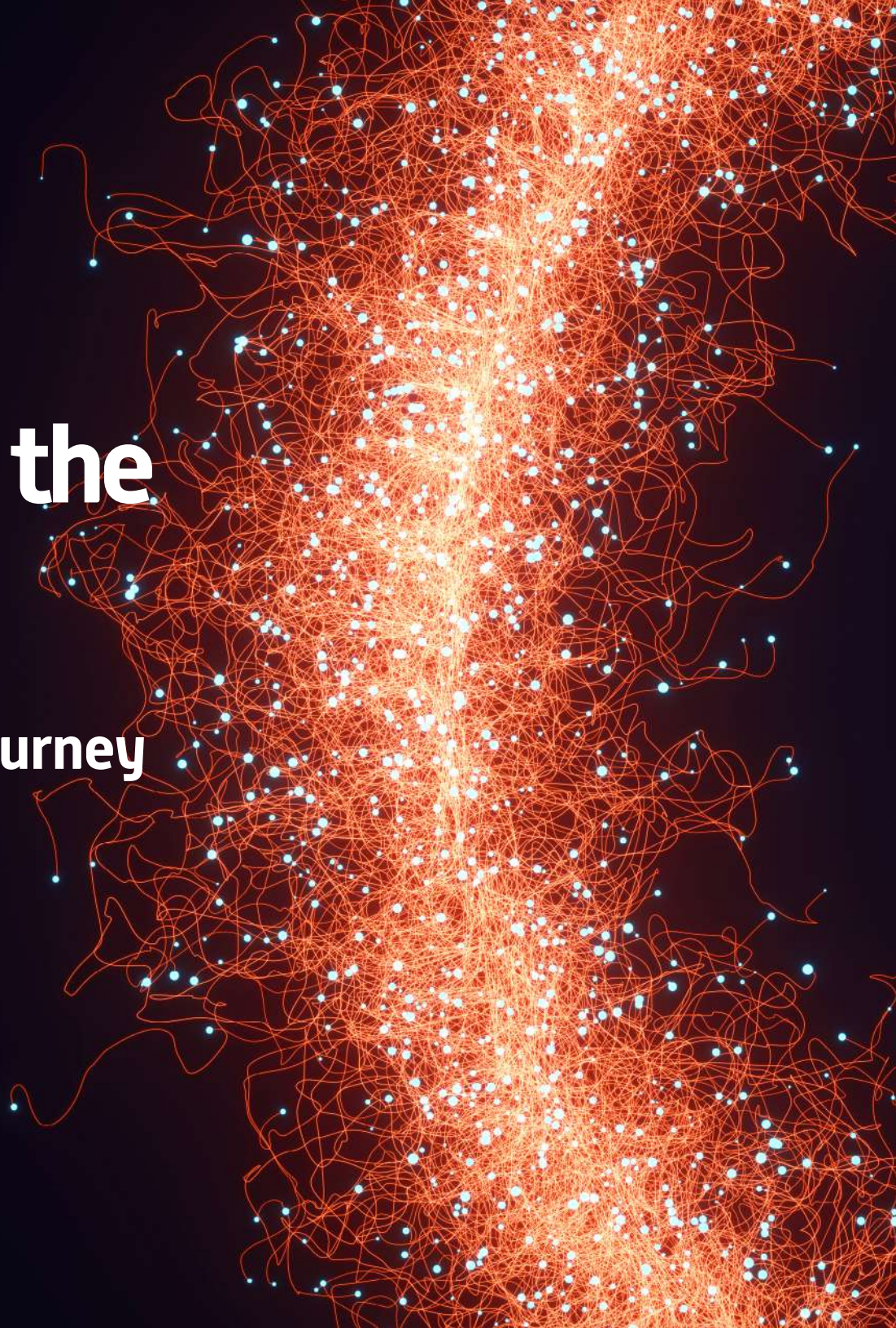
Government Business Council

Authentication at the Network's Edge:

The Federal Government's Journey to Secure Mobile Devices

FEDERAL ISSUE BRIEF



Sponsored by:

Panasonic TOUGHBOOK®

THE BIG ISSUE:

Mobility is critical to government productivity, but mobile data and devices present attractive targets to cybercriminals seeking to exploit vulnerabilities across the spectrum.

