GOVERNMENT GEARS UP FOR A BETTER CYBER FUTURE

govloop

Introduction

For government cybersecurity teams, the emergence of readily available, easy-to-use AI tools is both business as usual and a disruptor. Yes, AI has the potential to make many attacks more effective and difficult to detect. But the overarching goals remain the same: keeping on top of security basics, while staying agile enough to respond to emerging threats, whatever their source.

We begin this final installment of our three-part Cyber Guide series with a look at the state of the threat landscape as 2024 draws to a close. The big themes are familiar, including the persistent threat of ransomware, ongoing funding challenges and heightened concerns about data privacy. At the same time, the Department of Homeland Security (DHS) is working on several initiatives to help agencies make progress on issues such as incident response and information sharing.

This guide also spotlights the DHS Unified Cybersecurity Maturity Model (UCMM), a framework that helps the department ensure that proposed cyber spending aligns with key priorities and results in quantifiable improvements. The department plans to share the framework with other agencies.

Finally, we take a close look at how AI is changing cybersecurity. And it's not all bad news. Although AI can make malicious actors more dangerous, it also can strengthen cyber defenses in areas such as threat detection, incident response and remediation. For perennially short-staffed security teams, AI can be a boon.

We look forward to seeing how all these issues and initiatives play out in 2025, when we undertake our next Cyber Guide series.

CONTENTS

3 Cybersecurity 2024: A Work in Progress

6 How AI Could Revolutionize Cyber Operations

7 DHS Brings New Discipline to Cyber Planning

9 How to Make Zero Trust More Manageable

10 AI's Impact on Cybersecurity: The Good, the Bad and the Automation

13 How to Build Mission-Capable Security Talent

15 Conclusion

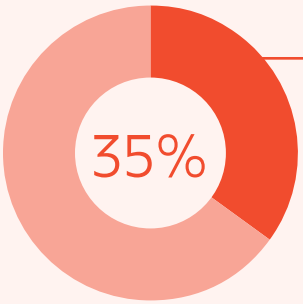
16 About and Acknowledgments

Cybersecurity 2024: A Work in Progress

For more than 25 years, the U.S. Government Accountability Office (GAO) has listed information security as a high-risk area for the federal government. Cybersecurity, of course, is a moving target, with new advances in cyber defenses being met with new threats, making it very difficult for agencies to keep pace.

Since 2010, GAO has made more than 1,600 recommendations as part of its audits of agencies, and more than a third have not been implemented. Here is the breakdown, according to GAO's June 2024 High-Risk Series report:

GAO has made **1,610** recommendations in public reports regarding the four cybersecurity challenge areas

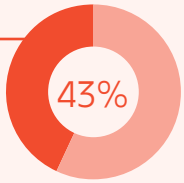


567 of those 1,610 recommendations have NOT been implemented as of May 2024

CHALLENGE 1:

Establishing a comprehensive cybersecurity strategy and performing effective oversight

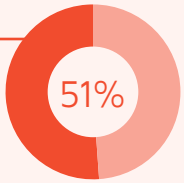
170 of 396 recommendations have NOT been implemented



CHALLENGE 3:

Protecting the cybersecurity of critical infrastructure

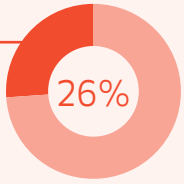
64 of 126 recommendations have NOT been implemented



CHALLENGE 2:

Securing federal systems and information

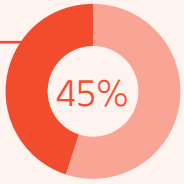
221 of 839 recommendations have NOT been implemented

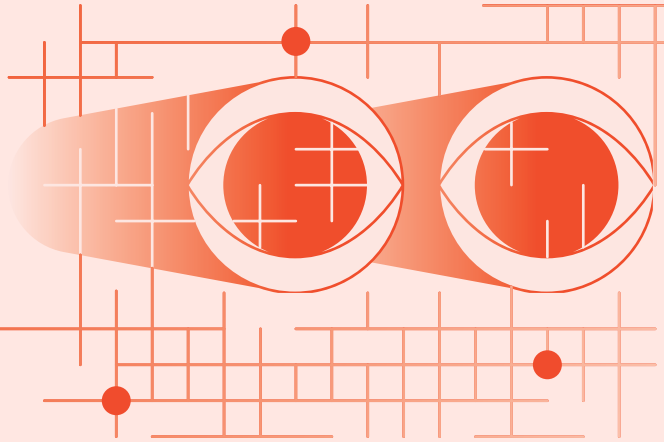


CHALLENGE 4:

Protecting privacy and sensitive data

112 of 249 recommendations have NOT been implemented





FIVE TRENDS TO KEEP WATCHING

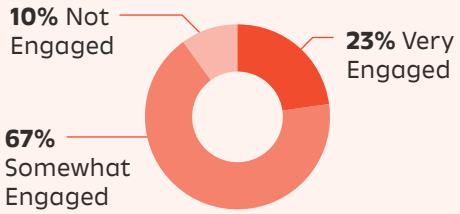
Here are the five big trends in cybersecurity that emerged in the past year, according to the 2024 Report on the Cybersecurity Posture of the United States:

1. **Evolving risks to critical infrastructure**, with nation-state adversaries increasingly targeting systems even if they have "no inherent espionage value."
2. **Ransomware**, which remains a persistent threat as ransomware groups continually find ways to evade defensive measures.
3. **Supply chain exploitation**, with malicious actors taking advantage of the complex and interconnected supply chains for software and other IT and services "to compromise victims at scale."
4. **Commercial spyware**, with private vendors supplying nation-state actors with an increasingly sophisticated and invasive cyber surveillance tools.
5. **AI**, which presents both "opportunities and challenges for cyber risk management at scale."

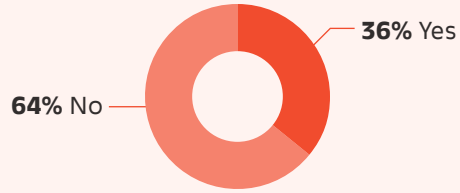
LOCAL AGENCIES SEEK CYBER SUPPORT

For cities and counties, the challenge often is getting legislators and other elected officials to understand the cyber risk and the need for more resources. Here are some findings from the Public Technology Institute's latest survey on cybersecurity in local government:

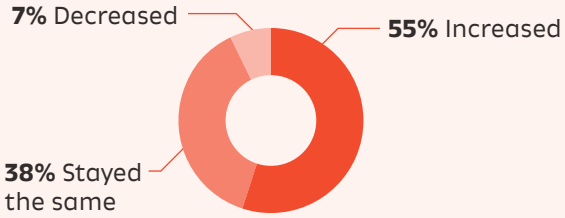
How engaged and familiar are your elected officials with your organizationwide cybersecurity efforts?



Is your cybersecurity budget adequate to support cybersecurity initiatives?



Regarding your current cybersecurity budget: How has your budget changed in comparison to last year's or your previous cyber budget?



STATE & LOCAL CYBER HYGIENE

Fiscal 2025 is the third and possibly final year of the State and Local Cybersecurity Grant Program, which has provided close to $1 billion in funding. In applying for grants, agencies are encouraged to address eight cybersecurity best practices:

- Implement multifactor authentication.
- Implement enhanced logging.
- Encrypt data at rest and in transit.
- Stop using unsupported/ end-of-life software and hardware that are accessible from the internet.
- Prohibit the use of known/fixed/default passwords and credentials.
- Ensure the ability to reconstitute systems (backups).
- Actively engage in bidirectional sharing between the Cybersecurity and Information Security Agency (CISA) and state, local, and territorial entities in cyber-relevant time frames to decrease cyber risk.
- Migrate to the .gov internet domain.

FEDS STEP UP CYBER PLANNING

DHS and other organizations are working hard to help government agencies take a more proactive, agile approach to improving their cyber defenses and responding to cyber events. Here are four initiatives that launched in 2024.

Think Tank Forms Center to Advise Feds

In July 2024, the Institute for Critical Infrastructure Technology, a nonpartisan think tank, launched the Center for Federal Civilian Executive Branch Resilience. The goal is to bring together experts in security, policy and technology to educate government leaders and policymakers on emerging technologies and strategies.

CISA Buttons Up Cyber Incident Reporting Process

CISA is developing a new, more automated process through which the agency and its partners can share information about cyber incidents. As part of the initiative, CISA will work on an incident reporting portal, a unified ticketing system for tracking response efforts, and other tools, according to a July 2024 GAO report.

DHS Delivers Guidance on AI and Critical Infrastructure

DHS is leading an effort to get critical infrastructure organizations up to speed on the opportunities and risks that AI presents. In June 2024, the agency released AI-related Safety and Security Guidelines for Critical Infrastructure Owners and Operators. The guidelines reflect lessons learned from an AI risk assessment survey conducted by the Sector Risk Management Agencies, representing the 16 critical infrastructure sectors. The guidance looks at cross-sector AI use cases in addition to the most common risks.

CISA Tests Response Plan for AI-based Cyber Incidents

Also in June 2024, CISA brought to together cyber leaders from government and industry to test initial ideas for coordinating responses to AI-related cyber incidents. Such tabletop exercises are a staple of cyber incident planning, but traditional incident response processes might not work for AI-based attacks, which can be stealthier and more lethal. CISA will incorporate the lessons learned from the exercise in a forthcoming AI Security Incident Collaboration Playbook.

How AI Could Revolutionize Cyber Operations

An interview with Robert Imhof, Consulting Systems Architect, Fortinet Federal



Adoption of AI has been widespread in recent years, touching every area of life because of its potential to improve operations. For government agencies' cybersecurity operations, AI holds especially great promise.

