MeriTalk

RSAC Cybersecurity, Together

The 2025 Collective Cyber Resilience Index

April 2025

Introduction

In today's interconnected world, cybersecurity resilience depends on **coordinated action** across sectors.

What steps are organizations taking to enhance **cyber collaboration**? How has reliance on external partnerships changed over the past three years? What role does collective action play in mitigating threats, improving response times, and securing critical infrastructure? And what challenges remain?

MeriTalk and RSAC surveyed **100 U.S. Federal and 100 U.S. private sector cybersecurity decision-makers** to examine how cybersecurity leaders are building cohesive defense strategies through modern security practices, community collaboration, and collective action.

The study explores:

- Breadth of shared cyberthreat intelligence
- Depth of supply chain and third-party risk monitoring
- Maturity of zero trust security implementation
- Adoption of shared cloud security and interoperability standards
- Integration of AI and automation for incident response
- Effectiveness of cross-sector cybersecurity initiatives

For this research, we define **collective cyber resilience** as coordinated efforts among organizations to withstand, adapt to, and recover from cyber threats.

Executive Summary

Collaboration is strengthening cyber defenses – but execution gaps limit impact:

85% of cybersecurity decision-makers surveyed say cross-organizational collaboration is essential to their cyber defense strategy, but only **35%** rate current strategies as highly effective

79% have increased engagement with external partners over the past three years, but participation is inconsistent

53% engage in government-led information-sharing; only **31%** take part in joint threat-hunting initiatives

---

AI and supply chain vulnerabilities present new risks:

99% of cybersecurity decision-makers surveyed have automated some portion of their vulnerability management, but only **33%** feel well-prepared to combat AI-driven cyberattacks

75% worry about overreliance on key technology providers

72% say inconsistent security practices across partners pose a greater risk to resilience than cyber adversaries

---

High-performing organizations drive resilience through deep collaboration and structured coordination:

40% of survey participants who rate their organization's collective resilience efforts as "excellent" share threat intelligence daily, compared to just **8%** of other organizations

77% have formal incident response coordination with all key partners, compared to **44%** of others

64% have implemented zero trust across most or all systems, compared to just **23%** of others

Rethinking Cyber Resilience

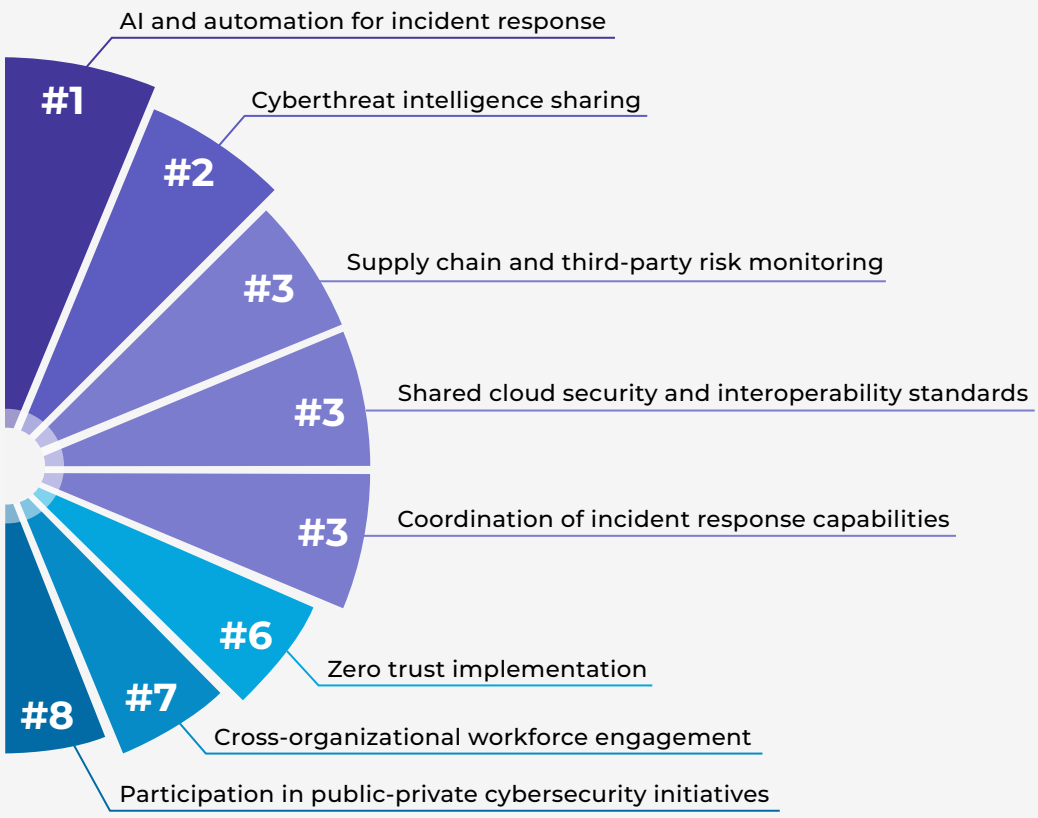
Cybersecurity decision-makers surveyed recognize the critical importance of cross-sector partnerships, but turning intent into action remains a challenge. While 85% agree that cross-sector partnerships are **essential**, just 35% consider current strategies highly effective – noting the need for improved AI adoption, threat intelligence sharing, and supply chain security.

