MeriTalk
Improving the Outcomes
of Government IT

Contact:
Kelsea Bond
kbond@meritalk.com
703-883-9000 x304

Shifting the Cyber Mindset from ‘Assume Breach’ to ‘Breach Prevention’ is Critical in Next Three Years, Say 91 Percent of Government Cyber Leaders

70 Percent Say HVAs Have Been Potentially Compromised in Last 12 Months;
93 Percent Say Zero Vulnerability Platforms are Possible

Alexandria, Va., July 27, 2021 – Ninety-one percent of cybersecurity leaders say they want to see their organization shift from ‘assume breach’ to breach prevention in the next three years, according to a new study from MeriTalk, a public-private partnership focused on improving the outcomes of government IT.

The study – which surveyed more than 300 cybersecurity leaders across Federal, state, and local government – found that 83 percent of public sector organizations operate on an ‘assume breach’ model today. Seventy percent estimate their high-value assets (HVAs) have been compromised in the past 12 months, and fifty percent believe there will be a cyber 9/11 in the next 10 years.

But it’s not all bad news. The study – underwritten by INTEGRITY Global Security (IGS) – found that 93 percent of leaders believe it is possible to build zero vulnerability platforms. They say a major shift in prioritized focus will be necessary to get there. Today, 61 percent of cyber decision makers report their organization focuses most cyber resources on detection, confinement, or remediation, 39 percent say their primary focus is on prevention.

“Cyber leaders are underwater, but it is possible that we can move toward a reality where breaches are not a given,” said Jimmy Sorrells, President, INTEGRITY Global Security (IGS). “The industry needs to know that there are zero vulnerability platforms available, and those platforms are the key to helping our public servants better protect critical systems and citizens. It is going to take a stronger commitment to cyber hygiene, platform security, and breach prevention to make real progress. We cannot continue to do the same things and expect different results.”

While 98 percent of respondents are taking steps to improve risk management, just half are reporting progress on foundational cyber hygiene, including enforcing multi-factor authentication and encryption, deploying endpoint detection and response systems, and auditing hardware security. Only 45 percent of organizations have developed a prioritized list of HVAs.

Eighty-nine percent of respondents say further prioritizing platform security is a key step toward breach prevention. It will help organizations improve ability to isolate critical infrastructure from vulnerable devices, as well as reduce exposure and risk.

To make the shift successfully, government cyber leaders say they need:

- Centralized access to cybersecurity data and analytics (91 percent)
- Improved vulnerability management (90 percent)
- Hardened endpoint devices (89 percent)

-more-

- Fundamental culture change (89 percent)
- Increased investments in zero vulnerability solutions (89 percent)

The *Containing the Cyber Threat Tsunami* report is based on an online survey of more than 300 government cybersecurity leaders across Federal, State, and Local organizations. The report has a margin of error of ±9.54% at a 95% confidence level. To review the full findings, visit: https://www.meritalk.com/study/containing-the-cyber-threat-tsunami/.

About MeriTalk

The voice of tomorrow's government today, MeriTalk is a public-private partnership focused on improving the outcomes of government IT. Our award-winning editorial team and world-class events and research staff produces unmatched news, analysis, and insight. The goal: more efficient, responsive, and citizen-centric government. MeriTalk connects with an audience of 160,000 Federal community contacts. For more information, visit https://www.meritalk.com/ or follow us on Twitter, @MeriTalk. MeriTalk is a 300Brand organization.

###