BY THE NUMBERS

$ THE AVERAGE COST OF A DATA BREACH IN 2018 WAS $3.86 MILLION[1]

APPROXIMATELY 3 OUT OF EVERY 4 FEDERAL EMPLOYEES SURVEYED IN 2017 ADMITTED TO DOWNLOADING UNAUTHORIZED APPS TO THEIR WORK-ISSUED MOBILE DEVICE IN VIOLATION OF ORGANIZATIONAL POLICY[2]

IN 2017, ONLY 54 PERCENT OF AGENCIES REQUIRED EMPLOYEES TO LOCK DEVICES WITH A PIN OR PASSWORD

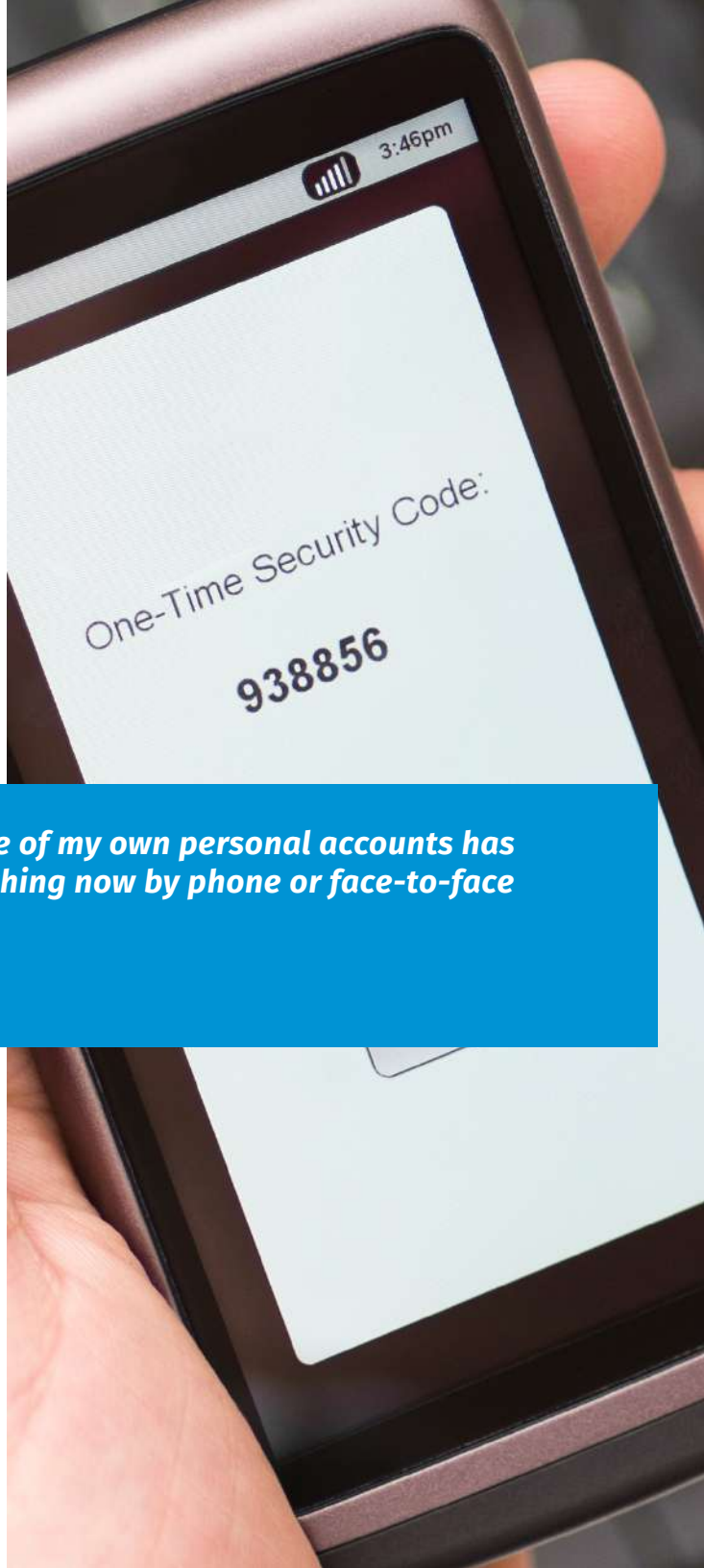
THE STATUS QUO IS OBSOLETE:

Federal agencies are no strangers to cybersecurity attacks, but recent high-profile breaches involving mobile devices demonstrate ongoing vulnerabilities in government's expanding network of endpoints:

- While serving as Department of Homeland Security (DHS) Secretary, it was revealed that John Kelly's smartphone had been hacked, providing attackers a foothold into his personal email account. [3] Around the same time, the NSA urged the new administration to cease use of personal smartphones and email out of fear they might already be compromised by foreign adversaries.[4]
- In early 2018, a popular mobile fitness app publicized heat map signatures of its users, which happened to include the classified operating locales of US military officers stationed abroad. The incident spurred DoD leadership to review a potential ban on mobile devices allowed into the Pentagon and other sensitive locations.[5]

> ***"Then there is the hacking which one of my own personal accounts has suffered recently. I do almost everything now by phone or face-to-face comms."***
>
> *— DHS Secretary John Kelly (2017)*

- In July 2018, the Government Accountability Office (GAO) placed mobile cybersecurity on its High-Risk Series report, citing agency deficiencies in protecting private and sensitive data due to ubiquitous Internet connectivity available through mobile devices.[6]
- Most recently, DHS issued an emergency directive in 2019 demanding agencies take immediate steps to secure their mobile Domain Name System infrastructures, including multi-factor authentication, enforced password changes, and audits of DNS records.[7]



"Threats to the Government's use of mobile devices are real and exist across all elements of the mobile ecosystem. The enhanced capabilities that mobile devices provide, the ubiquity and diversity of mobile applications, and the typical use of the devices outside the agency's traditional network boundaries requires a security approach that differs substantially from the protections developed for desktop workstations."

— Study on Mobile Device Security (2017), Department of Homeland Security[8]

Even though mobile devices widen the potential attack vector, eliminating their use for federal employees would undermine the tremendous gains to productivity and communication such devices have created in recent years. Instead of resisting the tide of devices, agencies need to get smart about protecting their devices by introducing and enforcing sensible security measures across the enterprise.

WHAT CAN BE DONE:

Multi-factor authentication is one of the more viable options agencies can use to fend off increasingly sophisticated attacks on mobile devices. When multi-factor is in place, it requires a user to input both their password as well as a one-time signature generated by a second device in the possession of the user. This means even if a password is compromised, a hacker would still need to steal a government worker's physical device to gain access.[9]

More and more government agencies are moving to implement multi-factor protocols: recent adopters include the Office of Personnel Management (OPM), Department of State, Department of Justice, and Department of Defense. "Two-factor has always been the gold standard, and this gets us there," says Michelle Earley, program manager at USAJobs within OPM.[10] Her department made the changes in response to user frustrations at password length requirements and bottlenecks caused by accounts automatically deactivating following long periods of inactivity.

There are additional multi-factor safeguards agencies can use to protect their devices at the hardware level. For example, smart card authentication (e.g., PIV cards) and biometrics (e.g., retinal scans) are increasingly popular options for government users handling devices in secure zones. Each smart card contains a miniature computer chip that, when plugged into the device, can provide secure storage and access privileges to authorized users. Likewise, biometric technology assigns access to a user's unique biological signature, whether retinal or fingerprint-based.

THE BOTTOM LINE

Agencies can comply with federal mandates and bolster enterprise mobile security by adopting a set of practices that protect devices at both the hardware and software level.

