MeriTalk
Improving the Outcomes
of Government IT

RSAConference™

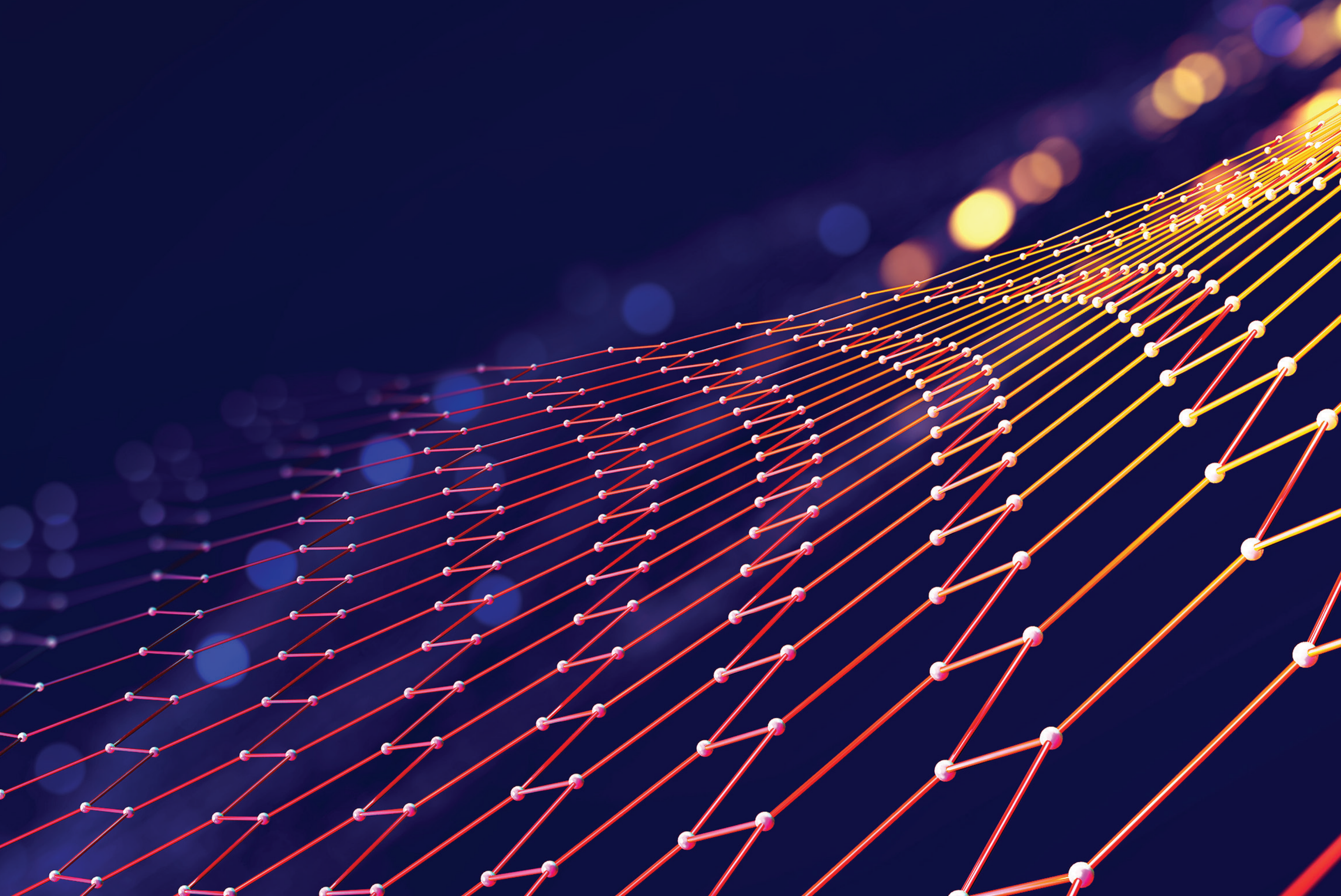
Underwritten by:

netskope

A Foundation of Collaboration:

Enhancing and Acting on Shared Cybersecurity Intelligence

April 2023



Introduction

As threat environments become increasingly complex, the White House recognizes the need for a "more intentional, more coordinated, and more well-resourced approach to cyber defense." The March 2023 National Cybersecurity Strategy affirms "robust collaboration, particularly between the public and private sectors, is essential to securing cyberspace." In short, we're all in this together.