85%
say cross-organizational collaboration is essential to their cyber defense strategy

And **79%**
say their collaboration with external cybersecurity partners has increased over the past three years

But just **35%** feel current strategies are “very effective”

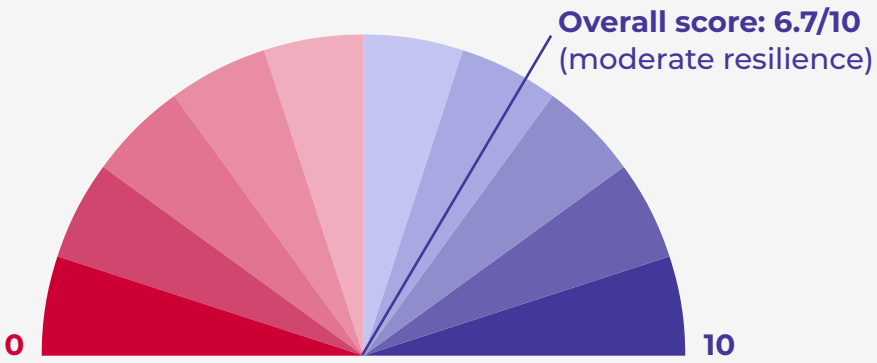
What do you see as the most critical component of collective cyber resilience?



The 2025 Index

The 2025 **Collective Cyber Resilience Index** (CCRI) provides a snapshot of mutual cybersecurity readiness, highlighting advancements in cross-sector collaboration while identifying opportunities to strengthen cloud security, supply chain risk management, and AI-driven defense strategies.

2025 CCRI



Collaboration 7.6

Measures engagement in cross-sector partnerships, effectiveness of collective resilience strategies, and perceptions of broader community coordination.

Intelligence Sharing 7.0

Assesses frequency of threat intelligence exchanges, incident reporting activity, and participation in government-led information-sharing initiatives.

Incident Response 6.8

Evaluates the strength of coordination protocols and frequency of joint response simulations with external partners.

Cloud & Zero Trust Security Standards 6.4

Tracks multi-cloud security efforts and progress in zero trust implementation.

Supply Chain Security 6.2

Reflects visibility into third-party vendor security and organizational continuity capabilities in case of a critical provider outage.

AI & Automation 6.1

Measures the extent of security automation and preparedness for AI-enabled cyber threats.

Despite AI and automation ranking as the No. 1 most critical component of collective cyber resilience, participating organizations report the lowest readiness in this area.

