carahsoft

SecurityScorecard

Building Toward Cyber Resilience

A GovLoop Guide

Thank you for your interest in exploring this content.

Carahsoft is the **Trusted Government IT Solutions Provider**® supporting a broad portfolio of industry-leading technologies through GSA, NASA SEWP V, ITES-SW2 and a wide range of other contract vehicles.

As the **Master Government Aggregator**®, Carahsoft connects government agencies, industry partners, and technology providers to deliver innovative, mission-focused solutions.

In partnership with SecurityScorecard, we provide technology solutions that drive modernization, strengthen operations, and ensure compliance with evolving government standards.

To learn more about how Carahsoft can support your technology needs, please visit carahsoft.com

Explore More Resources:
carah.io/SSCResources

Join Events & Webinars:
carah.io/SSCEvents

Discover Technology Solutions:
carah.io/SSCSolutions

Learn About Procurement:
carah.io/SecurityScorecardContracts

Connect With Our Team:
SecurityScorecard@carahsoft.com
(844) 214-4790

Building Toward Cyber Resilience

A GovLoop Guide

Introduction

Government agencies are long past imagining they can stop all cyber threats and incursions, but that doesn't mean they need to give up. The secret is resilience — the ability to contain and recover from attacks with minimal downtime. In this guide, the first in a series of three on cybersecurity, we examine how to foster resilience inside an agency and defend against the threats outside it.

Some cyber issues are evergreen: Users remain a weak point that's easy for bad actors to exploit. But don't blame your colleagues. Attacks using new, Artificial Intelligence (AI) powered techniques make it easier to fool anyone. Meanwhile, agentic AI will help automate detection and response faster and more independently than previous tools.

In this guide, you'll learn from Jerred Edgar, Chief Information Security and Operations Officer for the state of Idaho, about how to make a cyber-resilient organization built on competence, trust and collaboration. And you'll hear from Rebecca Cai, Hawaii's Chief Data Officer, on why sound governance is essential to data security and best practices for ramping up your data management.

The cyber landscape remains challenging. But agencies are adapting and developing more effective tactics to keep their data safe. We hope you'll find the information here useful for bolstering your own security strategies.

Contents

The State of Cyber: 6 Trends

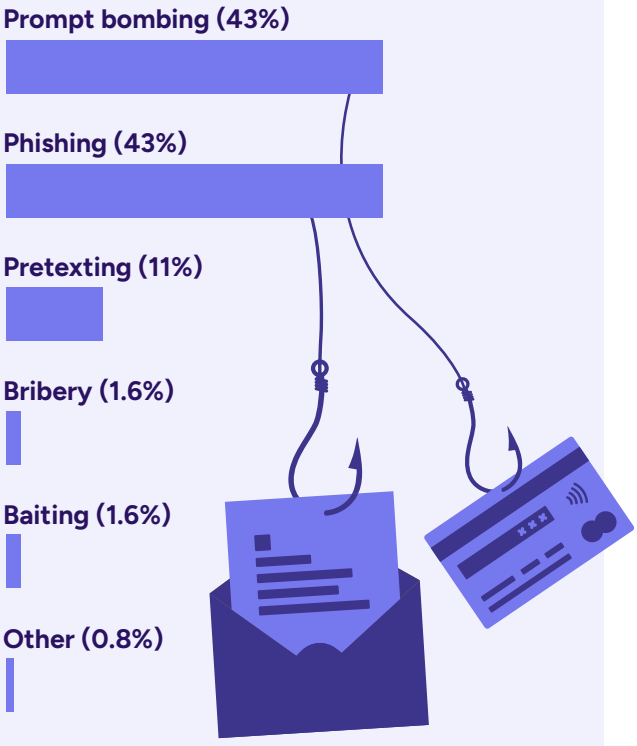
1 The Dual Promise and Threat of AI

With 2026 poised to be the year of agentic AI, you can expect more sophisticated and complex attacks — and better tools to head them off. Bernard Marr, writing in Forbes magazine, called agentic AI "the new frontline of the cybercrime battlefield" as these autonomous machine learning modules can interface with third-party services and spelunk systems for weaknesses.

