FEDERAL ISSUE BRIEF

Government
Business
Council

THREAT DETECTED:

Cybersecurity at Scale in the Federal Government

Sponsored by:

Google Cloud

THE BIG ISSUE

The evolving threat landscape is forcing agencies to look beyond traditional safeguards and embrace solutions that scale to protect a growing and fluid environment, from data center to device.

WHY IT MATTERS

Recent government studies present a damning portrait of federal cybersecurity practices. Four years after the devastating OPM breach that exposed records of millions of federal employees, the government has made only incremental progress to shore up its defenses.[1] Poor cyber hygiene and fragmented authority impede modest reforms, leaving agencies vulnerable to and unaware of the most sophisticated threats facing them today.

WHO NEEDS TO KNOW

Everyone: Federal CIOs, CISOs, CTOs, cybersecurity program managers, information specialists, and rank-and-file employees

PLAYERS AND POLICIES TO KNOW

- **The Internet of Things Cybersecurity Improvement Act:** Bipartisan legislation still awaiting votes from both chambers, the law would formalize a vulnerability disclosure process within NIST for internet-connected devices and prohibit agencies from buying such devices from vendors that don't participate in said process.

- **GAO Report on Supply Chain Risks Affecting Federal Agencies:** In its first report on the subject in 7 years, the Government Accountability Office (GAO) found persisting vulnerabilities in the IT supply chains of 4 national security-related agencies. According to the report, such vulnerabilities included the acquisition of products or parts from unauthorized distributors; inadequate testing of software updates and patches; and incomplete information on IT suppliers.

- **Senate Subcommittee Report on Federal Cybersecurity:** Following a 10-month review, the Senate Subcommittee on Investigations found significant cybersecurity weaknesses in place at 8 federal agencies. Agencies were cited for failing to secure personally identifiable information (PII), using systems that lacked authorization-to-operate (ATO) status, continuing reliance on outdated legacy IT, and neglecting measures to empower CIO authority.

THE STATUS QUO IS *OBSOLETE*

The needle is moving, but not fast enough: with every leap federal agencies make, cyber adversaries go farther.

For example, a 2018 White House report found that 3 out of every 4 federal cybersecurity programs were **‘at risk’ or at ‘high risk’** of an attack.

Moreover, 38% of federal cyber incidents studied were **never able to identify the attack vector**, indicating substantial gaps in awareness of the types and severity of attacks being launched on agencies.[2]

Since 2010, GAO has made 3,000 cybersecurity recommendations to agencies, yet nearly 700 of these had not been fully implemented as of December 2018.[3] And according to one study of federal IT managers, **the average cost of a data breach is around $91,000**, which amounts to $637 million dollars in lost taxpayer money every year.[4]

TODAY’S CHALLENGES

Many reasons exist as to why agency cybersecurity continues to suffer...

THE DATA TSUNAMI: First, the rapid increase in Internet of Things devices and mobile connections has resulted in a flood of data, a great portion of which exceeds current data infrastructure capacity. Moreover, the push to create digital services and digitize records is estimated to produce 175 zettabytes of data by 2025 — at least a **400% increase over 2018 levels**, a large portion of which will be collected, processed, and stored by U.S. government organizations.[5]

SYSTEM OVERLOAD: Second, many agencies continue to use **duplicate, outdated, or overlapping versions of software**, which compounds the number of vulnerabilities they must address. Because of this, agency networks result in an abundance of disparate systems managing various elements of security (network, endpoint, storage), but lack defined channels for sharing and delegating cyber responsibilities effectively.

WORKFORCE WOES: Third, agencies lack critical cyber expertise and methods for validating cyber credentials. According to GAO, 3 agencies it investigated had failed to conduct baseline assessments of professional certifications held by their cybersecurity employees.[6] Aggravating matters further, the highest levels of IT leadership have experienced high turnover -- **from 2012 to 2017, at least 3 agencies saw a rotation of six different CIOs**, which inspectors believe undermined their ability to follow through on strategic cyber objectives.[7]

THE BOTTOM LINE

Traditional safeguards have continued to fuel a reactive cybersecurity environment. If agencies hope to survive in the new cyber landscape, they must adopt a comprehensive cybersecurity stance in the cloud that provides automated, in-depth protection, from device to the data center.