Expanding Cyber Collaboration

Participating cybersecurity decision-makers are increasingly reliant on **external intelligence**, yet involvement in public-private initiatives remains inconsistent. While 68% report greater dependence on external threat data, engagement varies – 53% take part in government-led information sharing, but only 31% are involved in joint threat hunting efforts.

68% say they are significantly more reliant on intelligence from external partners than they were three years ago

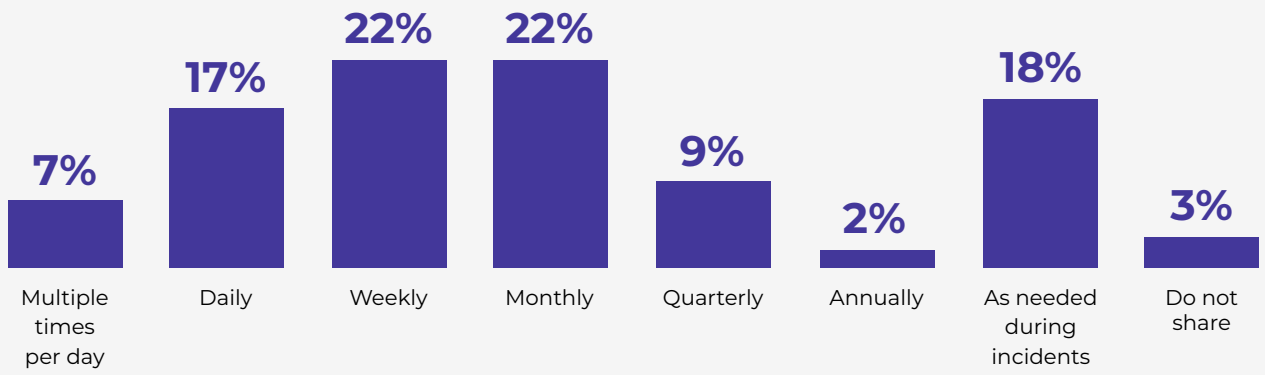
In which types of public-private cybersecurity initiatives does your organization participate?

71% of private sector participants who experienced a cyber incident in the past year reported it to a Federal agency or local field office.

Operationalizing Threat Intelligence Sharing

Participating organizations are establishing regular communication channels and structured protocols for **coordinated incident response**, with the vast majority conducting joint simulations to strengthen their collective defensive capabilities.

How often does your organization share cyberthreat intelligence with external partners?



93% have formal communication protocols for coordinating incident response:

53%
with all key partners

40%
with select partners

80% conduct joint incident response simulations at least annually:

Monthly or more frequently **10%**

Quarterly **29%**

Semi-annually **20%**

Annually **21%**

Balancing Risk and Reward

Participating organizations report **significant benefits** from collective cyber resilience, from enhanced security postures to faster threat detection. While data privacy concerns and organizational differences create obstacles, the vast majority of cyber decision-makers surveyed say the benefits of sharing intelligence outweigh the risks.

Top benefits realized from collective cyber resilience efforts:

#1 Enhanced security posture
50%

#2 Access to better threat intelligence
49%

#3 Faster threat detection
47%

#4 Knowledge and skills development
43%

#5 Improved incident response times
39%

#6 Greater protection of critical infrastructure
35%

85%

say the benefits of sharing cyber threat intelligence outweigh the risks

Top challenges to establishing collective cyber resilience partnerships?

#1 Data privacy concerns
43%

#2 Organizational culture differences
35%

#3 Technical integration difficulties
33%

#3 Legal and regulatory constraints
33%

#5 Information classification conflicts
30%

From AI to Zero Trust

Participating organizations are advancing automation and zero trust principles as foundational elements of their security strategies. While most have made significant progress, many still feel underprepared to combat sophisticated **AI-driven attacks** targeting these evolving defense systems.