2 A New Generation of Phishing Attacks

AI is also driving a new generation of phishing attacks. Heard of prompt bombing? That's when an automated intruder sends a user so many requests for multifactor authentication that the user gives in and allows access. How about pretexting, in which the AI develops a plausible story, using deepfakes and natural language to craft messages, voices and conversations that induce a user to give up personal information? According to the latest Verizon Data Breach Investigation Report (DBIR), prompt bombing was implicated in more than 43% of "social engineering" attacks on public service agencies, and pretexting in 11%.

Top Social Actions in Public-Sector Breaches



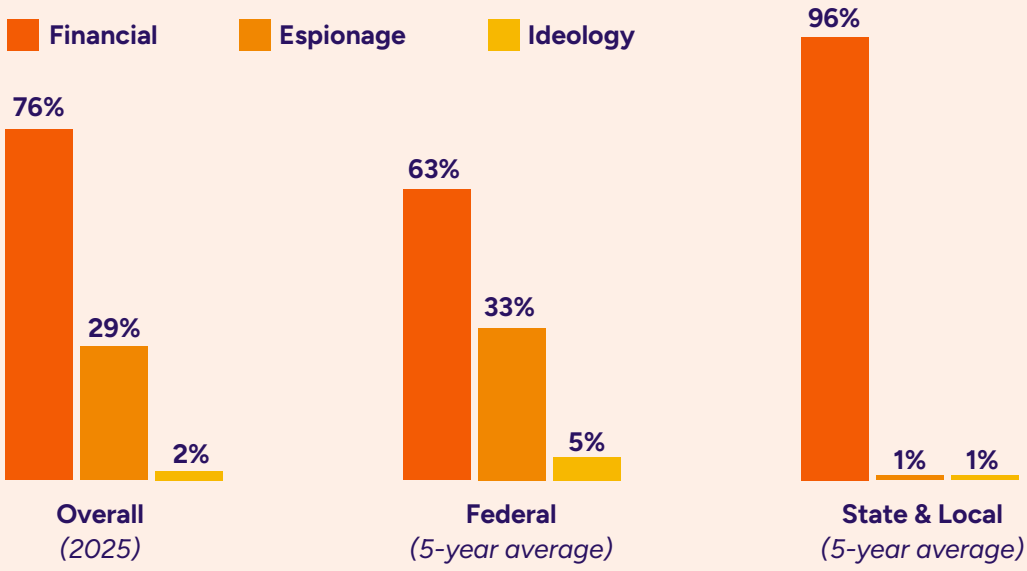
3 3 Most Frequent Attack Patterns Stay the Same

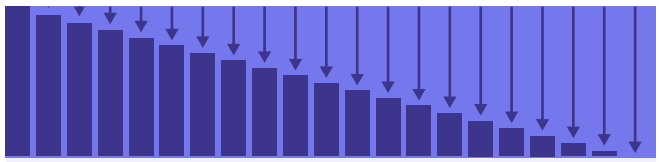
The most frequent attack patterns the DBIR reported were the same as in previous years: system intrusion, miscellaneous error, and basic web application breaches. Together, these accounted for 78% of breaches. But while humans were the culprits in about half of incursions in 2024, last year they were responsible for only about 30%. System intrusion rose to the top spot in 2025, at around 40%. Attacks that hijack basic web applications are beginning to increase after a two-year lull, this time also abetted by — you guessed it — generative AI (GenAI).

4 Most Attackers Seek Financial Gain

The vast majority of attacks on state, local, tribal and territorial (SLTT) governments are for financial reasons, which is not surprising given that 75% of ransomware attacks target them. Some 43% of ransomware victims are local governments in the Southeast and Midwest. Two-thirds of attacks on federal agencies are also looking to make a buck, but a third seek sensitive information. Only about 25% of ransomware victims are federal.

Top Motives for Public-Sector Breaches





5 Insufficient State and Local Funding

Lack of resources continues to keep state and local governments at risk. The Multi-State Information Sharing and Analysis Center's Nationwide Cybersecurity Review, which represents more than 4,000 SLTT respondents, found that 73% reported lack of sufficient state and local funding as a top security concern. "Inadequate availability of cybersecurity professionals" was also a concern — 80% of respondents reported fewer than five security personnel.

