People Still Weakest Link in Government Cybersecurity

Govies show the riskiest behavior in social media use, physical security and mobile computing.

Amanda Ziadeh
Tue, 05/22/2018 - 16:04

Undetected threats to the privacy and security of government agencies may be coming from within — not from internal breaches or whistleblowers, but from a lack of employee awareness and cyberhygiene.

In a recent survey by MediaPRO titled “Government Industry Insights: State of Privacy and Security Awareness,” 1,016 local, state and federal government employees were asked questions regarding security, data and cyberscenarios and behavior. The results were a bit alarming; 46 percent of those surveyed are in the
“risk” category, meaning their actions pose “a serious potential threat to the privacy or security of their organizations.”

And sure enough, 61 percent of those were executives and managers at government organizations.

These numbers don’t measure well next to the 19 percent of employees of the general population who also scored as “risk.” In fact, internal privileged misuse and various errors make up a third of breaches, according to the 2018 Verizon Data Breach Investigations Report.

And perhaps most surprising, government was 13 percent more lax on security protocols than general employees from other industries. But the government sector actually performed worse in all eight threat vector categories from the report when compared to the general population:

1. **Incident reporting**: Government responded 7 percent worse at reporting incidents.

2. **Identifying personal information**: 20 percent of government respondents failed to recognize some examples of personally identifiable information.

3. **Physical security**: 45 percent of respondents chose risky behaviors when given scenarios related to building security.

4. **Identifying phishing attempts**: 23 percent of government employees struggled to identify phishing attempts, compared to the 8 percent of general employees.

5. **Identifying malware warnings**: 27 percent of government employees couldn’t identify common warning signs of malware, compared to the 12 percent of general employees.
**Working remotely**: 26 percent of government employees said they would take unnecessary risks when working remotely.

7. **Cloud computing**: 18 percent of government employees chose risky actions when given scenarios about storing sensitive data in personal cloud storage or when sending work documents through personal email.

8. **Use of social media**: 37 percent of government employees reported making risky behavioral choices here. They were given scenarios about re-tweeting sensitive or inappropriate info, and joining public social conversations about sensitive info controlled by the organization.

Perhaps agencies should make sure employees brush up on security, privacy and data protection best practices as they continue implementing cyberdetection solutions and software.

Because it’s not just the technology that needs an update; the humans do, too. The report recommends keeping employees well informed about new and emerging threats, and how daily actions can impact sensitive data and operations, on a regular basis. And not just with yearly training, but with a year-round security and privacy awareness program.