AGENCIES LACK CONFIDENCE

Agencies can move beyond the reactive security posture by identifying and addressing shortcomings.

As a 2019 Government Business Council survey of over 500 federal employees shows, many employees lack the direction and confidence to follow through on cybersecurity concerns.[8]

37%

of respondents felt their organization's ability to harness data-driven insights trailed behind the capabilities of other agencies.

LESS THAN

25%

identified key cyber security practices (e.g., hiring and retention of skilled personnel, reviewing existing security tools) as top priorities for their organization.

MORE THAN

1 in 4

of those surveyed said their organization does not possess clear channels for elevating security-related concerns.

These findings show that agencies lack confidence in their current security posture and are challenged in directing resources and personnel to solve their top security gaps.

RAISING THE BAR

Fortunately, the expectations for a secure environment are being redefined. The White House, NIST, OMB, and GAO have called on agencies to pursue a comprehensive cybersecurity approach that can anticipate threats before they emerge, keep agencies vigilant to the latest attack vectors, fill needed gaps in cyber expertise, and create greater visibility and accountability across the IT enterprise.

- ➔ Under this type of approach, agencies will be able to protect user data, configure applications and user privileges with appropriate access, and secure devices at their network's edge.
- ➔ They can leverage sophisticated analytics and machine learning tools to model and predict threats, as well as automatically flag noteworthy concerns from the noise of incredible volumes of data.
- ➔ Additionally, IT administrators and cyber personnel would have access to a centralized console where they can view attempted threats, relay suspicious behavior in the network, and stop intruders in their tracks.

The end result is a consolidation of cybersecurity operations under one roof, a standardized set of tools and practices across government that puts agencies on collaborative footing, greater cyber awareness and adherence among employees, and a system that holds cyber leadership accountable for breaches occurring on their watch.

WORKING WITH GOOGLE CLOUD

Threats posed by attackers to government organizations have only grown more sophisticated and urgent.

At Google Cloud, our customers' need to securely store data and defend against threats—either in the cloud or on premise—is a top priority. We approach security holistically, from the chip to the datacenter, with a continuously growing set of security capabilities that work in concert to deliver defense-in-depth at scale: from hardware infrastructure, service deployment and user identity, to storage, internet communication and security operations.

Moreover, our security offerings address important requirements customers have to protect their infrastructure and mission critical application workloads in the cloud; to protect their data; to protect their users; and to give them transparency and auditability of their workloads running in Google Cloud.

> **“In 2017 alone, federal agencies reported 35,277 cyber incidents. After a decade of negligence, our federal agencies have failed at implementing basic cybersecurity practices, leaving classified, personal, and sensitive information unsafe and vulnerable to theft.”**
>
> ***-- Sen. Rob Portman (R-Ohio)***

WHAT CAN AGENCIES DO TO BECOME CYBER READY?

Raise awareness and provide continuous training to workforce: Agencies should never downplay the value of an educated workforce, especially when it comes to cyber. Cybercriminals will always look for the weakest link when targeting any organization, and an employee who hasn't received basic cybersecurity courses will create an attractive target to such offenders.

Training deficiencies are known to have plagued agencies in recent years: for example, a 2019 audit of the DoD's Cyber Mission Force (CMF) found that Cyber Command "[had] not established training task lists for foundational training courses," creating a slipshod system for exempting certain personnel from mandatory courses. Moreover, it found that the Army and Air Force did "not have time frames for required validation of foundational courses," nor "a plan to establish required independent assessors to ensure the consistency of collective CMF training."[9]

DHS is working to solve the training gap. It recently invested $5.9 million in the Distributed Environment for Critical Infrastructure Decision-Making Exercises, or DECIDE, an interactive platform that allows players to simulate cyber-threat response tactics in a virtual, online environment to prepare them for handling real-life crises.[10]

Create elevation channels with authority at top, and hold authority accountable: As GBC's survey respondents attested to, cyber leadership is still ill-defined and susceptible to interference and over-reach from other departments.

In the wake of President Trump's Executive Order empowering CIOs with greater authority over IT operations, agency leadership should be held accountable for how they enforce this hierarchy and should additionally assign clear channels for elevating cybersecurity concerns without fear of reprimand or retaliation.