6 Internal Errors Due to Poor Data Governance

Although miscellaneous errors aren't in the top spot this year, they remain a significant cause of breaches. The most frequent slip-ups involved misdelivery — a hazard for agencies that do mass mailings — but data misconfiguration and classification errors accounted for nearly as many exposures.

(See more about the role of data governance in cybersecurity in our interview with Rebecca Cai, Chief Data Officer for the state of Hawaii, on page 13.)

Securing Your Supply Chains From the Threats You Do, and Don't, See

Agencies have hardened their cyber defenses in many ways, but there is one vulnerability they often under-appreciate: the complex ecosystem of vendors, subcontractors, and other entities that comprise government supply chains. A single agency might rely on hundreds or even thousands of third parties, creating hidden risks that IT teams may not see before an attack. Yet adversaries, including nation states, know how to exploit supply-chain weaknesses — endangering mission-critical functions, public safety and other services, and core infrastructure.

To counter these threats, agencies need visibility into their supply-chain risks so that IT teams can be proactive, not reactive. Because vendors pose different security challenges, organizations must identify and prioritize their most vulnerable suppliers. And a mature approach to supply-chain security also means weaving security into the entire vendor lifecycle — from procurement to oversight and incident response — and collaborating with outside experts.

In this video interview, Michael Centrella, Head of Public Policy at SecurityScorecard, discusses how agencies can safeguard their supply chains from increasingly skilled and motivated adversaries. Topics include:

- → Why government supply chains are especially vulnerable
- → How to adopt a mature approach to supply-chain security
- → Resources that can help agencies protect their vendor networks

"We are really at a pivotal moment. Over the last several years, government agencies have made significant investments in strengthening their internal cybersecurity posture. But what we're seeing is that adversaries have shifted, and their focus has turned toward suppliers."

— Michael Centrella, SecurityScorecard

About SecurityScorecard

SecurityScorecard modernizes Third Party Risk Management (TPRM) using AI and threat intelligence to continuously manage, detect, and respond to global supply chain risk.

Learn more about SecurityScorecard.

SecurityScorecard

carahsoft.

Three Building Blocks for Improving Cyber Resilience

Jerred Edgar's 24 years in the U.S. Army shape his work as Idaho's Chief Information Security Officer in ways both intangible and practical.

Early in his Army career, he focused on combat arms and military intelligence, then shifted to IT and cybersecurity. Over the years, Edgar gained experience in problem solving at every level, from individual teams to U.S. Central Command. "It was essentially one problem after another, and it instilled in me this unique perspective that I bring to everything I do," Edgar said.

He also picked up some good tools for building cyber resilience. The art of resilience, he said, comes down to core principles around planning, execution and communications. In particular, he uses the Army's seven Mission Command Principles as a framework (see below). Edgar sees the first three as foundational pieces for cyber efforts:

#1 Competence

#2 Trust

#3 Collaboration

These principles can help cyber teams simplify their approach to cybersecurity, which reflects another lesson Edgar learned in the Army: **Simplicity survives, while complexity dies.**

The Seven Principles of Mission Command

Source: Army University Press

1

BUILDING BLOCK #1
Executing With Competence

Definition: Edgar defines competency as the ability to execute a mission with discipline and initiative: "Are we exceptionally good at what our role requires us to do?"

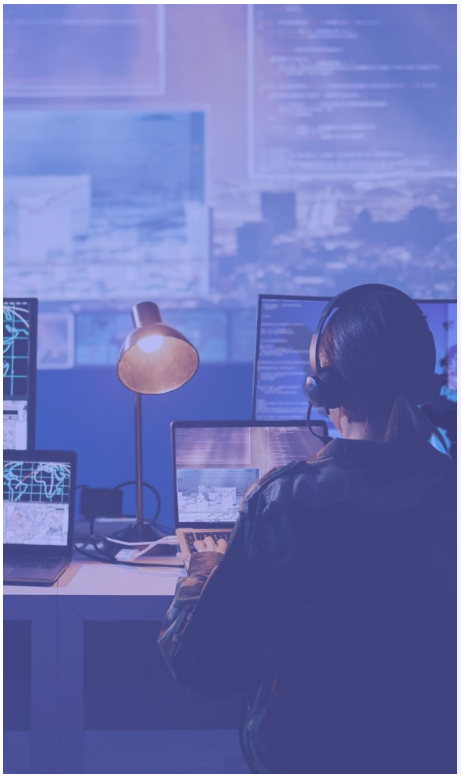
Cyber tools and tactics don't amount to much if employees do not have the experience and skills to wield them effectively, Edgar said. "Socrates said that a disorderly mob is no more an army than a pile of rubble is a building," he said. In the same way, "you can buy stuff, but it's just a pile of stuff. It's up to you to turn it into that house you're going to live in."