For instance, AI can automate and enhance cybersecurity practices by recognizing and remediating threats faster than a human could. These capabilities are more important than ever because as attackers weaponize AI, agencies need to respond by implementing defensive AI in their networks.

"It will be an essential technology and tool that really every security professional is going to eventually need to master," said Robert Imhof, of Fortinet Federal, which delivers modern, secure infrastructure to government agencies.

WHERE AI CAN HELP

Imhof highlighted several uses for AI in cybersecurity operations. The most profound is anomaly detection, or finding unusual patterns in behavior in network traffic, user activity or application usage that may indicate a compromise.

"We have these in a lot of tools right now, but this is really going to become more sophisticated and more advanced," he said.

AI can also assess risk by quickly analyzing large amounts of data. Eventually, it could even suggest ways to better design security systems.

"The speed of AI to accomplish these tasks, while ingesting that significant amount of data, is going to give it that distinct advantage over traditional tools," Imhof said.

WHAT TO WATCH OUT FOR

Because use of AI is relatively new, agencies must take care to avoid missteps with it.

The biggest is replacing support staff with AI tools, said Imhof. "Sometimes you have issues like hallucinations" with AI, where it gives false positives, he said. "You still need those security professionals to be able to parse that data and really put it into context."

They also must understand how AI conducts its analysis. "Does it remain local to the agency, or is it sending that data back to somewhere else?" Imhof said. "If it's being sent somewhere else, how is that [controlled unclassified information] data being protected?"

AI BEST PRACTICES

Whenever a new technology is involved, there's a learning curve — and there's always new technology, Imhof said.

"It's going to be worth investing the time and effort to learn this technology," he explained. "Security professionals who can master utilizing AI in addition to their other technical skills are going to be highly sought after by employers."

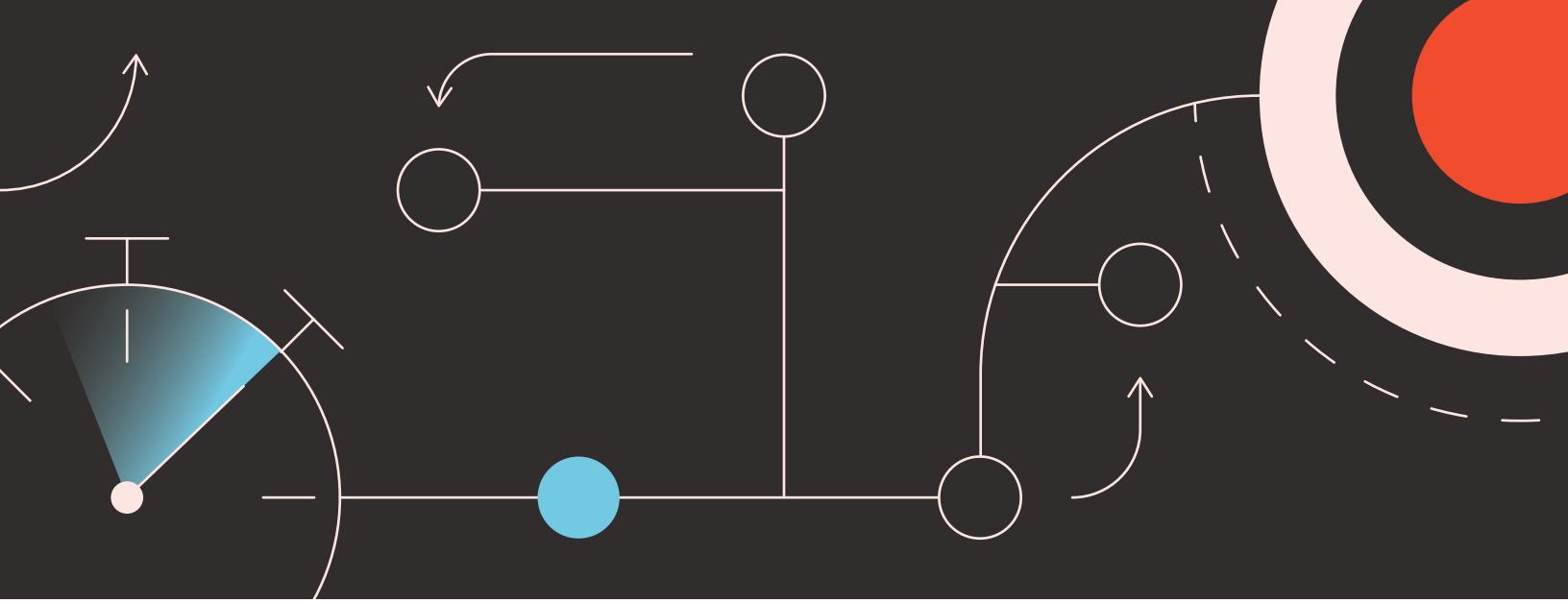
That will also help separate fact from hype, which is rampant because of the excitement around the technology. That's where cybersecurity operations officials come in again, Imhof said.