Consolidate, centralize, and streamline resources in the cloud: Many agencies feel burdened by a bloat of legacy systems they feel they can't do without. In some cases, 95% of an agency's entire IT budget is allocated toward operations and maintenance of existing legacy IT.[11] This type of model isn't sustainable in today's threat landscape and agencies are suffering for it. What's needed is a centralized command from which agency personnel can view the entire spectrum of network operations, with automated cloud tools for flagging and validating suspicious threat activity. If agencies hope to move faster than their adversaries, they'll need to start acquiring AI tools that automate 'search and destroy' threat hunts in the cloud. Such tools wouldn't replace cyber personnel, but provide them with greater functionality and choice in how they protect the perimeter.

! RISK OF INACTION

If agencies continue without a security-at-scale approach in the cloud, they will ultimately cede their authority as servant institutions capable of safeguarding the personal data of millions of Americans.

To reverse this trend, they can start by implementing guidance from federal bodies like GAO and NIST, integrating the Cyber Framework into their risk management practices, and looking toward new AI capabilities and automation for reducing the data overload on their limited supply of cyber specialists.

Additionally, engaging a trusted private sector partner can solve many of these limitations: by leveraging these partnerships, agencies can acquire advanced cloud and AI technology that automates security at scale, updates on a routine basis to defend against the latest threats, and resolves critical gaps in cyber expertise.

SOURCES

1. *Nextgov*: “Timeline: What We Know About the OPM Breach (UPDATED).” June 2015.
https://www.nextgov.com/cybersecurity/2015/06/timeline-what-we-know-about-opm-breach/115603/

2. Executive Office of the President: “Federal Cybersecurity Risk Determination Report and Action Plan.” May 2018.
https://www.whitehouse.gov/wp-content/uploads/2018/05/Cybersecurity-Risk-Determination-Report-FINAL_May-2018-Release.pdf

3. GAO: “High Risk Series: Ensuring the Cybersecurity of the Nation.”
https://www.gao.gov/highrisk/ensuring_the_security_federal_government_information_systems/why_did_study#t=0

4. Beyond Trust: “Federal Cybersecurity Threat Survey Report.” 2017.
https://www.beyondtrust.com/resources/whitepapers/federal-cybersecurity-threat-survey-report

5. IDC: “Data Age 2025: The Digitization of the World From Edge to Core.” Nov. 2018.
https://www.seagate.com/files/www-content/our-story/trends/files/idc-seagate-dataage-whitepaper.pdf

6. See [3]

7. U.S. Senate: “Federal Cybersecurity: America’s Data at Risk.” 2019.
https://www.portman.senate.gov/sites/default/files/2019-06/2019.06.25-PSI%20Report%20Final%20UPDATE.pdf

8. GBC: “Assessing Cybersecurity Readiness in the Federal Government.” May 2019.
https://cdn.govexec.com/media/gbc/docs/assessing-cybersecurity-readiness.pdf

9. *Nextgov*: “Pentagon’s Cyber Mission Force Needs Better Training Plan.” March 2019.
https://www.nextgov.com/cybersecurity/2019/03/pentagons-cyber-mission-force-needs-better-training-plan/155372/

10. *Nextgov*: “DHS Invests $5.9 Million into Cyber Training Tool for Energy Sector.” March 2019.
https://www.nextgov.com/cybersecurity/2019/03/dhs-invests-59-million-cyber-training-tool-energy-sector/155808/

11. See [7]

Government Business Council

Google Cloud

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 a commitment to the highest ethical values, GBC studies influential decision makers from across government to produce intelligence-based research and analysis.

Learn more at www.govexec.com/insights.

Report Author: Daniel Thomas

ABOUT GOOGLE CLOUD
Google Cloud is widely recognized as a global leader in delivering a secure, open, intelligent and transformative enterprise cloud platform. Our technology is built on Google's private network and is the product of nearly 20 years of innovation in security, network architecture, collaboration, artificial intelligence and open source software. We offer a simply engineered set of tools and unparalleled technology across Google Cloud Platform and G Suite that help bring people, insights and ideas together. Customers across more than 150 countries trust Google Cloud to modernize their computing environment for today's digital world.

Learn more at https://cloud.google.com/.