Key Enablers

Governance. Standards, definitions, guidance and related documents provide employees with "compass north," Edgar said, ensuring that everyone understands the organization's goals and their role in achieving them.

Training. Once the goals are clear, cyber leaders must help employees develop the skills they need to carry out their roles and align with the standards and guidance defined as part of governance.

Ownership. To be effective, both governance and training require meaningful support from the organization, said Edgar. "Are we investing our time, our leadership and our [resources] to support that?"



Case Study

Idaho Readiness Training

After Hurricane Andrew hit Florida in 1992, the Defense Department (now the War Department) created the Innovative Readiness Training program through which military personnel help local communities rebuild after disasters. In the process, those military members receive on-the-job training in skills that support military readiness, such as operating heavy equipment.

About 26 years later, the department expanded IRT to include cybersecurity work. Edgar, still in the military at the time, helped build a strategic partnership with the state of Idaho to put this idea into practice, eventually becoming Director of Cyber IRT for the Idaho Army National Guard. Now, as Idaho's CISO, he has built on the IRT to create the Idaho Readiness Training initiative, which advances cyber competencies for state and local governments, critical infrastructure owners, and other key players statewide. The initiative is part of a larger program called Operation Cyber Idaho.

BUILDING BLOCK #2

Fostering Trust Among Stakeholders

Definition: Trust is an environment where people and institutions can rely on each other, said Edgar. That includes competency (each stakeholder is good at what they do), veracity (each stands by their word) and transparency (each is upfront about their goals and objectives and acts accordingly).

Trust is essential in cybersecurity because it involves various stakeholders, both within an agency and across various partner organizations. "We need to build an equitable system that allows us to stay in our lanes but collectively move in the direction we need to move," Edgar said. "If we don't establish that trust, we might as well just be fighting these fights individually."

Key Enablers

Shared problem solving. The different stakeholders should determine how they can tackle problems together most effectively, based on their individual roles and strengths, while being careful not to overstep their areas of responsibility, Edgar said.

Ownership. In many cases, the key issue is follow-through, he said. As the stakeholders work together to solve problems, they need to take their commitments seriously and, if they make a mistake or fail to follow through, they need to own up to it.

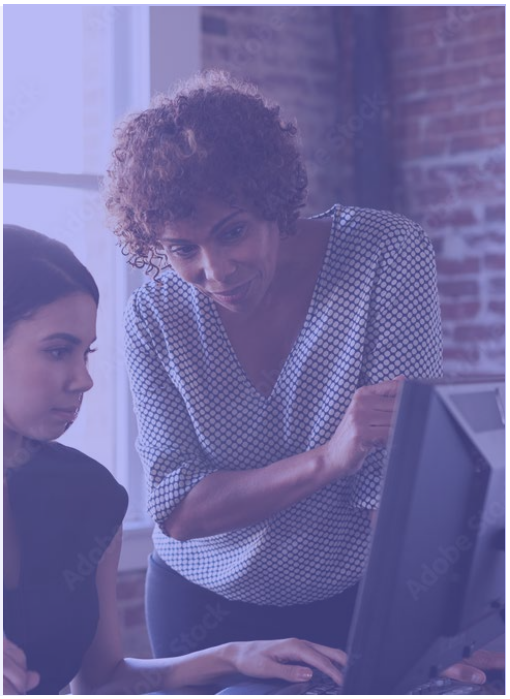
Adaptability. That said, sometimes things go amiss because of outside factors. In those cases, the stakeholders need to work together to find a new path forward. "We don't always have everything go our way, and so we're going to collectively adjust to it," Edgar said.