Nearly all participating organizations (99%) have automated some portion of their vulnerability management processes

86% are actively implementing a zero trust architecture:

34%
Full implementation across most or all systems

52%
Partial implementation

12%
Initial planning

2%
No plans to implement

How prepared is your organization to combat AI-driven cybersecurity threats?

Well prepared

Somewhat prepared

Not very or not at all prepared

Participating organizations are making notable strides in AI defense: just 4% described their organization as well prepared in 2024[2]

[2] https://meritalk.com/study/art-of-human-and-ai-team-cybersecurity/

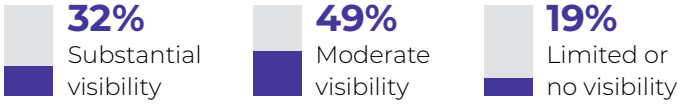
The Dependency Dilemma

Reliance on external technology providers has created a double-edged sword for participating cybersecurity teams.

75% say overreliance on key technology providers is a growing concern for their cybersecurity strategy

Less than half (43%) feel well prepared to maintain minimal viable operations if a critical provider (e.g., cloud or cybersecurity service) becomes unavailable due to an outage or attack

How would you rate your organization's visibility into the security posture of its third-party vendors and suppliers?



32% Substantial visibility

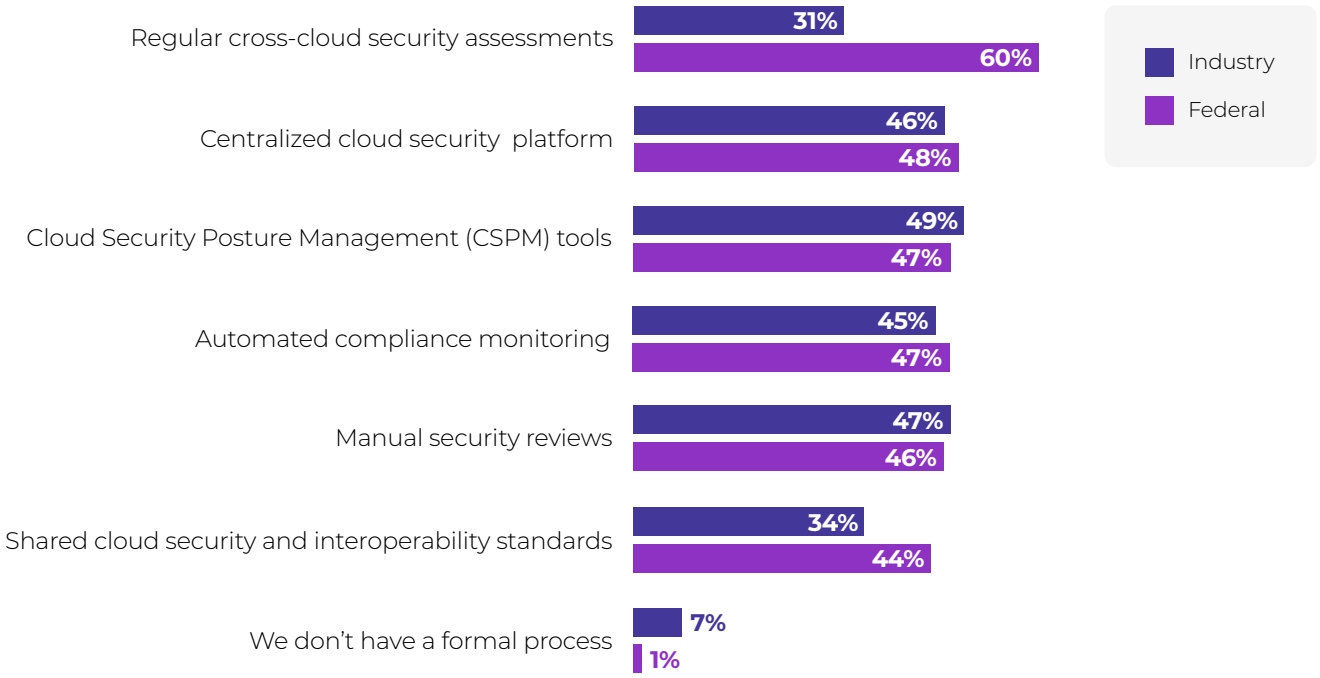
49% Moderate visibility

19% Limited or no visibility

Bridging Gaps in Multi-Cloud Security

Participating organizations are taking a mixed approach to securing multi-cloud environments, and gaps in standardization remain a major concern. Nearly **three in four** (72%) say inconsistent security practices across partners may pose a greater risk to resilience than cyber adversaries.

