Media Contact:
Christie Deane
MeriTalk
703-883-9000, ext. 103
cdeane@meritalk.com

Government Cyber Resiliency Survey Finds Reasons for Hope and Areas for Improvement

Only 18 percent of respondents grade their organization's current cyber resilience with an A

ALEXANDRIA, Va. – November 23, 2022 – Eighty-nine percent of Federal and 79 percent of state and local government IT decision-makers leaders say heightened world tensions have led to an increased focus on cyber resilience within their organization. However, just 18 percent give their organization's current cyber resilience an A grade, according to a new study sponsored by Splunk and conducted by MeriTalk, a public-private partnership focused on improving the outcomes of government IT.

Cyber resilience is the ability to anticipate, withstand, and recover from cyber incidents while delivering essential services. To explore how prepared the government is to deliver vital services in the face of an attack, MeriTalk surveyed 310 Federal, state, and local government IT decision-makers familiar with their organization's cybersecurity.

The resulting report, "Cyber Resiliency: Sustaining Government Operations in Complex Threat Environments," developed in partnership with Splunk, explores operational threats, efforts to improve visibility and security, investment priorities, existing challenges, and the capacity for cyber resilience across government. Government and industry experts will further explore these themes through a series of panel discussions, breakout sessions, and networking events at Splunk's GovSummit, "Mission Possible: Cyber Resilience for Every Mission," on December 14 in Washington, D.C. Registration is now open.

The study found disparities in cyber resilience at different levels of government. Federal agencies were three times more likely than state and local organizations (27 percent compared to 9 percent) to grade their current cyber resilience with an A. However, fewer than 40 percent of leaders in either group were "very confident" in their organization's ability to maintain vital services in the face of cyberattacks, insider threats, infrastructure outages, and critical application failures.

Eighty-seven percent of respondents said improved visibility is the foundation of improved resilience. "We cannot underestimate the importance of visibility," said Bill Rowan, Vice President of Splunk Public Sector - Americas. "Quite simply, agencies cannot secure what they cannot see. Enterprisewide visibility across cloud and on-premises environments is a baseline requirement for cyber resilience."

IT leaders did report progress toward cyber resilience over the past two years. Approximately half of the respondents saw an increased ability to mitigate risk, and about 45 percent experienced improved time to action. In other areas, there was a noticeable gap between Federal and state and local responses. Increased end-to-end visibility and improved consistent trust were both at 30 percent for state and local governments, compared to 47 percent for Federal agencies.

Despite the improvements, 94 percent of the respondents still face challenges that impede progress toward cyber resilience, including:

- Lack of support from top decision-makers
- Complicated Federal mandates
- Outdated, "check the box" resilience mentalities
- The increasing complexity of technology environments
- Lack of funding for investments
- Lack of consistent resilience strategies
- Manual, disjointed workflows

The study also found that government agencies often experience a general lack of understanding about what constitutes resilience. Eighty-two percent of those surveyed said their organization still associates the concept of resilience with basic compliance and risk management.

"The idea of resilience needs to be rebranded within government," said Bill Rowan, Vice President of Splunk Public Sector – Americas. "Organizations must continually promote modern resilience in terms of their ability to prevent, respond, and quickly recover from disruptions like cyberattacks, insider threats, infrastructure outages, or critical application failures."

Understanding resilience was at the heart of another striking finding. While 77 percent of respondents believe their efforts around security, IT, and workforce development resilience are at least somewhat integrated, 65 percent saw workforce as the weakest link. IT decision-makers cited numerous workforce-related stumbling blocks – including insufficient staff, staff turnover, and lack of familiarity with technology – underscoring the importance of training and retention efforts.

"Cyber Resiliency: Sustaining Government Operations in Complex Threat Environments," is based on an online survey of 310 Federal, state, and local IT decision-makers familiar with their organization's cybersecurity in September 2022. The survey has a margin of error of ±5.52 percent at a 95 percent confidence level. To review the full findings, view the report.

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 produce 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 www.MeriTalk.com or follow us on Twitter, @MeriTalk. MeriTalk is a 300Brand organization.

###