Case Study

Apprenticeship Program

One way state governments can earn local communities' trust is by helping them strengthen their cyber competency. That is the goal of the Operation Cyber Idaho apprenticeship program, which provides workers with 2,000 hours of developmental assignment opportunities. "We're investing in people to show that we're here to help, not just enforce mandates," Edgar said.

In many areas of the state, students or recent graduates pursuing cyber careers might have trouble finding opportunities to build their skills and strengthen their resumes. The program matches applicants with organizations that need cyber support, such as a rural telehealth provider or a school district. The program, formally launched in 2024, has placed 33 people so far, supporting 11 counties, two cities and five school districts.



BUILDING BLOCK #3

Collaborating on Collective Defense

Definition: Collaboration is essential, given how interconnected systems are — and how ready malicious actors are to exploit that. State and local governments, school districts, critical infrastructure owners, and other stakeholders need to move toward a collective defense.

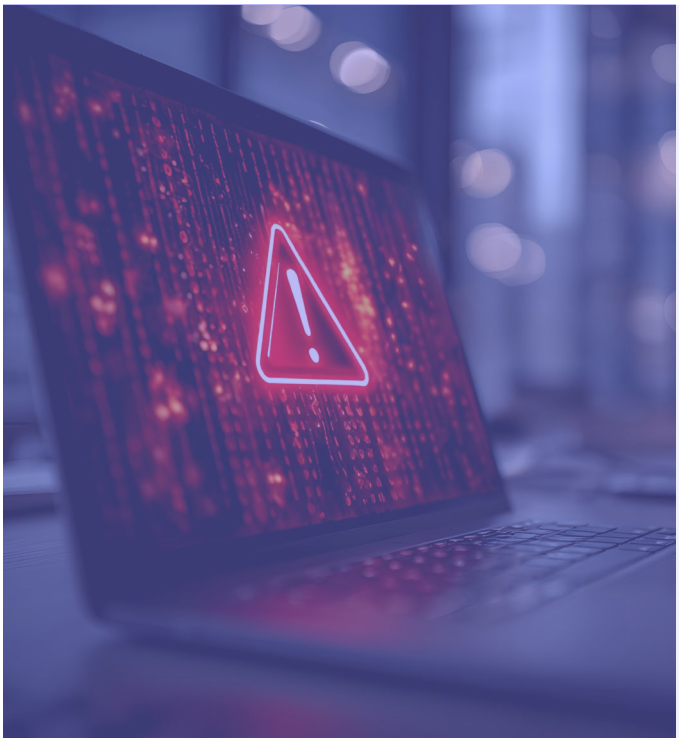
"As we've grown that competency, grown that trust, we are in a position where we can work together to defend ourselves," said Edgar. It's the same approach that proved decisive in the 20th-century world wars, he said.

Key Enablers

Shared vision. A collective defense begins with reaching a mutual understanding of what the group is trying to achieve. Everyone is rowing their own boat, Edgar said, but they need to move in the same direction.

Clearly defined roles. Collaboration across organizational boundaries often runs into legal obstacles. For example, if a state-level cyber team sees suspicious activity on a local network, does it have the authority to stop it? State-level legislation or policy might be needed to address these legal ambiguities, Edgar said.

Managed risk. No collaborative effort can fully eliminate risk. The key is to maximize what's working, then work on identifying and reducing the gaps. "It's a long fight," he said.



Case Study

Operation Grinch

In building a collective defense, you want to create layers that can slow an attacker. This approach paid off for Idaho when someone launched an attack against state systems on Christmas Eve 2025. Edgar's team dubbed it Operation Grinch, because it seemed likely to ruin everyone's holiday. However, the state's layered defense slowed the attack, giving the team enough time to thwart it, Edgar said.

"We're building in those layers of resilience, so that we can give our teams longer to detect [a threat]," he said. "That really has become key: Do the things that are going to give you the layers so that you can stay in the fight longer."

Security Starts With Data Governance

A conversation with Rebecca Cai, Chief Data Officer, State of Hawaii

When we envision cybersecurity, it's often as a barrier that keeps hostile actors out. But cybersecurity is also a matter of what's within the walls of your network: your data and how you protect it.

"Data governance is a proactive way of managing data security," said Rebecca Cai, Chief Data Officer for the state of Hawaii. Cai collaborates with her counterpart Vincent Hoang, State Chief Information Security Officer, on data privacy and incident management — the threats from outside. But it's her office that safeguards the information where it lives. "In practice, security controls are only as effective as the governance framework," Cai said.