How does your organization ensure security across multiple cloud environments?

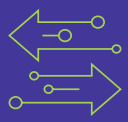


72% say the lack of standardized security practices across partners may pose a greater threat to resilience than cyber adversaries

Lessons from Cyber Resilience Leaders

Participating cybersecurity decision-makers who rate their organization's collective resilience efforts as "excellent" take a more proactive, structured, and integrated approach to cybersecurity.

What sets leaders[3] apart?



Sharing threat intelligence more frequently –

40% of leaders share daily vs. **8%** of other organizations

Reporting cyber incidents at higher rates –

81% of private sector leaders reported incidents to Federal agencies vs. **67%** of others

Having stronger incident response coordination –

77% have formal communication protocols with all key partners vs. **44%** of others

Conducting more frequent joint stimulations –

23% test response plans at least monthly vs. **5%** of others

Leveraging automation at scale –

58% have automated over 60% of their vulnerability management vs. **33%** of others

Leading in zero trust adoption –

64% have fully implemented zero trust across most or all systems, vs. **23%** of others

Maintaining better visibility into third-party risks –

62% have substantial visibility into vendor security vs. **20%** of others

Standardizing cloud practices –

55% have adopted shared cloud security and interoperability standards vs. **33%** of others

[3] Participating cybersecurity decision-makers who rate their organization's collective resilience efforts as "excellent"

Advice from the Front Lines

What is the most important piece of advice you would give another organization working to build collective cyber resilience?

On strategy:

"Understand what your motivations are for collective cyber resilience and then seek out partner organizations that are both like-minded and essential to your joint mission outcomes."

On preparedness:

"Have a dynamic playbook, conduct quarterly tabletop exercises with external and internal parties, and refine any weaknesses identified."

On incident response:

"Reach out to your regional CISA & FBI partners so you know who to call in the first hour(s) of an event."

On intelligence sharing:

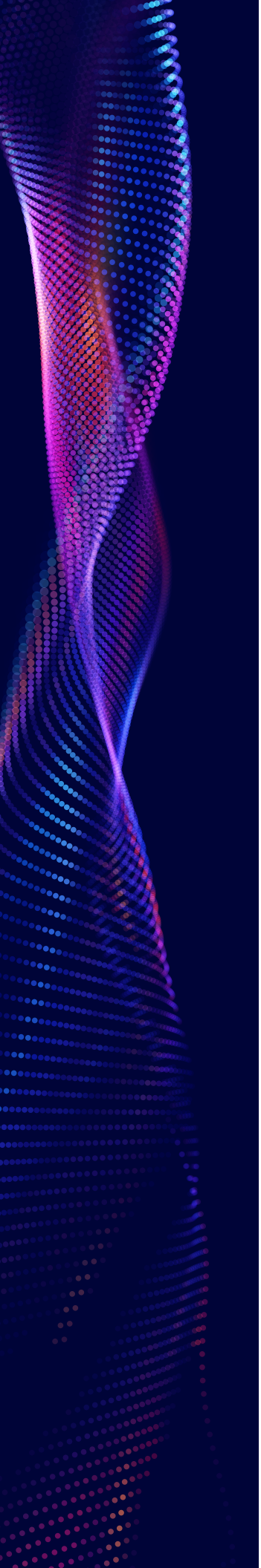
"Use standards for information sharing such as Structured Threat Information eXpression (STIX) and Common Security Advisory Framework (CSAF)."

