



Contact:

Emily Wood

ewood@300brand.com

(703) 883-9000 ext. 127

Ben Waring

RSAConf@shiftcomm.com

New Research Affirms National Cybersecurity Strategy’s Vision: 90% of Cyber Decision-Makers See Public-Private Partnerships as a Force Multiplier in Cyber Resilience

Forty-seven percent of cybersecurity decision-makers say their organization proactively responded to a threat thanks to shared cybersecurity intelligence

Alexandria, Va., April 10, 2023 – Nine out of ten cybersecurity decision-makers (90 percent) see public-private partnerships as a force multiplier in cyber resilience but only 40 percent find current partnerships very effective, according to a new study from [MeriTalk](#), government IT’s top digital platform, and [RSA Conference](#), the world’s leading information security conferences and expositions.

The study – which surveyed 100 Federal and 100 private sector cybersecurity decision-makers – found the biggest roadblocks to effective data sharing are a lack of training, trust, resources, and specific information sharing requirements. Seventy-one percent of cyber decision-makers feel their organization underutilizes their relationships when sharing and acting on cybersecurity intelligence and 75 percent say there is still some reticence in their organization around cyber information sharing, with public sector employees significantly more likely than private sector employees to hold back (91 percent to 56 percent).

Despite challenges, the majority of cybersecurity decision-makers say the volume and value of shared cyber intelligence has improved over the past year. Additionally, forty-seven percent say their organization proactively responded to a threat thanks to shared cybersecurity intelligence and forty percent patched a vulnerability.

Cyber decision-makers say Federal government agencies – namely the Cybersecurity and Infrastructure Security Agency (CISA) – and Information Sharing and Analysis Organizations (ISAOs)/Information Sharing and Analysis Centers (ISACs) are the best resources for trusted and

actionable cybersecurity intelligence. Still, just forty-three percent of small organizations say they reported a cyber incident they experienced to a Federal agency or field office in the past year, compared to eighty-two percent of medium organizations and ninety-one percent of large organizations. Small and medium organizations say improved Federal government resource centers are their number one recommendation to help increase cybersecurity resilience for organizations of their size.

“Continuing to improve information sharing between public and private sector organizations of all sizes is key to cyber progress,” said Nicole Burdette, principal, MeriTalk. “The recent [National Cybersecurity Strategy](#) confirms what the data reveals, the Federal government can and should incentivize good cyber habits. The hard work will be ahead in terms of enabling and encouraging real trust and collaboration.”

“The stakes are high for effective collaboration across public and private organizations,” said Britta Glade, Vice President, Content & Curation, RSA Conference. “To really move the needle for global institutions, large and small, we must better address this collaboration with particular attention on SMBs, who are faced with starkly different experiences and challenges, as reflected in this research.”

Going forward, public sector leaders should focus on data centralization, strategic planning, and improved government resource centers for small and medium organizations, while private sector leaders should prioritize data delivery speeds and detailed instructions for responding to cyber intel.

Additional recommendations for organizations and policy makers across the digital ecosystem include:

Near-term:

- Develop a strategic plan for improved information sharing – appoint a team to develop a step-by-step roadmap for gathering, analyzing, and disseminating cyber threat intelligence
- Conduct biannual training for end users and IT – educate end users on the importance of cybersecurity and their role in vigilance; IT should work with private and public partners to expand training



- Reach out to IT leaders from smaller organizations – bring smaller organizations into the fold to improve our collective resilience

Mid-term:

- Define and promote a culture of collaboration – establish internal cybersecurity intelligence teams with representatives from multiple departments
- Centralize cybersecurity intelligence – develop and circulate a shared repository of security issues, vulnerabilities, and exploits
- Build trust with every exchange – ask cyber leaders what makes a piece of information trustworthy and what would make them feel more comfortable sharing information externally

Long-term:

- Prioritize investments in modernization – rearchitect, rebuild, or replace legacy technology to set the foundation for sharing and ingesting machine-readable alerts, applying patches and universal updates, and seamlessly integrating with peers
- Incentivize healthy cybersecurity hygiene – consider tax credits or rebates, cybersecurity modernization funding, and awards programs for cyber leaders
- Innovate and stay vigilant – reassess cyber goals annually and stay up to date with industry best practices through webinars and conferences

The *A Foundation of Collaboration: Enhancing and Acting on Shared Cybersecurity Intelligence* report is based on an online survey of 100 Federal and 100 private sector cybersecurity decision-makers in January and February 2023. The study is underwritten by presenting sponsor [Carahsoft](#), as well as [Axonius](#), [Fortinet Federal](#), [Invicti](#), [Maximus](#), [Netskope](#), [RSA](#), [Tenable](#), [Trend Micro](#), and [Zscaler](#). The report has a margin of error of $\pm 6.93\%$ at a 95% confidence level. To review the full findings, visit: www.meritalk.com/study/foundation-of-collaboration

About MeriTalk

The voice of tomorrow's government today, MeriTalk is government IT's top digital platform. 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 www.meritalk.com or follow us on Twitter, @MeriTalk. MeriTalk is a [300Brand](#) organization.

About RSA Conference

RSA Conference™ is the premier series of global events and year-round learning for the cybersecurity community. RSAC is where the security industry converges to discuss current and future topics and gain access to the experts, unbiased content and ideas that enable individuals and companies to advance their cybersecurity posture and build stronger and smarter teams. Both in-person and online, RSAC brings the cybersecurity industry together and empowers the collective “we” to stand against cyberthreats around the world. RSAC is the ultimate marketplace for the latest technologies and hands-on educational opportunities that help industry professionals discover how to make their companies more secure while showcasing the most enterprising, influential and thought-provoking visionaries and leaders in cybersecurity today. For the most up-to-date news pertaining to the cybersecurity industry, visit www.rsaconference.com. Where the world talks security.