Governance practices such as data minimization, access controls and sensitivity classifications can protect data even when there's a breach. "If my Social Security number doesn't exist anywhere, it doesn't matter how many systems [attackers] hack. They can never see it," Cai said. "If it's always classified [as confidential] and access-protected, even if they hack in … it should be less risk."

Data Governance That Protects

Hawaii has adopted a data strategy that highlights transparency, regulatory compliance and privacy, while promoting data-driven decision-making.

To help implement the strategy, the data office received funding for a data governance platform, which Cai is now implementing. She outlined a process that begins with "understanding the data we have today, how it is classified and how it may be used."

The first step, she said, is **cataloging:** knowing what data an agency possesses. Simply identifying what you have is the foundation for securing it. It's also the starting point for any analytics project. "When we try to solve a business problem, first, I need to figure out what data I can use to solve [it]," Cai said. "That's [also] the cataloging feature of governance."

The next step is to **classify** the data. Does it include personally identifiable information? Is it confidential or sensitive? If so, what extra measures are needed to protect it? "Should we mask it, should we tokenize it or should we delete that data?" Cai asked. Sometimes the best way to protect information is not to collect it at all.

Governance and security also depend on assigning **ownership** of the data — establishing who is responsible for it and accountable if there's a leak. But, Cai notes, that's valid only when **access controls** are in place.

"If I'm responsible for sensitive data, I need to be sure that I have full access control. You can't make me accountable if everyone can access my data without me knowing it," she said. Limiting who can access what data, for what purpose and for how long protects information from unwanted exposure and makes it easier to audit data and ensure transparency.

Controlling access reduces the risk of human error. "As an IT person, I shouldn't have access to anyone's Social Security number," Cai explained. "If I don't have access, I don't need to worry about leaking it."

To encourage public trust, Cai's office publishes its privacy guidelines and data governance framework, and the state's data task force holds a quarterly open public meeting to discuss policy, governance guidelines, privacy and any other concerns. If there's a breach, it's important not just to notify the public, but to share what went wrong and how you're responding, Cai said. "Trust always starts with transparency. After an incident, tell me what you would change about your process, what extra steps you're taking to ensure similar things won't happen [in the future]," she added.

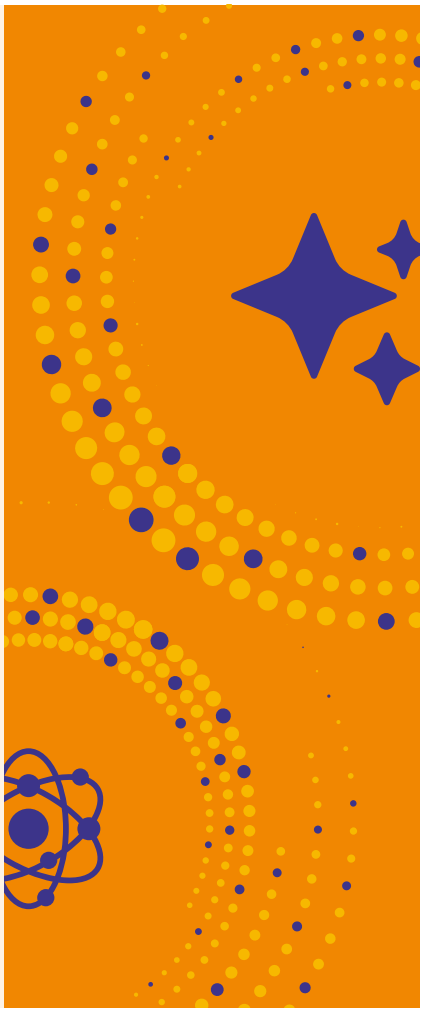
Facing Today's Threats — and Tomorrow's

You can't talk about cybersecurity these days without mentioning AI. It's is a great tool for cataloging and classifying data, but it's also helping threat actors devise new forms of attack. "On the threat side, with AI, it's easier to attack us. Bad guys have access to the same technology as good guys do," Cai observed.