"They're going to have to learn how the AI itself works to assess how it fits in [a given] environment," he added.

To do that, Imhof recommends using a test environment to determine how AI-powered defenses work within the network one at a time.

Ultimately, he said, "AI is a tool that can be used to enhance the security of a network, so it should be used in that correct context."

FORTINET FEDERAL®



DHS Brings New Discipline to Cyber Planning

An interview with Hemant Baidwan, Chief Information Security Officer (CISO), DHS



In 2021, DHS, like many agencies, was putting together a funding request to boost its cybersecurity work after the SolarWinds cyberattack. Hemant Baidwan was leading the effort and reviewing requests from various DHS components when he realized something was missing: the ability to connect funding to outcome.

Now the department's Chief Information Security Officer, Baidwan puts it this way: "OK, we got $5. What have we done with that? What weakness is the $5 remediating or what exactly is it going to? You need to be able to quantitatively show that."

With that in mind, DHS developed the Unified Cybersecurity Maturity Model (UCMM), a framework that "allows us to tie the investment dollars to the cybersecurity of a [high-priority] program and its component systems," Baidwan said.

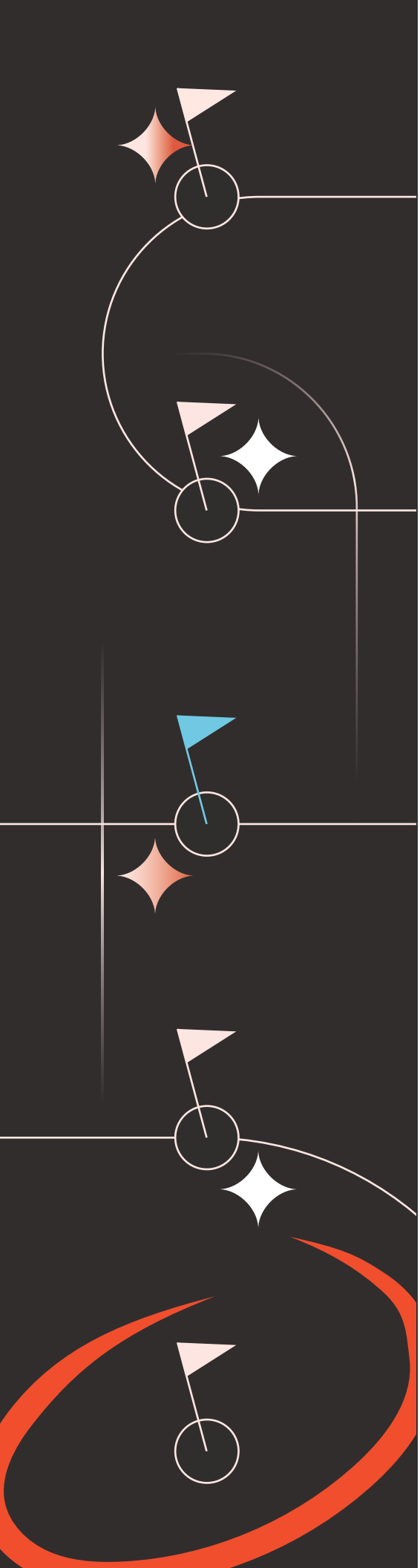
In simple terms, the model guides the department through the process of identifying critical cybersecurity challenges, determining the resources needed to address them and showing how that investment qualitatively improves the program's overall cyber maturity.

Baidwan said this automated risk prioritization allows system teams to optimize the time they spend remediating system deficiencies to provide the best achievable system maturity with the least time and staff expenditures.

UCMM has proven invaluable when talking about cyber investments not just with IT experts, but with chief financial officers, budget examiners and lawmakers, he added. The agency also uses the model to track and report on the outcomes of those investments.

DHS highlighted UCMM in its "Integrated Strategy for High-Risk Management," a biannual update to the Government Accountability Office.

"The UCMM framework has been a key in aligning recovery actions from the SolarWinds Incident and guiding implementation of critical cybersecurity capabilities and above guidance requests," the report states. "Going forward, the framework provides a means to guide cybersecurity maturity level measurement for the Department."



EARLY WINS

Today, UCMM is part of modernization planning. DHS recently shifted from large-scale modernization efforts to what DHS CIO Eric Hysen refers to as "modernize in place," which focuses on fixing specific weaknesses or delivering specific new capabilities.

As part of this move, DHS leaders use UCMM to guide evaluations of modernization risk, Hysen said while testifying before the Senate Committee on Homeland Security and Governmental Affairs in May 2023. "For modernization programs, assessments under UCMM are critical to determine future investments," he explained.