To assess the role of public-private partnerships as a force multiplier in cyber resilience, MeriTalk and RSA Conference surveyed 100 Federal and 100 private sector cybersecurity decision-makers. We examined key communications roadblocks and actionable opportunities to enhance collaboration and data sharing – not just between the public and private sectors, but across the cyber ecosystem, including small and medium-sized organizations.[1]

The study explores:

- Progress over the past year, including strategic information-sharing and its effectiveness
- Opportunities for enhancing the speed and value of content exchanged
- Top barriers across people, processes, and technology that continue to impede collaboration
- Perceptions on recent Federal legislation, such as the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA)
- Recommendations for near-, mid-, and long-term actions

For this research, we define **public-private partnerships** as two or more public and private sector organizations working together to improve national cyber and infrastructure resilience. We define **shared cybersecurity intelligence** as information shared directly with your organization from another organization (either public or private). This can include information about cybersecurity trends, threats, vulnerabilities, and more. Not included is information obtained through sources such as news articles or public announcements.

[1] For this research, we define small organizations as those with fewer than 500 employees, medium organizations as those with 500-999 employees, and large organizations as those with 1,000 employees or more

Executive Summary

Shared cybersecurity intelligence bolsters national defense:

90%

Nine out of 10 cyber decision-makers (90%) see public-private partnerships as a force multiplier in cyber resilience

The majority of cyber decision-makers agree the volume and value of shared cyber intelligence has improved over the past year and **47%** say their organization proactively responded to a threat thanks to shared cybersecurity intelligence

Cyber decision-makers see Federal government agencies, particularly the Cybersecurity and Infrastructure Security Agency (CISA), as the **best resources** for trusted and actionable cybersecurity intelligence

Despite progress, public-private partnerships still lack efficacy:

40%

Just 40% of cyber decision-makers find current partnerships very effective, with small and private sector organizations least likely to find them valuable

When it comes to sharing and acting on cybersecurity intelligence, **71%** say their organization underutilizes relationships

Decision-makers say the **biggest roadblocks** to effective data sharing are a lack of training, trust, resources, and specific information sharing requirements

Cyber decision-makers need to divide and conquer the most urgent needs:

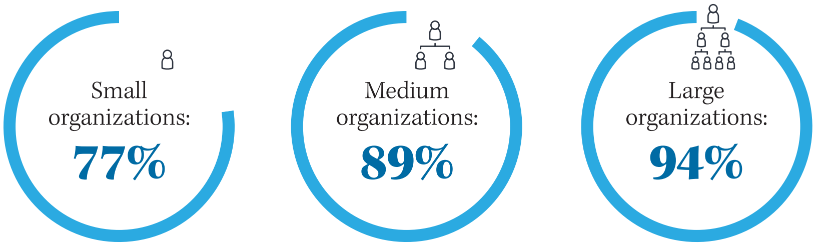
Small organizations call for a strategic plan for **coordinated threat response**, medium organizations need a centralized repository of shared cybersecurity intelligence, and large organizations want faster data delivery

To maximize their impact on the nation's shared cybersecurity posture, 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 refine instructions for responding to cyber intel

Public-Private Partnerships – Effectiveness Varies

Public-private partnerships are designed to mitigate cyber risks through coordinated information sharing, threat detection, and incident response. Current efforts are **working better for some than others**, with cyber decision-makers from small organizations least likely to find the relationships constructive.