One example of AI's double-edged sword is when a search reveals connections within agency data stores that no one recognized. Although this hasn't happened under Cai's watch, she's heard of incidents elsewhere in which people suddenly had access to someone else's data.

Outsiders can exploit those connections, but Cai sees an opportunity to improve data governance and head them off. "I think that's a good thing because proactively identifying those [connections] is better than [data] leaking out and someone external finding it," she said. "And once AI finds [these connections], people understand more about the criticality of having data governance."

On the horizon, quantum computing poses a threat — specifically, the risk that one day it will render current encryption algorithms useless. "They say bad actors can just save our [encrypted] data until quantum computing is available, and then they can just unmask all the data," Cai said. "That's scary, so I think everyone is trying to become quantum-ready."



Getting Started

Cai warned that it's impractical — if not impossible — to impose comprehensive data management on everything from the outset. "You can never catalog all the data because new data is generated every day," she said. To catch up, start with some important use cases and roll it out that way.

"Go little by little, use case by use case, and before you know it, you're almost there. But you can never, ever be perfect on data governance, never be perfect on quality. You're never done. It's a journey," she said.

And it's a journey Cai said all agencies must take.

"In the AI age, data governance and security become more and more important. There are always bad guys there, but I'm … optimistic," she said. "[That] shouldn't stop us from doing things. We just have to move faster [than they do]. And even a small step forward on data governance, on security, is better than nothing, right? Don't wait for the perfect solution, don't wait for the perfect moment. Start now."

Additional Resources

Check out GovLoop's previous guides for more about the state of cybersecurity.

The AI Cyber Arms Race Is On (October 2025)

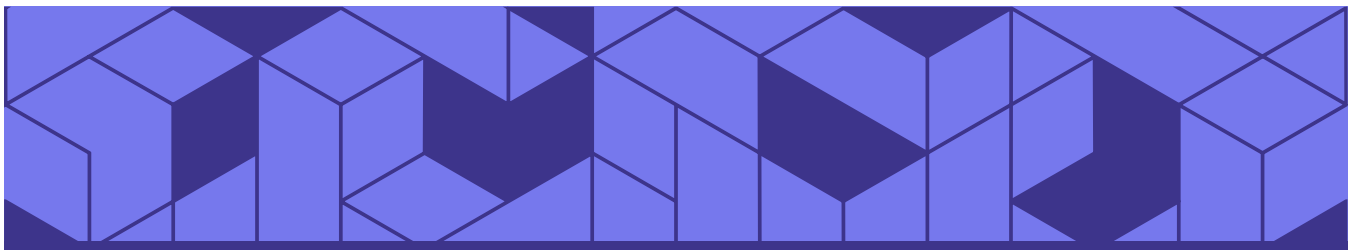
Government agencies know what they are up against. Malicious actors are leveraging AI to launch a higher volume of attacks and make attacks more targeted and harder to detect. This guide explores recent developments that will shape security strategies in 2026 and beyond.

Focus on Cyber Force Multipliers (June 2025)

Cybersecurity teams, like everyone in government, deal with tight budgets and staffing limits. At the same time, the IT environment is growing more complex and the cyber threats more sophisticated. This guide explores technologies and tactics that can serve as force multipliers for cyber teams, helping them do more with less.

Agencies Accelerate Cyber Advances (January 2025)

Basic cyber hygiene is no longer enough, especially in an environment where hackers have access to AI-powered tools and the rapid expansion of digital services leaves agencies more vulnerable. This guide looks at how agencies at all levels of government are reinforcing their existing cyber defenses and partnering with the private sector to develop innovative technology and practices.



About GovLoop

GovLoop's mission is to inspire public-sector professionals by serving as the knowledge network for government. GovLoop connects more than 300,000 members, fostering cross-government collaboration, solving common problems and advancing government careers. GovLoop is headquartered in Washington, D.C., with a team of dedicated professionals who share a commitment to the public sector.

For more information about this report, please reach out to info@govloop.com.

govloop.com | @govloop

Thank You

Thank you to Carahsoft and SecurityScorecard for their support of this valuable resource for public-sector professionals.

Authors

Lauren Walker, Senior Staff Writer

John Monroe, Director of Content

Candace Thorson, Managing Editor

Designer

Kaitlyn Baker, Senior Creative Manager