



RSA
Conference


Underwritten by:



Reimagining Public-Private Partnerships:

Minimizing Systemic Risk and Transforming National Cybersecurity Resilience

May 2022



Introduction

Malicious cyber activity threatens both the **public and private sectors**. In today's world of connected digital systems, one vulnerability can bring down an entire chain of government agencies, businesses, and critical infrastructure. As President Biden notes, it will take a “whole-of-the-nation” approach¹ to address the danger.

MeriTalk and RSA Conference surveyed 100 Federal and 100 private sector cybersecurity decision-makers to explore the effectiveness of public-private partnerships today, uncover key perception gaps, and provide recommendations on strengthening collaboration and cyber resilience in the year ahead.

The study considers:

- How can the public and private sectors unite to protect the nation?
- Who is responsible for key elements of cyber defense?
- What tactics can we use to minimize systemic risk and supply chain ramifications?
- What impact are efforts like President Biden's Executive Order on Improving the Nation's Cybersecurity, the Cybersecurity and Infrastructure Security Agency's (CISA) Joint Cyber Defense Collaborative, and the recent Strengthening American Cybersecurity Act of 2022 having on information sharing and incident response?
- Where are we making inroads, and where is more progress needed?

¹Source: FACT SHEET: Biden Administration and Private-sector Leaders Announce Ambitious Initiatives to Bolster the Nation's Cybersecurity, <https://www.whitehouse.gov/briefing-room/statements-releases/2021/08/25/fact-sheet-biden-administration-and-private-sector-leaders-announce-ambitious-initiatives-to-bolster-the-nations-cybersecurity/>, August 25, 2021

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.



Executive Summary

Public-private partnerships need an overhaul:

While
93%

of cyber decision-makers say public-private partnerships are vital to national defense, just **one in three (34%)** believe they are very effective



When asked to grade current efforts, cyber **decision-makers give “C’s”** for coordinating incident response, protecting critical infrastructure, and identifying systemic risk – one of the biggest threats they see to national and economic security

Trust and complexity issues stifle information sharing:

While
92%

of organizations are actively sharing threat information with partners, **43%** feel it is more common for the private sector to share threat information with the government than the other way around

69%

say there is still some reticence in their organization around cyber information sharing, and just **41%** feel confident they have a direct line to a government agent/agency when needed



Top roadblocks? Concerns about data privacy, lack of trust, and lack of streamlined information-sharing requirements

Cyber decision-makers are looking to government to spearhead vital collaboration efforts:

95%

say improved information sharing will provide critical insight in an interconnected world and **97%** feel successful public-private partnerships are key to their organization’s cyber resilience



Most agree a government-led partnership is the way forward.


Top private sector responsibilities: developing innovative cyber tools and patching vulnerabilities; **top public sector responsibilities:** defending against international cyber attacks and punishing those responsible




Most impactful strategies for the future? Modernizing legacy systems, adopting identity strategies, and implementing zero trust architectures

Public-Private Partnerships – Are They Working?

Effective public-private partnerships mitigate cyber risks through coordinated information sharing, threat detection, and incident response. While nearly all cyber decision-makers view this collaboration as critical, just one in three see today's efforts as very effective.

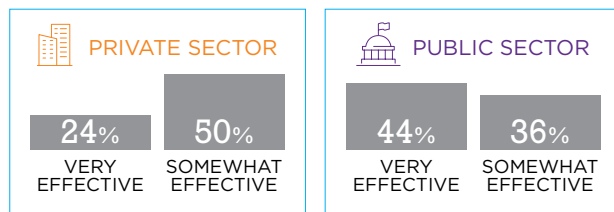
93% feel public-private partnerships are **vital** to national cyber defense 

91% feel systemic risk is one of the biggest threats to national and economic security 



Just **one in three** (34%) believe public-private partnerships are **very effective** at working together to mitigate cyber risks

Private sector decision-makers are significantly less likely than the public sector to **find the partnerships very effective**



When asked to grade current efforts, cyber decision-makers say today's public-private partnerships average a C+

Public-Private Partnership Report Card:	
Overall score	C+ (2.4 GPA)
Sharing threat information	B- (2.6)
Identifying systemic risk	C+ (2.4)
Coordinating incident response	C+ (2.4)
Protecting critical infrastructure	C+ (2.3)
Private sector decision-makers graded all four factors lower than the public sector	



Communication is Key

When it comes to sharing threat information, cyber decision-makers claim it is more common for the private sector to share threat information with the government than the other way around.

Which is more common?