Nine out of 10 cyber decision-makers (90%) feel public-private partnerships are a force multiplier in cyber resilience



Still, just 40% of cyber decision-makers feel public and private sector organizations are very effective at working together to mitigate cyber risks – with no significant change from 2022[2]

38% say the efforts are somewhat effective and **22%** say somewhat or very ineffective

Private sector decision-makers are significantly less likely than those from the public sector to find the partnerships very effective **(24% to 55%)**

Small organizations are three times less likely than medium and large organizations to find the partnerships very effective **(14% to 45% and 45%, respectively)**

[2] MeriTalk and RSA Conference's Reimagining Public-Private Partnerships: Minimizing Systemic Risk and Transforming National Cybersecurity Resilience

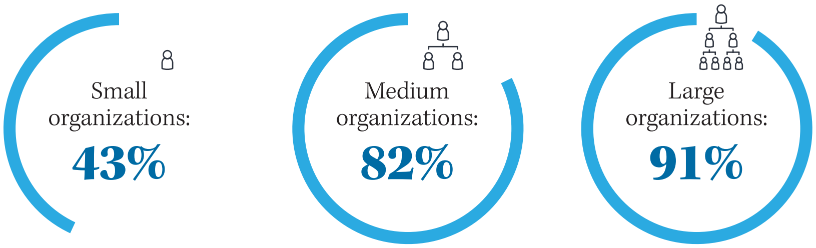
Information-Sharing Impacts

The good news? **One hundred percent** of cyber decision-makers from public sector organizations and 96% of those from private sector organizations say they've experienced at least one benefit from shared cybersecurity intelligence.

What threat information are organizations actively sharing?[3]

Malware	**47%**
Cybersecurity lessons learned	**41%**
Phishing threats	**40%**
Viruses	**38%**
Data theft	**32%**
Threats to critical infrastructure	**31%**

After experiencing a cyber incident, how many report it to a Federal agency or field office?



Small organizations: **43%**

Medium organizations: **82%**

Large organizations: **91%**

What has your organization achieved thanks to shared cybersecurity intelligence?[3]

Educated staff on a threat	**50%**
Proactively responded to a threat	**47%**
Fine-tuned overall cybersecurity posture	**45%**
Evaluated most important assets for protection	**41%**
Patched a vulnerability	**40%**
Deepened trust with public-private partners	**33%**

[3] Respondents asked to select all that apply

Progress Markers

Cyber decision-makers agree both the **volume and value** of the cybersecurity intelligence they're receiving has increased over the past year, with public sector decision-makers and those from large organizations most likely to report a significant improvement.

What is one change your organization made in the past year to improve its ability to collaborate on shared cybersecurity intelligence?

"**Worked with CISA** to standardize information sharing, improve quality, and create confidence in feeds."
– Large public sector organization

"Established an internal **cybersecurity intelligence sharing team** composed of representatives from multiple departments to coordinate and manage shared intelligence."
– Large public sector organization

"Conducted **regular training sessions** for staff to ensure they understand the importance of sharing intelligence and the protocols for doing so."
– Large public sector organization

"Several members of our cybersecurity team joined **multiple outside organizations** such as local chapters, InfraGard, and others."
– Small private sector organization

"Invested in a better threat intelligence service and are **refining our internal process** to anonymize and classify incident data to ensure appropriate sharing through a threat intelligence feed."
– Medium private sector organization

"Better **coordinated with our legal department** to facilitate ease of intelligence sharing."
– Large private sector organization

Culture of collaboration – Those who strongly agree collaboration is a core principle of their organization are significantly more likely than others to find public-private partnerships very effective **(53% to 33%)**

Trusted Resources

Cyber decision-makers see **Federal government agencies** and Information Sharing and Analysis Organizations (ISAOs)/Information Sharing and Analysis Centers (ISACs) as the best resources for trusted and actionable cybersecurity intelligence.