Principle of least privilege: Agencies are still struggling to determine appropriate authorization for mobile device use. In a 2017 investigation, GAO reported that 24 agencies had weaknesses in implementing effective authorization controls, amounting to 108 access control weaknesses. Three of these agencies failed to periodically review user access to ensure access was appropriate for the user's job function, and five others were found to have active accounts for users no longer employed by that agency. By restricting access to the minimal number of users required to fulfill a job function, organizations can mitigate the likelihood of authorized users misusing the trust that's been granted to them.

User education: Where multi-factor authentication and least-privilege authorization go a long way toward protecting devices, a workforce engaging in bad cyber hygiene can undermine even these mechanisms. In recent years, federal agencies have consistently reported over 30,000 cyber incidents to DHS, approximately one-fifth of which resulted from employee violations of online activity, susceptibility to email and phishing attacks, and misplaced equipment.[11]

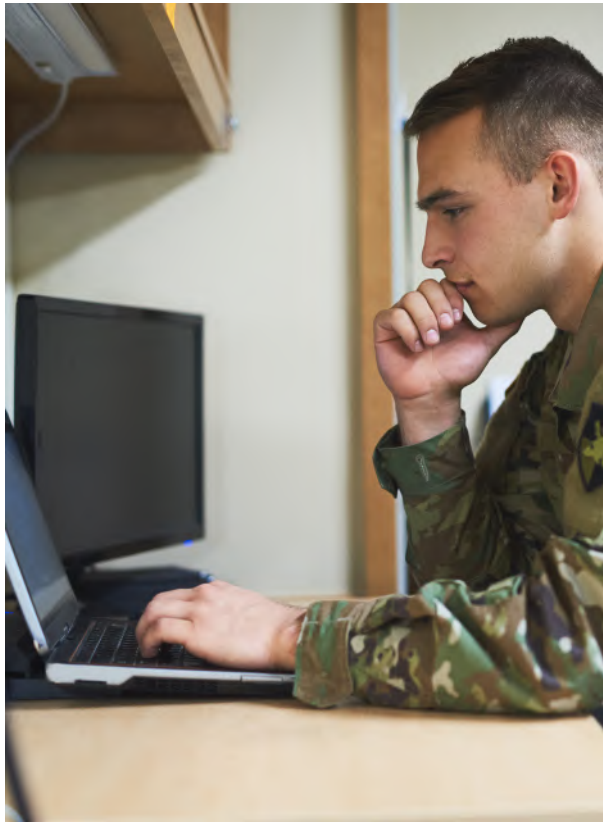
In 2018, the National Geospatial-Intelligence Agency (NGA) said enough was enough and agreed to host two week-long cyber escape room events to train its employees in demonstrating basic cyber hygiene.[12] Meanwhile, DHS's Continuous Diagnostics and Mitigation program is planning to expand its AWARE initiative in the coming year. AWARE, which stands for Agency-Wide Adaptive Risk Enumeration, will use algorithms to scan online activities of employees and then generate a cyber hygiene score (much like a credit score) that reflects the health of the organization's overall cybersecurity.[13]

RISK OF INACTION:

Agencies can't afford to ignore the growing problem of mobile security. When devices don't receive the necessary protection, it introduces substantial risks to an organization's data, the efficiency of its mission, and the privacy and well-being of its people. Unprotected devices can result in exposure of agency proprietary data, undermine the trust that citizens have in seeking government services, and create negative publicity that takes years to recover from.

Most importantly, mobile devices devoid of strong protection can spell huge consequences for the safety of everyday Americans: whether it's misplacing a tablet holding sensitive data in a hostile war zone or unwittingly leaking personal health records that find their way to the black market, vital endpoints must be secured across the network or the fallout could be severe.

Federal agencies have a limited window to implement critical gains to their security posture. Multi-factor authentication and additional protections at the hardware level can substantially reduce the attack vector while enabling employees the degree of mobility needed to perform at the highest level.



WORKING WITH PANASONIC:

Mobile device security is a critical part of an organization's overall security approach. Panasonic has a 20+ year history of delivering secure, rugged, mobile devices for government. The ruggedized design largely eliminates the threat of data loss due to device damage and other features help prevent device theft TOUGHBOOK devices also include various enterprise-level security features enabling IT to protect data, access privileges and connections to the network.