43% The **private sector** shares threat information with the government

30% There is an **equal** exchange of information

23% The **government** shares threat information with the private sector

4% Unsure

92% of organizations are actively sharing threat information with partners, including:¹

58% CISA

49% Information sharing groups/Information Sharing and Analysis Centers (ISACs)

40% National Security Agency (NSA)

38% Federal Bureau of Investigation (FBI)

29% Other private sector organizations

17% Other public sector organizations

What threat information is your organization actively sharing?¹

66% Malware

52% Phishing threats

52% Ransomware

51% Viruses

44% Supply-chain related threats/implications

32% Lessons learned

¹ Respondents asked to select all that apply

69% 


say **there is still some reticence** in their organization around cyber information sharing

Exploring Ownership

Most cyber decision-makers are looking to the government to lead public-private collaboration efforts. Still, there is little consensus on the best approach.

What is the ideal way for public and private organizations to work together to reduce cyber risk?

29% **Government-led** committee of private and public cybersecurity leaders 

21% **Government-issued** directives for both public and private organizations 

20% Private organization-led committee of public and private cybersecurity leaders

22% Both sectors work individually, only sharing information that is believed relevant

5% Organizations focus on individual customer/vendor relationships

3% Other

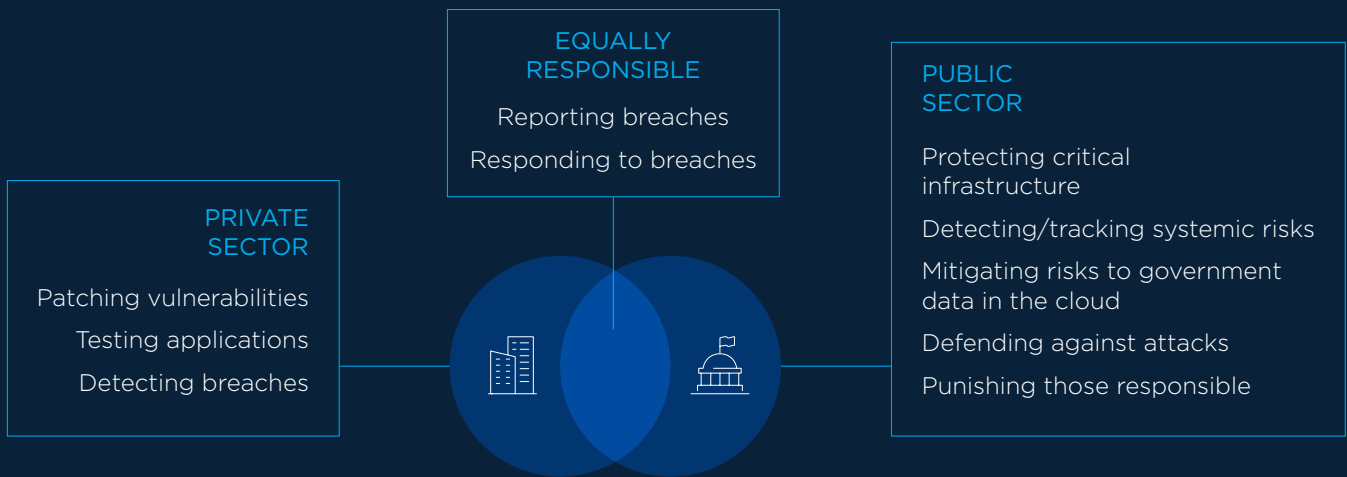
Private sector decision-makers prefer a **government-led committee**



Public sector decision-makers prefer for **both sectors to work individually**

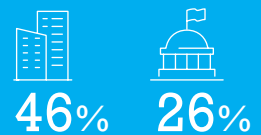


Who is more responsible for each of the following?

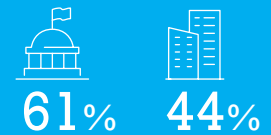


Organizations are significantly more likely to **put the onus for testing and patching on their own sector** than the other side

Private sector organizations are significantly more likely to put the responsibility of mitigating risk to **government data in the cloud** on the public sector,



while the public sector is significantly more likely to say it **should be equal**



Where should the support come from?

Who is more responsible?



Relationship Roadblocks

Cyber decision-makers agree data privacy concerns and trust issues hold public-private partnerships back.

