10 Cybersecurity Issues New Federal CISO Should Focus On

We made a list of the top priorities, in case he needs one.

Amanda Ziadeh

Tue, 07/24/2018 - 16:15

Illustration: erhui1979/iStock

If you haven’t heard, there’s a new federal chief information security officer in town — or, in the White House. The Office of Management and Budget announced Grant Schneider as the second federal CISO, filling the shoes of Greg Touhill after he stepped down in January 2017.

Schneider previously served as Defense Intelligence Agency chief information officer, and was deputy CISO to Touhill. He was appointed interim CISO after Touhill’s departure, and now his title is permanent. We’re sure Schneider has his own pile of cybercritical issues to prioritize and manage, but we thought we’d help with a list of our own:

Bumping Up FITARA Scores

According to the most recent Federal IT Acquisition Reform Act Scorecard 6.0 from May, four agencies received an F, five received a D and five received a C under transparency and risk management. Having visibility into system networks — like who's on the network and which adversaries are trying to breach them — is crucial. And risk management is an important part of system, network and cybersecurity as a whole.

Boosting Situational Awareness

According to OMB's Federal Cybersecurity Risk Determination Report and Action Plan published in May, 38 percent of federal cyberincidents did not have an identified attack vector. In other words, agencies couldn't identify the method of attack or attack vector in 11,802 of the 30,899 cyberincidents that compromised information or system functionality in FY 2016. OMB said it's helping to implement a cyberthreat framework so cyberthreats and risks can be communicated quicker.

Mitigating Ransomware Attacks

Ransomware is growing at a yearly rate of 350 percent, according to Cisco's 2017 Annual Cybersecurity Report. And financial damages are skyrocketing; Cybersecurity Ventures predicts ransomware and other cybercrimes will cost the global economy $6 trillion per year by 2021.

Holding Agencies Accountable for Managing Risk

Agencies lack a standardized process for managing risk, and accountability is uneven across the federal government, according to OMB. Agency heads need to be accountable for their security and governance processes, perhaps by implementing quarterly risk assessments that track agency progress in deploying cybersecurity controls. OMB said it'll use its visibility into agency cybersecurity spending to make sure agencies invest in the right protections, so this may be a priority area for the CISO.

Keeping Up to Date with Tech and People

Of the top four cybersecurity challenges Touhill told GovernmentCIO Media in an interview, replacing antique equipment and software, and keeping up with out-of-date personnel, was a must. According to Touhill's "law," one human equals 25 computer years. "If you take a look at people, processes and technology as the keystones of a good security program, you need to make sure you're keeping up to date with the people, process and technology," he said. Right now, Touhill thinks we're 9.5 years behind where we need to be.

Standardizing IT Capabilities Governmentwide

OMB's risk assessment also found agencies lack standardized cybersecurity processes and IT capabilities, negatively impacting the ability to see and fight off threats. Congress has enhanced CIO authorities and IT spending visibility through FITARA, but it's not enough. How can an agency mitigate threats when they can't identify them? They need to improve access management, email consolidation, and software and application standardization; and someone needs to oversee it.

Protecting Election Systems & U.S. from State-Sponsored Attacks

This isn't just a job for the CISO, but for the overall cybercritical space. In 2016, the Homeland Security Department issued a statement about the Russian government's intention to interfere with the U.S. election process, compromising emails from citizens, institutions and political organizations. Though Christopher Krebs, undersecretary for DHS' National Protection and Programs Directorate, said there is no evidence of specific hacking of election systems for upcoming midterms, there are vulnerabilities to U.S. electronic election systems by nature. Plus, Booz Allen listed compromising political elections as part of its “9 Ways Cybercriminals Will Make Waves in 2018” predictions report.

Improving Network Visibility

The OMB report found 27 percent of agencies said they can detect and investigate attempts to access large volumes of data, but what about the rest? This leaves 73 percent of agencies at risk or high risk in this area. They’re lacking the ability to see what is going on in their networks, or detect data exfiltration to properly respond to cyberincidents. To start, the CISO should prioritize rolling out DHS’ Continuous Diagnostics and Mitigation program enterprisewide, and helping to consolidate agency security operation centers that currently don’t communicate with one another.

Securing the Nation’s Critical Infrastructure

This, too, is a collective responsibility among all sectors — and according to Sabra Horne, director of DHS’ Stakeholder Engagement and Cyber Infrastructure Resilience division, of the 16 critical infrastructure sectors, the electrical, financial services and IT sectors draw significant importance. They’re largely interconnected and can have the most devastating and cascading damages if hit. Earlier this year, MIT Technology Review predicted cyberphysical attacks on critical infrastructure are ones to watch in 2018.

Deploying Proper Security on Emerging Technologies

The growing number of connected devices mean more endpoints for network entry; artificial intelligence and machine learning provides transformative capabilities to government but also a new weapon for adversaries; and cryptocurrency mining is spurring a new kind of cryptomining attack. One person can’t track all of these advancing technologies, but they come with their own set of security and privacy challenges that must be addressed before enterprisewide adoption.

View printer friendly version

cyberattacks
Federal Cybersecurity
CISO
federal CISO
White House
OMB
Department of Homeland Security
Russia
Greg Touhill