Indeed, the department plans to give the model an increasingly larger role in IT and budget planning, according to DHS's Information Technology Strategic Plan (FY 2024-2028). "To support risk-based decision-making, DHS is aligning future IT budget requests with the DHS UCMM framework," the plan states. "We will issue annual IT resource planning guidance and approve funding for projects that are in line with our modernization objectives."

The framework also has helped the department do a better job of resolving cybersecurity concerns that its Office of Inspector General (OIG) has raised. As a standard practice across government, agencies create a Plan of Action and Milestones (POA&M) to identify and track tasks needed to address an audit concern.

As part of its annual cybersecurity audit, the DHS OIG had identified POA&M tracking as a key deficiency several times. But in fiscal 2022, the department's Management Directorate used UCMM to prioritize overdue POA&Ms and successfully closed about 64% of them, according to the OIG. DHS then began implementing the same approach at other components.

FOCUS ON OUTCOMES

UCMM's value extends well beyond risk assessments and planning. When DHS makes an investment, Baidwan and other DHS leaders can use the framework to report on its outcomes, whether they are talking to the Office of Management and Budget or Congress.

It comes back to that $5, Baidwan said. "I want to make sure that I'm able to internally track that. 'OK, we got $5. What have we done with that?'"

DHS plans to share UCMM, which is patent pending, with other agencies, so they can use it, too, he said.

How to Make Zero Trust More Manageable

An interview with John Kindervag, Chief Evangelist, Illumio



Zero-trust architecture, while widely recognized as essential to modern security, has earned a reputation as a daunting undertaking. John Kindervag, who is credited with defining the zero-trust approach in 2010 when he was a principal analyst at Forrester Research, would like to bust that myth.

Granted, zero trust is not a quick fix. "People want to buy a product, and they want it to be easy, and they want to do just one thing — that's human nature," said Kindervag, now with Illumio, which provides solutions for network segmentation. "But cybersecurity is a phenomenally complex system, and it's a system of many parts that all have to interact to be successful."

A 5-STEP PROCESS

If agencies take a methodical approach to zero trust, they are likely to find that it is more manageable and less expensive than they think, he said. With that in mind, Kindervag has developed a five-step process for implementing zero trust:

- Determine the protect surface, which includes data, applications, assets and services (DAAS).
- Map the transaction flows, looking at how the different elements interact and how data flows through the network.
- Once you understand how the network works, create the zero-trust architecture, implementing the controls to safeguard your protect surface.
- Define the policies for enforcing zero trust.
- Monitor and maintain it.

Note that the first step is to identify what you need to secure — that is, your protect surfaces. Rather than building a comprehensive zero-trust architecture, agencies can begin small by focusing on specific DAAS elements, Kindervag said.

"You take a single DAAS element, you put it into a single protect surface, and you build out your zero-trust environment one protect surface at a time," he said. "In this way, zero trust becomes incremental." Many organizations make the mistake of trying to deploy zero trust across their entire organization, he added, "and that will never work."

THE FOUNDATION: NETWORK SEGMENTATION

Kindervag says the foundation of this approach is network segmentation. The idea is to implement security controls within the network, breaking up the protect surface into "bite-sized chunks" that make it easier to control access to those DAAS elements.

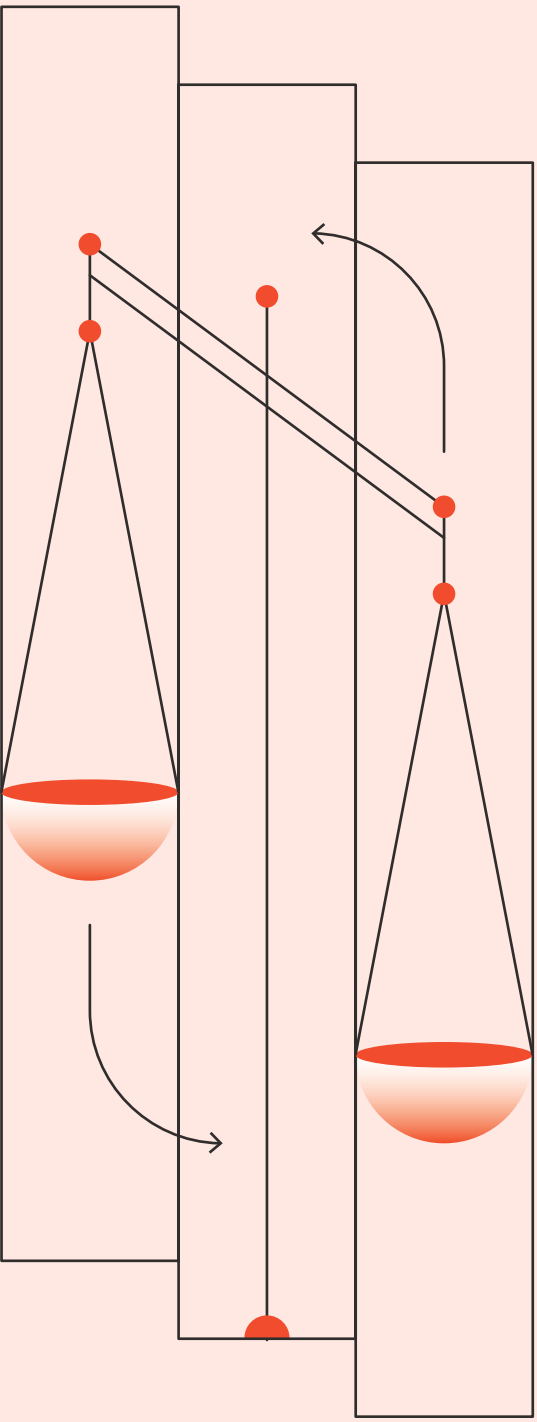
Segmentation plays a critical role in the event of a network breach. Traditional security measures lean hard on identity management and multifactor authentication to manage the perimeter, but credentials can be stolen or trusted individuals can go rogue, which lets malicious actors roam freely. You can block that lateral movement by breaking the network into small segments and limiting who has access to each segment.