Where is the most actionable and trusted cybersecurity intelligence coming from?[4]

#1	Federal government agencies (CISA, NSA, FBI, etc.)	**(34%)**
#2	ISAOs/ISACs	**(26%)**
#3	Large private sector organizations	**(18%)**
#4	Small or medium private sector organizations	**(11%)**
#4	State or local government organizations	**(11%)**

Large organizations are nearly three times as likely as small organizations to see ISACs as their lead resource **(31% to 11%)**

Small organizations are significantly more likely to see large private sector organizations as their best informant **(34% to 14%)**

Which Federal government agency provides the most actionable and trusted intelligence?[5]

#1	Cybersecurity and Infrastructure Security Agency (CISA)	**60%**
#2	Federal Bureau of Investigation (FBI)	**18%**
#3	National Security Agency (NSA)	**15%**
#4	National Institute of Standards and Technology (NIST)	**7%**

[4] Respondents were asked to select one

[5] Those who said Federal government agencies offer the most actionable and trusted intelligence were asked to further specify which Federal government agency provides the best information

Remaining Roadblocks

Despite progress, **71%** of cyber decision-makers feel their organization underutilizes their relationships when sharing and acting on cybersecurity intelligence. **Seventy-five 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% to 56%)**.

Top people-related challenges:[3]

#1 Lack of training/education for end users **(39%)**

#2 Lack of trust in intelligence from outside sources **(36%)**

#2 Lack of training/education within the IT department **(36%)**

#4 Lack of trust in outbound intelligence to the source **(30%)**

#5 No clear contact for sharing cybersecurity intelligence **(26%)**

Small organizations are more than twice as likely as large organization to say they lack a clear contact **(49% to 22%)**

Top process-related challenges:[3]

#1 Lack of specific information sharing requirements **(35%)**

#2 Challenges having to report to multiple organizations **(32%)**

#2 Lack of effective policy/legislation **(32%)**

#4 No clear process for sharing relevant findings externally **(29%)**

#4 Concerns that information is not truly anonymized **(29%)**

Top technology-related challenges:[3]

#1 Budget shortfalls to update existing/legacy technology **(34%)**

#1 Lack of technology to share alerts **(34%)**

#3 Lack of technology to ingest alerts **(33%)**

#4 Lack of technology to apply patches or updates universally **(32%)**

#5 Fear of modifying essential software or infrastructure **(31%)**

Public sector decision-makers are significantly more likely to report budget shortfalls **(43% to 25%)** and a lack of technology for universal updates **(41% to 22%)**

Of the three factors listed below, what do you see as the single biggest barrier to improving shared cybersecurity intelligence?[4]

#1 Regulations	**38%**
#2 Liabilities	**35%**
#3 Legal/Policies	**27%**

Public sector decision-makers are significantly more likely to point to regulations **(47% to 29%)**, where private sector decision-makers point to liabilities **(44% to 25%)**

Urgent Needs and Desired Leadership

Many hands make light work. To improve public and private collaboration on shared intelligence, cyber decision-makers recommend **dividing** the most urgently needed actions between leadership teams.

Public sector to-do list:

- Centralized repository for shared cyber intel (**50%** urgent need, **91%** total need)
- Formal, overarching cybersecurity strategy that bridges the public and private sector (**47%** urgent need, **94%** total need)
- Strategic plan for coordinated threat response (**46%** urgent need, **91%** total need)
- Series of universal alert codes that denotes urgency (**42%** urgent need, **86%** total need)

Private sector to-do list:

- Accelerated data delivery (**52%** urgent need, **90%** total need)
- Outline of specific steps to take delivered alongside cyber intel (**42%** urgent need, **88%** total need)

Joint to-do list:

- Shared best practices on acceptable liability mitigation and indemnification (**48%** urgent need, **92%** total need)
- Simplified incident reporting procedures (**48%** urgent need, **91%** total need)
- Shared cybersecurity technologies/services (**46%** urgent need, **89%** total need)
- Help implementing universal frameworks such as the NIST Risk Management Framework (**46%** urgent need, **88%** total need)
- Signed mutual trust agreements between the public and private sector (**46%** urgent need, **86%** total need)
- Formal documentation of policies and procedures to address specific risks (**42%** urgent need, **88%** total need)

Needs vary by size:

Large organizations are significantly more likely than small organizations to say faster data delivery (**58% to 37%**), signed mutual trust agreements (**53% to 29%**), and help implementing universal frameworks (**52% to 29%**) are urgent needs

89% say the government should do more to incentivize healthy cybersecurity hygiene

Legislative and Technical Outlook

Looking ahead, cybersecurity decision-makers say **CISA's** proposed cyber threat intelligence exchange platform, Threat Information Enterprise Services (TIES), and data protection technologies will have the biggest impact on public-private cyber resilience over the next five years.

