/

[43] "Trump's budget proposal gives DHS $1.5 billion for cybersecurity", The Hill. Published March 2017. http://thehill.com/policy/cybersecurity/324238-trumps-budget-proposal-gives-dhs-15-billion-for-cybersecurity

[44] "What Trump's Skinny Budget Says About Cybersecurity", Nextgov. Published March 2017. http://www.nextgov.com/cybersecurity/2017/03/what-trumps-skinny-budget-says-about-cybersecurity/136217/

About Forcepoint

Forcepoint is transforming cybersecurity by focusing on what matters most: understanding people's intent as they interact with critical data and intellectual property wherever it resides. Our uncompromising systems enable companies to empower employees with unobstructed access to confidential data while protecting intellectual property and simplifying compliance. Based in Austin, Texas, Forcepoint protects the human point for thousands of enterprise and government customers in more than 150 countries. For more about Forcepoint, visit www.Forcepoint.com and follow us on Twitter at @ForcepointSec.

About Government Business Council

As Government Executive Media Group's research division, Government Business Council (GBC) is dedicated to advancing the business of government through analysis, insight, and analytical independence. An extension of *Government Executive*'s 40 years of exemplary editorial standards and commitment to the highest ethical values, GBC studies influential decision makers from across government to produce intelligence-based research and analysis.