By taking a methodical approach to building their security architecture from the ground up, agencies can go a long way to making zero trust both manageable and effective, Kindervag said. "I've been doing this for a long time too, for a lot a different systems," he said, "and it's something that translates to every single DAAS element that I've run across."

illumio

AI's Impact on Cybersecurity:

THE GOOD, THE BAD & THE AUTOMATION



AI, particularly generative AI (GenAI), is having a growth spurt of Big Bang proportions. Two or three years ago, GenAI was nowhere to be found in government or business applications; now, it's seemingly everywhere.

Splunk's State of Security 2024: The Race to Harness AI found that 93% of organizations — and 91% of security teams — say they use GenAI, although 65% said they don't fully understand the technology or its implications and 34% said their organizations lack a GenAI policy.

One thing everyone agrees on, however, is that AI will have a significant impact on cybersecurity. The global market for GenAI in cybersecurity is expected to grow to $3.13 billion by 2033 from $628 million in 2023.

The technology can greatly enhance monitoring, detection, response and recovery capabilities, but also allow threat actors to sharpen their attacks. However, that doesn't change the threat landscape as much as it accelerates each type of risk.

"First of all, let's define what AI is, and what it isn't — and how it's connected to governments," said Igor Lys, Founder of Gambit, a government advisory group, and Secretary General of the Government Tomorrow Forum, an international public/private partnership. "AI today is language models, predictive algorithms that are very powerful but are only good for specific tasks and, most of all, are for working with textual data. It is not an intelligence in the sense of something with a point of view, a capacity to understand things or being able to generate independent tasks for itself."

It may be only a tool, but it's a powerful one that can add much to cyber defenses, if organizations remember that AI-enhanced cybersecurity still depends on people. "The danger of AI is not coming from any new angle," Lys said. "In most cases, the weak link in cyber protection schemes is human, not the machine."

Here's a look at the ways GenAI can help government agencies, businesses and other institutions better protect their systems and data, and how it might supercharge attacks. For more details, click on the numerous hyperlinks throughout the article.

The Cybersecurity Benefits of GenAI



CYBER HYGIENE

The basics of cybersecurity, from using reputable software and promptly installing patches to encryption, fall under the umbrella of cyber hygiene. AI enhances many of these practices with real-time analysis, pattern recognition and, especially, automation.

"There are numerous examples of AI being used in government agencies to maintain cyber hygiene autonomously, without human supervision," Lys said. For example, the Department of Defense (DoD) uses AI-driven endpoint detection and response tools to monitor and analyze activities on computers, servers, mobile devices and other endpoints to gain a comprehensive view of a system's activities and health.

THREAT DETECTION AND IDENTIFICATION

Collecting and analyzing vast amounts of data enables AI models to quickly detect patterns and anomalies such as unusual user behavior or unexpected spikes in network traffic that could indicate the presence of malware, a phishing campaign or other attacks. Using automation, AI can identify potential threats in real time, send alerts to security teams and, in some cases, initiate a response.



Phishing detection and prevention are important uses of AI, since phishing is the most common attack channel that bad actors use to compromise user identities and facilitate ransomware and other attacks. A GenAI model can analyze an email asking for the recipient's login information and detect signs of fraud in the sender's address, website links or grammatical errors. The model then can alert the user and the organization's security operations center.



ENHANCING BIOMETRICS

Fingerprints and facial and voice recognition are essential components of multifactor authentication, which organizations increasingly use to deter identity compromises. GenAI can generate synthetic but very realistic biometric templates that improve biometric authentication systems, preventing attempts to spoof systems with deepfake biometrics.