What do you see as the most impactful Federal legislation or effort over the next five years?[6]

#1 TIES, CISA's proposed cyber threat intelligence exchange platform	**52%**
#2 Strengthening American Cybersecurity Act of 2022	**47%**
#3 Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA)	**44%**

Public sector decision-makers are significantly more likely than private sector decision-makers to see promise in the:[6]

- Federal Rotational Cyber Workforce Program Act of 2021 (**53% to 24%**)
- Infrastructure Investment and Jobs Act (**51% to 19%**)
- State and Local Government Cybersecurity Act of 2021 (**51% to 33%**)
- CISA's Shields Up campaign (**47% to 25%**)

Which types of cybersecurity solutions do you think will have the biggest impact on intelligence gathering and collective response over the next five years?[3]

Data protection	**53%**
Security analytics	**47%**
Security automation	**46%**
Security information and event management (SIEM)/ security orchestration, automation, and response (SOAR)	**45%**
Identity and access management (IAM)	**45%**
Network/endpoint detection	**39%**
Application security	**35%**
Zero trust	**35%**

[6] Percentage who expect each effort to play a "major role" in the nation's shared cyber resilience

Spotlight on Small and Medium Organizations

Today's world of interconnected digital systems requires **all organizations** to be vigilant, regardless of size. Larger organizations can help smaller ones by making sure they are properly informed and protected.

Small and medium organizations: How should large private companies and the Federal government help you increase your cybersecurity resilience?[3]

#1 Improved Federal government resource centers for organizations our size	**48%**
#2 Cybersecurity services provided by large companies	**40%**
#3 Better representation in ISAOs/ISACs	**39%**
#4 Universal cybersecurity scan results shared with organizations our size	**38%**
#5 Federal incentive program specific to organizations our size	**36%**

> "As we bring in more companies and more new cybersecurity professionals, we need to make it **easy for them** to come up to speed. Right now, there is a lot of fumbling in the dark trying to find the right information sources. The United Kingdom's National Cyber Security Centre (NCSC) is a good example of an org making it easier for SMBs and newer professionals to find things."
> – Small private sector organization

Stronger Together

If you could tell your public or private sector counterparts **one thing** about how to improve the usability of shared cybersecurity intelligence, what would it be?

“Develop a **centralized** repository of cybersecurity intelligence and real-time intel sharing between security analysts, engineers, and management teams.”
– Medium public sector organization