Hardware-level security includes:

- Trusted Platform Module 1.2 or 2.0 and FIPS 140-2 compliant encryption
- NIST BIOS compliance for TOUGHBOOK laptops to protect against unauthorized modification
- Removable hard drives
- Options for accessories such as fingerprint and smart card readers to authenticate user access
- Cable locks

END NOTES

1. CSO : "6 mobile security threats you should take seriously in 2019." Nov 20, 2018 https://www.csoonline.com/article/3241727/mobile-security/6-mobile-security-threats-you-should-take-seriously-in-2019.html
2. Nextgov : "Report: Most Feds Break Smartphone Security Rules." Feb 14, 2018. https://www.nextgov.com/it-modernization/2018/02/report-most-feds-break-smartphone-security-rules/145986/
3. Engadget : "White House confirms its chief of staff was hacked." June 11, 2018. https://www.engadget.com/2018/06/11/john-kelly-hacked-foia-request/
4. Politico : "NSA warned White House against using personal email." Sept 29, 2017 https://www.politico.com/story/2017/09/29/white-house-private-email-nsa-warning-243324
5. Nextgov : "Pentagon Reviewing Electronic Device Policy." Jan 31, 2018. https://www.nextgov.com/policy/2018/01/pentagon-reviewing-electronic-device-policy/145625/
6. GAO: High-Risk Series: Urgent Actions Are Needed to Address Cybersecurity Challenges Facing the Nation." July 25, 2018. https://www.gao.gov/assets/700/693405.pdf
7. Nextgov : "Agencies Have 10 Days to Review, Secure Critical IT Weakness." Jan 23, 2019. https://www.nextgov.com/cybersecurity/2019/01/agencies-have-10-days-review-secure-critical-it-weakness/154372/
8. DHS: "Study on Mobile Device Security." April 2017. https://www.dhs.gov/sites/default/files/publications/DHS%20Study%20on%20Mobile%20Device%20Security%20-%20April%202017-FINAL.pdf
9. The Washington Post : "The government is rolling out 2-factor authentication for federal agency dot-gov domains." Oct 8, 2018. https://www.washingtonpost.com/technology/2018/10/08/government-is-rolling-out-factor-authentication-federal-agency-gov-domains/?utm_term=.8a4906b76e91
10. The Washington Post : "Central federal jobs site tightens security controls." Feb 27, 2018. https://www.washingtonpost.com/news/powerpost/wp/2018/02/26/central-federal-jobs-site-tightens-security-controls/?utm_term=.1208c96c63ab
11. Nextgov: "Agencies Faced More Than 35,000 Cyber Incidents in 2017, Watchdog Says." Dec 18, 2018. https://www.nextgov.com/cybersecurity/2018/12/agencies-faced-more-35000-cyber-incidents-2017-watchdog-says/153659/
12. Nextgov: "One Agency Plans to Lock Employees In a Room Until They Learn Cyber Hygiene." Aug 13, 2018. https://www.nextgov.com/cybersecurity/2018/08/one-agency-plans-lock-employees-room-until-they-learn-cyber-hygiene/150487/
13. Nextgov: "Agencies Will Soon Have a Cyber Hygiene Score—And Will Know Where They Rank." Nov 28, 2018. https://www.nextgov.com/cybersecurity/2018/11/agencies-will-soon-have-cyber-hygiene-scoreand-will-know-where-they-rank/153114/

Government Business Council

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

Panasonic TOUGHBOOK

ABOUT PANASONIC

Panasonic is changing the way work is done by delivering purpose-built mobile technology solutions designed to keep workers more connected and be more efficient. Manufactured with the evolving needs of the mobile worker in mind and engineered to stand up to the most challenging conditions, Panasonic TOUGHBOOK devices and accessories are part of an ecosystem of solutions, services and software designed to help today's worker go anywhere and achieve anything. To learn more, please visit toughbook.com.

Government Business Council

Sponsored by:

Panasonic TOUGHBOOK®