Contact:
Janice Clayton
304-870-4733
jclayton@meritalk.com

Despite Growing Focus on Insider Threat Prevention, Many Agencies Have Lost Data to Insider Incidents in the Last Year

Forty two percent have been targeted by insider cyber incidents; 23 percent have lost data

Alexandria, Va., May 15, 2017 – MeriTalk, a public-private partnership focused on improving the outcomes of government IT, today announced the results of its new report, "Inside Job: The Sequel – The 2017 Federal Insider Threat Report." Despite an increased focus on insider threats and the significant growth of formal prevention programs, the study, underwritten by Symantec, reveals that the rate of cyber incidents perpetrated by insiders remains relatively stagnant – 42 percent of agencies report incidents over the last year, compared to 45 percent in 2015.

"Inside Job: The Sequel," which builds on MeriTalk and Symantec's 2015 "Inside Job: The Federal Insider Threat Report," surveyed 150 Federal IT cybersecurity professionals to examine how agencies can effectively detect and address suspicious behaviors, how cloud adoption can complicate insider threat protection, and where the major gaps in agency prevention strategies lie.

Federal agencies are increasing their focus on insider threats, with 85 percent of survey respondents saying their agency is more focused on combating insider threats today than one year ago – up from 76 percent in 2015. Additionally, 86 percent say they have a formal insider threat prevention program in place – a big jump from just 55 percent in 2015.

But, despite these efforts, 75 percent of respondents say insider threats are just as or more challenging to identify and mitigate today than one year ago, and nearly a quarter say they lost data to an insider threat incident in the last year. Cloud is a big reason why. Fifty nine percent of the survey respondents say that the growing number of cloud-based systems has made insider threats more difficult to identify – due to increased complexity, endpoint monitoring challenges, lack of preventative measures, and difficulty implementing and enforcing identity and access management

-more-

policies. Despite the cloud's impact on the insider threat equation and the serious potential consequences of these incidents, fewer than half of agencies have taken specific steps to ensure cloud adoption does not jeopardize insider threat protection.

"As boundaries dissolve, the threat landscape is becoming more complex. Thanks to cloud adoption, endpoint multiplication, and the ever-growing remote workforce, insider threats are even more difficult to manage and prevent," said Rob Potter, vice president, public sector, Symantec. "Agencies can establish better control over their cybersecurity programs and manage risk more effectively by leveraging the NIST Cybersecurity Framework (CSF) to identify gaps in their security posture and chart a plan to address them. Formal threat detection and response protocols, as well as systems for reporting and maintaining potential or actual incidents, are critical to preventing data loss."

Yet, agencies that have lost data to insider incidents are less likely than those that have not to say they use key security technologies agency-wide. Case in point: just 34 percent of agencies that have lost data use data loss prevention (DLP) technology across their environment, compared with 65 percent of agencies that have not. Only a third of agencies give themselves an "A" rating for DLP.

"The recent Vault 7 Wikileaks release shone a harsh spotlight squarely on the insider threat issue," says Steve O'Keeffe, founder, MeriTalk. "Our study found that half of agencies report that unauthorized employees access protected information at least weekly. It's time to plug those holes. The potential consequences – from identity theft to national security crisis – are too dire."

Federal agencies see a clear path to insider threat prevention, the report found. To minimize data loss, respondents say agencies must limit access points (60 percent), adopt multi-factor authentication (50 percent), expand real-time activity monitoring (49 percent), implement data loss prevention capabilities (45 percent), and classify data (45 percent). The top investments planned for the next two years include user behavioral analytics, commercial threat intelligence, and anomaly detection tied with multi-factor authentication.

"Inside Job: The Sequel – The Federal Insider Threat Report" is based on an online survey of 150 Federal IT managers familiar with their agency's cyber security in March 2017. The report has a margin of error of ±7.97 percent at a 95 percent confidence level. To download the full report, please visit https://www.meritalk.com/study/inside-job-the-sequel/.

About MeriTalk

The voice of tomorrow's government today, MeriTalk is a public-private partnership focused on improving the outcomes of government IT. Focusing on government's hot-button issues, MeriTalk hosts Big Data Exchange, Cloud Computing Exchange, Cyber Security Exchange, and Data Center Exchange – platforms dedicated to supporting public-private dialogue and collaboration. MeriTalk connects with an audience of 115,000 government community contacts. For more information, visit www.meritalk.com or follow us on Twitter, @meritalk. MeriTalk is a 300Brand organization.

-30-