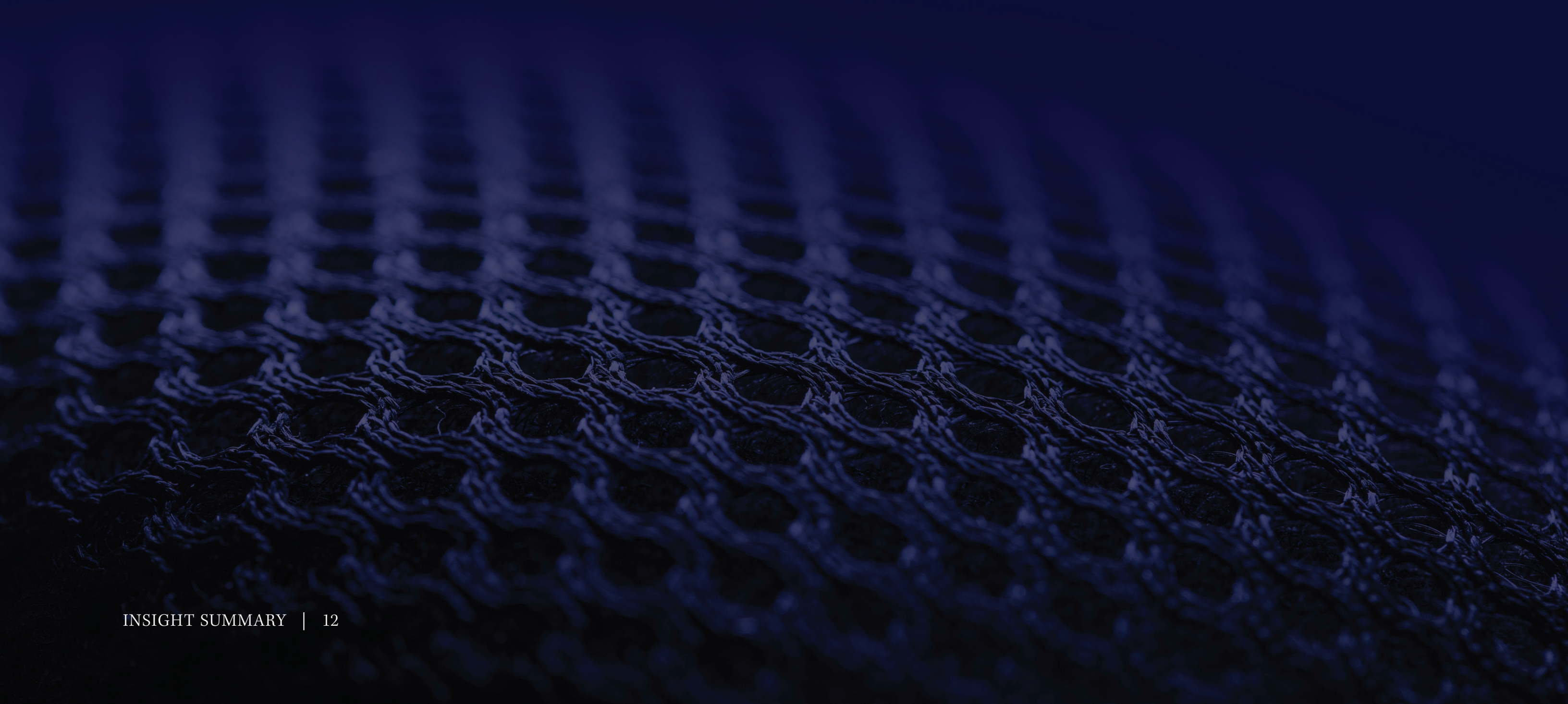
“A shared repository as well as a web forum where IT experts can **chat in real time** about threats would go a very long way in fixing this problem. If experts could send out alerts or chat in real time during an attack, that would be huge.”
– Small private sector organization

“Design and implement a **common language** and taxonomy for sharing and understanding cybersecurity intelligence.”
– Large public sector organization

“The public sector needs to have **more trust** with the private sector. The slow release of declassified information is often too late for private sector usefulness. The private sector completely understands how it affects the national security posture but has little faith in the equality of the partnership; a one-sided relationship is far from healthy.”
– Medium private sector organization

“Designate an **internal team** to manage shared intelligence in order to ensure the data is accurate, up-to-date, and actionable.”
– Large public sector organization

“Everything is becoming so interconnected and intertwined that if one goes down, more will as well. It is in our **shared best interest** to work together to … provide greater cybersecurity, as the need will only increase going forward.”
– Medium private sector organization



Recommendations

Near-term:

- **Develop a strategic plan for improved information sharing.** Appoint a team of the brightest cyber minds from across your organization to develop a step-by-step roadmap for gathering, analyzing, and disseminating cyber threat intelligence. Details should include which indicators to monitor, what constitutes an alert worth sharing, how to prepare the information, which data points to include, which points of contact to share it with, and how to deliver it.

- **Conduct biannual training for end users and IT.** For end users, educate them on the importance of cybersecurity and their role in vigilance. Explain how to identify threats, show examples of common cyber exploits, and review the process for alerting leadership to any issues. For IT, work with private and public sector partners to expand available training and credential programs. Additionally, schedule biweekly meetings on current threat indicators and expected impacts.

- **Reach out to IT leaders from smaller organizations.** With just 14% of small organizations feeling public-private partnerships are very effective, cyber leaders from large public and private sector organizations must bring smaller organizations into the fold to improve our collective resilience. Identify a contact locally or through LinkedIn, schedule quarterly meetings to trade details on cybersecurity strategies and challenges, and discuss how to improve ongoing information sharing. Federal government leaders should also work to make resource centers easier to use and share cyber services aimed at small organizations.

