FOR IMMEDIATE RELEASE

Contact:
Lisa Fisher
703-883-9000, ext. 156
lfisher@meritalk.com

Nearly Half of Federal Agencies Were Targets of Insider Threats in the Last Year, Despite Formal Prevention Programs

New Report Examines Actions Agencies Should Take to Minimize Risk and Cyber Incident Consequences

Alexandria, Va., September 14, 2015 – MeriTalk, a public-private partnership focused on improving the outcomes of government IT, today announced the results of its new report, "Inside Job: The Federal Insider Threat Report." The study, underwritten by Symantec, reveals that while the vast majority of Federal agencies – 76 percent – are more focused on combating insider threats today than they were one year ago, 45 percent were a target of an insider threat and nearly one in three (29 percent) lost data to an insider incident in the last 12 months.

The "Inside Job" report surveyed 150 Federal IT managers familiar with their organization's cyber security efforts to examine the most common insider threats agencies face today, the strengths and weaknesses of insider threat programs, and how agencies can reduce the risks and consequences of this growing vulnerability.

Agencies are making a concerted effort to minimize insider threats – many respondents note their agencies run mock attacks or other test scenarios to better understand unintentional insider threat risks (51 percent) and offer annual online training (73 percent). However, most could improve the personal touch when it comes to education. Just 39 percent offer in-person security training and only 29 percent update their security protocol manuals for employee review.

The consequences are real. Fifty-one percent of respondents say it is common for employees to not follow appropriate protocols, and 40 percent say unauthorized employees access

-more-

government information they shouldn't at least once weekly – putting their agencies at significant risk.

In addition, agencies don't know what they don't know – 45 percent cannot tell if a document has been inappropriately shared, 42 percent cannot tell how a document was shared, and 34 percent cannot tell what data has been lost.

"There's no shortage of news stories underscoring the risks of government data breaches, particularly those perpetrated by insiders, whether malicious or unintentional. Agencies must take a holistic approach when implementing formal insider threat programs to battle this risk head-on," said Rob Potter, vice president, public sector, Symantec. "Investments in the right technology, as well as employee training and education, are critical."

Indeed, there is no one silver bullet to address this complex. Survey respondents are split in their opinion on the linchpin for preventing insider threat activity, with 40 percent citing end-user education and/or training, 40 percent citing security technology, and 20 percent citing additional controls and/or guidance.

"This isn't just about Snowden," said Steve O'Keeffe, founder, MeriTalk. "If you Google how to make a nuclear bomb – and don't do it from your PC – you'll see the dangers of exfiltration. Training can help – but we need security systems that are smarter by design."

Fifty-five percent of survey respondents say their agency has a formal insider threat program in place. These agencies are more likely to have annual in-person security training; real-time alerts for inappropriate access/sharing and data loss; and agency-wide security technologies.

Federal IT managers also believe that government-wide initiatives will help. Seventy-seven percent say that Presidential Cross-Agency Priority (CAP) goals will aid efforts to combat insider threats across agencies. Agencies' top CAP goals include enhancing security culture (47 percent), developing an insider threat prevention program (38 percent), and sharing adverse information (35 percent). Federal IT managers also believe ISCM (86 percent), CDM (82 percent), and DoD Directive 5205 (82 percent) will provide valuable support.

"Inside Job: The Federal Insider Threat Report" is based on an online survey of 150 Federal IT managers familiar with their agency's cyber security in July and August 2015. The report has a margin of error of ±7.97% at a 95% confidence level. To download the full report, please visit http://meritalk.com/insidejob.

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-