PREDICTIVE ANALYSIS

The ability to analyze massive datasets and perform advanced pattern recognition also allows GenAI to predict threats and recommend steps to prevent them.



APPLYING SECURITY PATCHES

Overworked security teams often fall behind on patching because of the time and effort it requires, but with automated security patch generation, GenAI can streamline the process. GenAI can analyze a flaw, generate a customized patch, test it in a controlled environment (without exposing the production network) and then apply that patch to vulnerable programs or systems.





SECURE SOFTWARE DEVELOPMENT

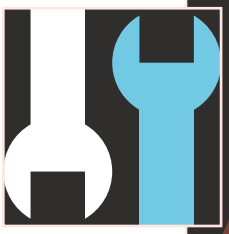
GenAI is used widely by software developers, who were among its first enthusiastic adopters. And although unsupervised AI code writing contributes to the problem of insecure software (see page 14), AI can also be part of the solution. When they find a flaw in code, AI models can help developers understand the problem and fix it faster. AI can also more efficiently carry out code reviews and generate tests to ensure that fixes were made and the code behaves as expected.



INCIDENT RESPONSE

AI's automation and analytics capabilities can strengthen each stage of incident response. Automated triage identifies the most critical incidents, allowing teams to focus on the most serious threats. AI also enables the use of automated playbooks that initiate responses, including basic steps such as blocking malicious IP addresses and isolating systems.

In today's cyber landscape, response isn't limited to individual agencies or organizations: Information sharing also is an important part of cyber defense. CISA recently staged a public/private tabletop exercise on AI security incidents, with the goal of identifying opportunities and protocols for information sharing and operational collaboration.



REMEDIATION

AI-powered security platforms can use predefined protocols and runbook strategies to isolate systems affected by an attack, stopping the spread of the intrusion and limiting damage. Meanwhile, AI analysis of both real-time and historical data can give security analysts insights to help speed recovery.



THREAT HUNTING

Manual threat hunting is typically a time-consuming, painstaking process involving teams of experts and numerous false positives. AI can help make effective threat hunting a reality with its powerful processing, accuracy at identifying threats and ability to detect patterns. High-speed automation and the ability to "learn" as it goes, adapting to changes in threat tactics, make AI an ideal tool when hunting for risk.

How to Build Mission-Capable Security Talent

An interview with Aaron Rosenmund, Senior Director of Content Strategy and Curriculum, Pluralsight



To navigate today's cybersecurity environment, federal agencies must build a pipeline of security talent. But that's a challenge: Depending on an organization's mission, it can take up to three years to train someone for a government security role, and during that time, they also need other on-the-job training.

"Beyond threats from other nations, I think the biggest issue for federal agencies is the skills pipeline," said Pluralsight's Aaron Rosenmund, who also serves as CyberShield's National Red Team Lead. There are several ways to address the cybersecurity talent shortage, he said.

REQUIRE RELEVANT HANDS-ON EXPERIENCE

Organizations need mission-related security training that addresses current threats and vulnerabilities — including hands-on learning tailored to specific jobs. "There's been really good progress, especially with some of the new work roles and IDs in the Department of Defense Cyber Workforce Framework," explained Rosenmund. "Part of that is you need to be hands-on and have someone check off that you've done that hands-on capability before you're qualified in your work role."

"One of the big things we need to do," he added, "is enable DoD to very quickly prove and check off [areas] of knowledge that people already have and offer practice in [areas] that people don't, so they can get qualified ... to go beyond mission."

INCORPORATE CIVILIAN EXPERIENCE

Although DoD and federal agencies require unique security training, they share certain tools and threats with the civilian sector. Exchanging such knowledge is key to strengthening cyber defenses. The National Guard offers an example, Rosenmund said, because "essentially half of [its] job is to provide as much support for the DoD as [it] possibly can." Though there's some concern regarding the training's impact on people's private lives, the relationship benefits both civilians and DoD, he said. Individuals return to their civilian jobs and a rotational, knowledge-sharing process develops. "I think that's our best way to keep the people and talent we need to ... dominate in the information space," said Rosenmund.

CONDUCT A SKILLS INVENTORY

Agencies must know what their team members can do, so Rosenmund recommended conducting a skills inventory or asking team members to complete skills assessments. Such benchmarking helps agencies distribute work quickly to the right people.

"We need to be nimbler," he said. "For instance, if there's something we [need to] execute on in two weeks, let's ... have a skills inventory within the DoD to identify people who are capable and qualified. And then let's get spaces where they can do missions regionally available to them [and] go back home."

HOW PLURALSIGHT HELPS

Pluralsight partners with federal agencies to develop security skills training that's specific to their individual needs, Rosenmund explained. "What we can do, and already do, is structure [our content] around the DoD Cyber Workforce Framework, but then also heavily focus on exactly what those agency missions are," he said. "And we provide a set of training that fully emulates the most advanced, persistent threats."