Mid-term:

- **Define and promote a culture of collaboration.** Cyber decision-makers who strongly agree collaboration is a core principle of their organization are significantly more likely to find public-private partnerships very effective. Begin by building bridges within your own organization – establishing internal cybersecurity intelligence teams with representatives from multiple departments to exchange and manage shared intelligence. Then deepen your engagement with resources including CISA's National Cyber Awareness System (NCAS), sector-specific ISAOs or ISACs, and local cybersecurity chapters.

- **Centralize cybersecurity intelligence.** Internally, cyber leaders should develop and circulate a shared repository of security issues, vulnerabilities, and exploits. Externally, public sector leaders should prioritize efforts such as CISA's Automated Indicator Sharing (AIS) capability and the proposed cyber threat intelligence exchange platform, TIES, to develop a singular, protected portal available to organizations of all sizes to catalog emerging threats, report vulnerabilities, and exchange best practices on preventing, mitigating, and recovering from cyber incidents.

- **Build trust with every exchange.** Seventy-five percent of cyber decision-makers say there is still some reticence in their organization around cyber information sharing. Bring this concern to light by asking fellow cyber leaders what makes a piece of information trustworthy and what would make them feel more comfortable sharing information externally. Communicate with reliable contacts, offer anonymity, and consider mutual trust agreements to improve confidence.

Long-term:

- **Prioritize investments in modernization.** Over the next five years, cyber decision-makers expect the biggest technological impacts for information sharing to come from data protection, security analytics, and security automation solutions. Effective, real-time information exchanges rely on modern, agile software and IT infrastructure. Rearchitecting, rebuilding, or replacing legacy technology will set the foundation for successfully sharing and ingesting machine-readable alerts, applying patches and universal updates, and seamlessly integrating with peers.

- **Incentivize healthy cybersecurity hygiene.** Cyber decision-makers say government organizations should do more to reward organizations with strong cybersecurity practices. Government leaders should consider tax credits or rebates, cybersecurity modernization funding, and awards programs for organizations not only protecting themselves, but helping the broader community gather, analyze, and disseminate cyber threat information.

- **Innovate and stay vigilant.** Living up to their name, malicious actors are constantly thinking of new ways to outmaneuver cyber defenders. To keep up and get ahead of them, organizations should reassess their cyber goals annually, stay up to date with industry best practices though webinars and conferences, and use public-private partnerships to not only inform each other of potential threats, but also to collaborate on the latest technologies and tactics for defense.

Methodology and Demographics

MeriTalk, in collaboration with RSA Conference, surveyed 100 Federal and 100 private sector cybersecurity decision-makers in January and February 2023. The resulting research has a margin of error of ±6.93% at a 95% confidence level.

Organization type:

- **50%** Industry or private sector business
- **41%** Federal government – Civilian agency
- **9%** Federal government – DoD or Intelligence agency
- Industries represented include cybersecurity/IT, financial services, software/hardware, healthcare, business services, manufacturing, utilities, and others

Organization size:

- **17%** Fewer than 500 employees
- **28%** 500-999 employees
- **40%** 1,000-4,999 employees
- **15%** 5,000 employees or more

Job title:

- **48%** C-suite (CIO, CTO, CISO, or other executive-level IT/IS decision-maker)
- **29%** Information Technology (IT), Information Security (IS), or Cybersecurity Director/Supervisor
- **7%** IT/IS or Cybersecurity Program Manager/Officer
- **4%** Data Center or Network Manager
- **4%** Cloud Specialist or Manager
- **3%** IT/IS or Cybersecurity Analyst/Engineer
- **2%** Software/Applications Development Manager
- **2%** IT/IS or Cybersecurity Specialist
- **1%** Other IT/IS or Cybersecurity Manager

100% of respondents make, contribute, or otherwise influence their organization's purchasing decisions for cybersecurity solutions

MeriTalk
Improving the Outcomes
of Government IT

RSAConference

Underwritten by:

netskope