On leadership buy-in:

"Get alignment and support internally with Legal and C-suite."

On collaboration:

"Cyber resilience is a team effort, and cross-organizational communication is key to strengthening defense strategies."



Maximizing Collective Cyber Resilience

- **Establish or Expand Real-Time Threat Intelligence Sharing.** Move beyond traditional information-sharing models to real-time, automated threat intelligence exchanges between public and private entities. Implement standardized, structured formats (e.g., STIX and CSAF) to improve interoperability and reduce delays in threat response. Create mutual trust frameworks with legal, compliance, and technical guardrails to break down barriers to collaboration.

- **Strengthen Supply Chain Security Through Continuous Visibility.** Develop a unified, cross-sector approach to third-party risk management, mapping supplier dependencies and vulnerabilities across industries. Require continuous security monitoring and threat reporting from vendors and integrate their risk posture into shared cybersecurity dashboards. Align with global security standards to enforce baseline protections for technology providers and critical suppliers.

- **Operationalize Collective Incident Response Through Joint Simulations.** Conduct quarterly, cross-industry cyber exercises to test joint response capabilities and eliminate breakdowns in communication. Develop Federal/local/private response playbooks that define roles, escalation paths, and immediate actions when major incidents occur. Formalize pre-incident agreements that allow organizations to rapidly share cyber personnel, forensic teams, and infrastructure resources during crises.

- **Enhance AI Defense Readiness Through Shared Protocols and Secure Collaboration.** Establish shared AI security standards across government and industry to guide the development, deployment, and monitoring of AI-enabled cyber defense tools. Encourage secure collaboration through federated learning approaches that allow organizations to refine threat detection models without sharing sensitive data. Invest in cross-sector pilot programs to evaluate the effectiveness of AI in identifying, containing, and responding to emerging threats.

- **Incentivize and Enforce Cloud and Zero Trust Standards.** Formalize cloud security baselines that all technology providers must meet, ensuring multi-cloud interoperability. Establish shared zero trust adoption benchmarks that include secure identity, network segmentation, and least privilege enforcement. Consider financial incentives, like tax credits or modernization grants, to accelerate adoption.

- **Foster a Culture of Trust and Collective Responsibility.** Cybersecurity is stronger when built on trust, transparency, and shared responsibility. Invest in cross-sector cybersecurity alliances to align on best practices, improve threat intelligence sharing, and build mutual trust. Create secure, structured forums for cyber leaders to discuss emerging threats and response strategies without legal or reputational concerns. Embed cyber resilience into leadership strategies, workforce training, and cross-organizational engagement.

Methodology

MeriTalk, in collaboration with RSAC, surveyed **100 U.S. Federal government and 100 U.S. private sector cybersecurity decision-makers** in January and February 2025. The Federal sample has a margin of error of ±9.7% at a 95% confidence level and the private sector sample has a margin of error of ±9.8% at a 95% confidence level.

Organization type:

- **50%** Industry or private sector business
- **35%** Federal government – Civilian agency
- **15%** Federal government – DoD or Intelligence agency

Organization size:

- **19%** Fewer than 500 employees
- **29%** 500-999 employees
- **26%** 1,000-4,999 employees
- **26%** 5,000 employees or more

Job title:

- **35%** C-suite (CIO, CTO, CISO, or other executive-level IT/IS decision-maker)
- **40%** Information Technology (IT), Information Security (IS), or Cybersecurity Director/Supervisor
- **14%** IT/IS or Cybersecurity Program Manager/Officer
- **4%** IT/IS or Cybersecurity Analyst/Engineer
- **2%** IT/IS or Cybersecurity Specialist
- **2%** Software/Applications Development Manager
- **1%** Data Center or Network Manager
- **1%** Cloud Specialist or Manager
- **1%** Other IT/IS or Cybersecurity Manager

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


MeriTalk
RSAC
Cybersecurity, Together