PLURALSIGHT

The Other Side of AI's Sharp Edge

Like any powerful tool, AI can be dangerous in the wrong hands, but attackers aren't the only concern. Unchecked AI also might create new vulnerabilities.

SUPERCHARGING EXISTING ATTACKS

Just as automation and analysis greatly enhance cyber defenses, AI tools can take cyberattacks to a new level. For example, where highly targeted spear phishing campaigns may begin with tens or even hundreds of emails, AI could enable an attacker to launch them by the thousands.

GenAI can sharpen those onslaughts, gathering such a detailed portrait of a target that the technology generates extremely sophisticated, personalized phishing attacks, even including visual elements such as logos to make its pitch seem more genuine.

Additionally, GenAI can create deepfakes of photos, videos or audio files that can be used in disinformation and smear campaigns. And bad actors can use GenAI for more practical matters, such as getting a victim to change their password or transfer funds.

AI VS. AI

Although most AI-fueled cyberattacks are just amplified threats from the so-called pre-ChatGPT era, Gambit's Lys said that AI itself can be vulnerable to AI-specific attacks, such as prompt injection and data poisoning, which fall under a class of cyberattacks called Adversarial AI or Adversarial Machine Learning.

In prompt injection attacks, attackers create a specific input designed to make the model behave in an unintended way. Data poisoning, meanwhile, feeds an AI model with specifically biased or purely fake data, causing the whole model to provide incorrect results from that point forward.

AI-GENERATED VULNERABILITIES

AI can introduce vulnerability on its own without proper supervision. For instance, research has found that AI-generated code contains roughly the same percentage of flaws as code humans create, and that programmers fail to identify incorrect ChatGPT code about a third of the time. Because many code snippets are reused, software vulnerabilities that go into production can quickly spread throughout the ecosystem.

STAY INVESTED IN PEOPLE

An important task for CISOs and other leaders is to educate themselves and others about AI and what it can do, Lys said. Use the most secure AI tools available, but don't expect miracles. "AI is not a magic wand," he said. AI can boost productivity, but only by so much. "Your main investment should be in human intelligence."

"Until we get to real, deployable, breakthrough technologies like the generalization of quantum encryption, AI-based cyber defenses, or cyber offense for that matter, all AI will just be an empowered version of what we already have today," Lys said.

Conclusion

This report is the third and final installment of our 2024 Cyber Guide series. Here is a look at the first two:



Part 1: The 2024 Cyber Agenda

2023 IN REVIEW: A YEAR OF GUIDELINES, HACKS AND NEW VISIONS

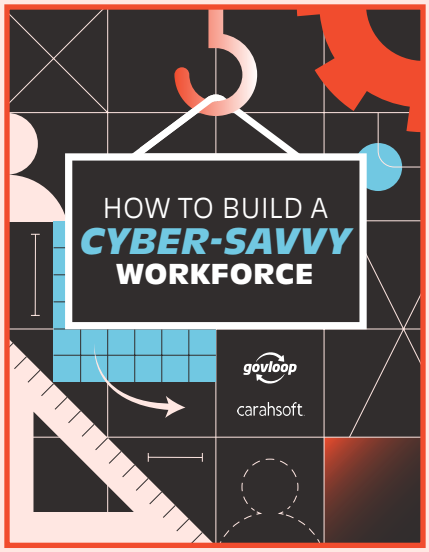
The March 2023 National Cybersecurity Strategy was just one of several federal efforts to put government agencies on better cyber footing.

THE 2024 CYBER AGENDA: URGENCY DRIVES INNOVATION

Federal, state and local agencies entered the year looking to make progress on numerous long-standing cyber challenges.

TURNING CYBER POLICY INTO PRACTICE

An interview with Cherilyn Pascoe, Director, National Cybersecurity Center of Excellence



Part 2: How to Build a Cyber-Savvy Workforce

AGENCIES ADAP TO SHIFTING THREAT LANDSCAPE

Among other challenges, government agencies find themselves fending off a wide range of state-sponsored hacking groups.

HOW ONE AGENCY WOVE ZERO TRUST INTO ITS CULTURE

The U.S. Department of Education is a case study in how to make zero-trust security a common cause across an agency.

BUILDING A CULTURE OF CYBER LITERACY

An interview with Rodney Petersen, Director, National Initiative for Cybersecurity Education, National Institute of Standards and Technology

Stay tuned for the latest developments when we begin our next Cyber Guide series in 2025!

govloop

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 Fortinet Federal, Illumio and Pluralsight for their support of this valuable resource for public-sector professionals.

CONTENT TEAM

John Monroe, Director of Content

Candace Thorson, Managing Editor

Lauren Walker, Senior Staff Writer

Susan Kirby-Smith, Senior Staff Writer

DESIGNERS

Kaitlyn Baker, Senior Creative Manager

Kelly Boyer, Motion Design Team Lead