What are the biggest challenges?¹

- 51%** Concerns about data privacy
- 45%** Lack of trust between the public and private sector
- 42%** Lack of streamlined information-sharing requirements
- 41%** Challenges having to report to multiple organizations
- 37%** Differing cultures/priorities

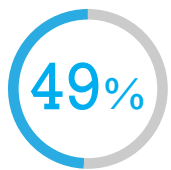
Private sector decision-makers are significantly more likely than the public sector to see **differing cultures/priorities** as a roadblock



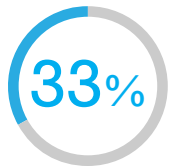
44%



29%



Just 49% of **public sector** decision-makers and

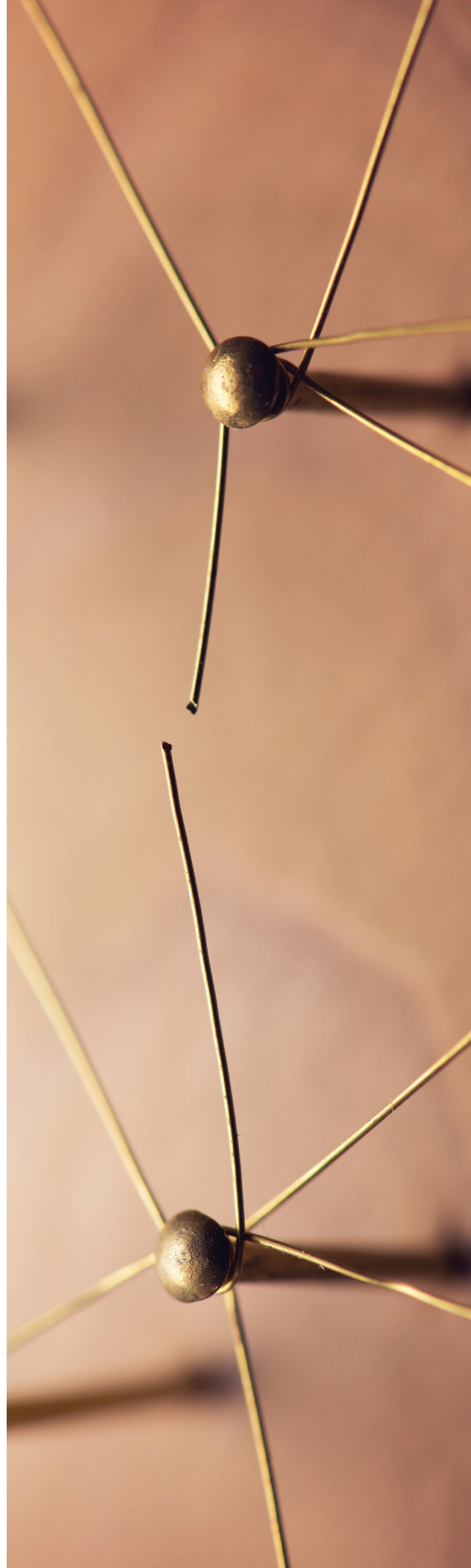


of **private sector** feel confident their organization has a **direct line** to a government agent/agency for sharing threat information

84%

see value in public and private sector organizations signing mutual trust agreements

¹ Respondents asked to select all that apply



EO Impact

The vast majority of public sector (95%) and private sector (73%) decision-makers say their **organization has been impacted** by President Biden's May 12, 2021, release of the Executive Order for Improving the Nation's Cybersecurity (cyber EO).

How has the cyber EO impacted your organization?¹



PUBLIC SECTOR

45% Created new methods for public-private collaboration

38% Provided a roadmap to improving cybersecurity

38% Enhanced our software supply chain security



PRIVATE SECTOR

41% Prompted a review of our incident response processes

29% Provided a roadmap to improving cybersecurity

29% Increased our threat information sharing

98% Nearly all cyber decision-makers (98%) are **working to minimize supply chain risks** – one of the key components of the cyber EO.



Top steps include:¹

46% Documenting a set of policies and procedures that address security, integrity, monitoring, resilience, and quality

45% Continually auditing the security practices of suppliers

45% Testing software before implementation/acceptance

43% Developing a list of critical components (e.g., hardware, software, and services) that enable the mission or business

42% Identifying suppliers and, when possible, their sources

42% Applying basic network segmentation where feasible

87% believe a Software Bill of Materials (SBOM) is an important tool for managing risk

¹ Respondents asked to select all that apply

Confidence in Cooperation

Overall, **97% feel successful public-private partnerships are key** to their organization's cyber resilience. This is especially true for government agencies, who are significantly more likely to say they are very important (81% vs 62%).

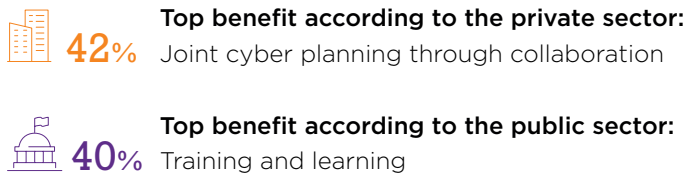
95% say improved information sharing will provide critical insight into how cyber risk manifests itself in an interconnected world



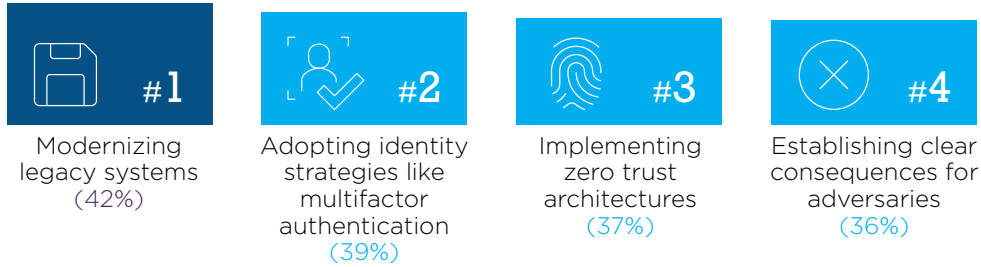
Most effective initiatives for mitigating threats?



Additionally, 93% feel there will be benefits to CISA's Joint Cyber Defense Collaborative (JCDC)²



Overall, which strategies will be most impactful for national cybersecurity resilience?³



² Respondents asked to select top four
³ Respondents asked to select top three



Perfecting the Partnership

What is **one thing** your organization needs to improve your collaboration with public or private sector organizations?

“ Share information early, simply, and as directly as possible without compromising sensitive or classified sources of information.”

“ Be open, transparent, and honest. It takes a completely trustworthy team to address cyber problems and issues.”

“ Don't dictate, don't make it hard, don't be untrusting. Do work together, do think outside the box, do make it easy.”

“ There are too many channels, too many players, too many leader committees of executives. Not enough sharing by technical people who actually do things.”

“ Collaboration is key. We all (public and private sector counterparts) need to work together in order to successfully mitigate cybersecurity threats. A piece of code can't run without its respective counterparts, neither can we as a nation.”



PUBLIC



PRIVATE

Recommendations

Clarify leadership responsibilities and build a unified strategy – then take action. While both public and private sector cyber decision-makers agree they share responsibilities for key defense measures, the majority would like to see the government lead efforts to improve coordination. That starts with developing a unified strategy that bridges both sectors and mandates immediate change. A mutually agreed-upon strategy should include a commitment from both public and private sector organizations to use initiatives like CISA's Joint Cyber Defense Collaborative as a central hub to enhance communication, minimize duplicate efforts, and execute on appointed responsibilities.

Assign a single point of contact to streamline communication. Today's cyber decision-makers claim it is more common for the private sector to share threat information with the government than the other way around. Both sides agree a lack of streamlined information-sharing requirements and the need to report to multiple organizations bottleneck efforts. Government leaders must simplify reporting procedures and appoint a single point of contact responsible for opening the flow of information and enabling decision-making at the speed of relevance.

Build transparency and mutual trust agreements. Concerns about data privacy and a lack of trust continue to stifle progress. Nearly seven out of ten cyber decision-makers still face reticence to share information – the bedrock of detecting threats and coordinating incident response. Transparency is needed from both sides to build trust. Leadership must solidify data privacy expectations and establish mutual trust agreements to combat hesitancy. This will encourage government agencies and private sector organizations to lower their walls and raise stronger defenses together.

Accelerate modernization and integration. Systemic risk is one of the biggest threats to our national and economic security. Going forward, cyber decision-makers from both sectors must accelerate modernization roadmaps, adopt identity strategies, and implement zero trust architectures to strengthen joint resilience. With the latest cybersecurity technologies and open lines of communications, public and private sector cyber leaders can go beyond simply sharing threat data to also share challenges, best practices, and lessons learned in the pursuit of modern cyber strategies. We are stronger together.

Methodology and Demographics

MeriTalk, in collaboration with RSA Conference, surveyed 100 Federal and 100 private sector cybersecurity decision-makers in April and May 2022. The resulting research has a margin of error of $\pm 6.93\%$ at a 95% confidence level.

Organization type:

- 50%** Industry or private sector business
- 32%** Federal government – Civilian agency
- 18%** Federal government – Department of Defense (DoD) or Intelligence agency

Private sector industries include cybersecurity/IT, financial services, software/hardware, healthcare, retail, manufacturing, and others.

Organization size:

- 23%** Less than 500 employees
- 24%** 500-999 employees
- 21%** 1,000-4,999 employees
- 32%** 5,000 employees or more

Job title:

- 36%** C-suite (CIO, CTO, CISO, or other executive-level IT/IS decision-maker)
- 28%** Information Technology (IT), Information Security (IS), or Cybersecurity Director/Supervisor
- 11%** IT/IS or Cybersecurity Program Manager/Officer
- 10%** Software/Applications Development Manager
- 7%** IT/IS or Cybersecurity Analyst/Engineer
- 3%** IT/IS or Cybersecurity Specialist
- 2%** Data Center or Network Manager
- 1%** Cloud Specialist or Manager
- 2%** 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

RSA
Conference

Underwritten by:

