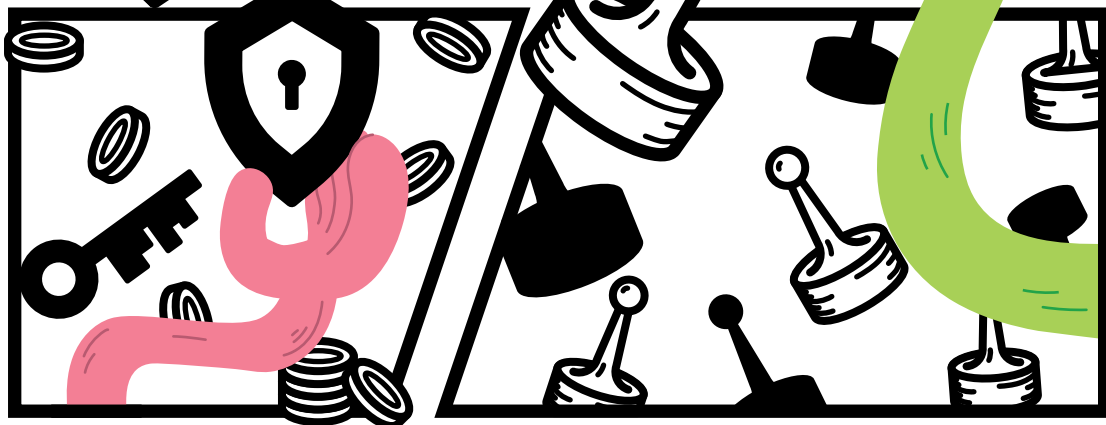
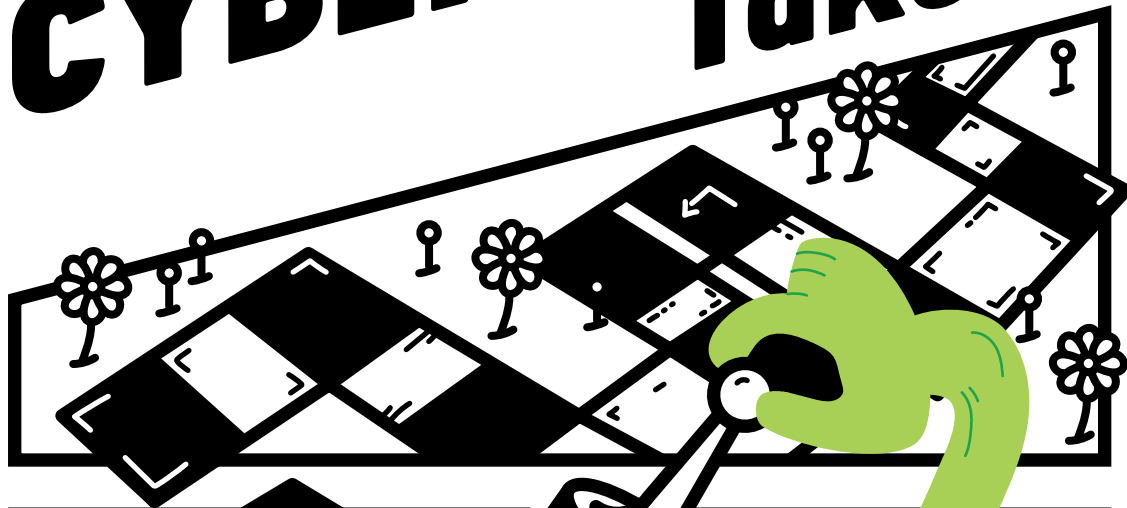
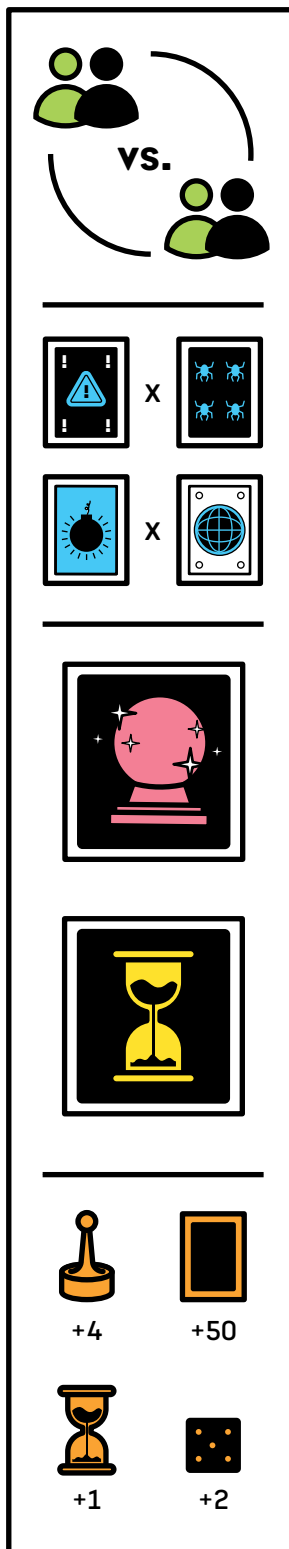




A New CYBER GAME PLAN Takes Shape



Introduction



It's not your imagination: The cyber threat landscape takes a turn for the worse every year.

Ransomware, once seen as slowing, has become a persistent threat. Data breaches continue to occur with alarming frequency. And now cyber experts are warning about the growing risk of potentially devastating attacks against non-traditional technology, such as that used by utilities and other critical infrastructure.

The problem is that malicious actors are endlessly inventive, finding new ways to get around existing defenses and engineering attacks for which no defenses exist yet. Agencies can't hope to find a foolproof approach to cybersecurity.

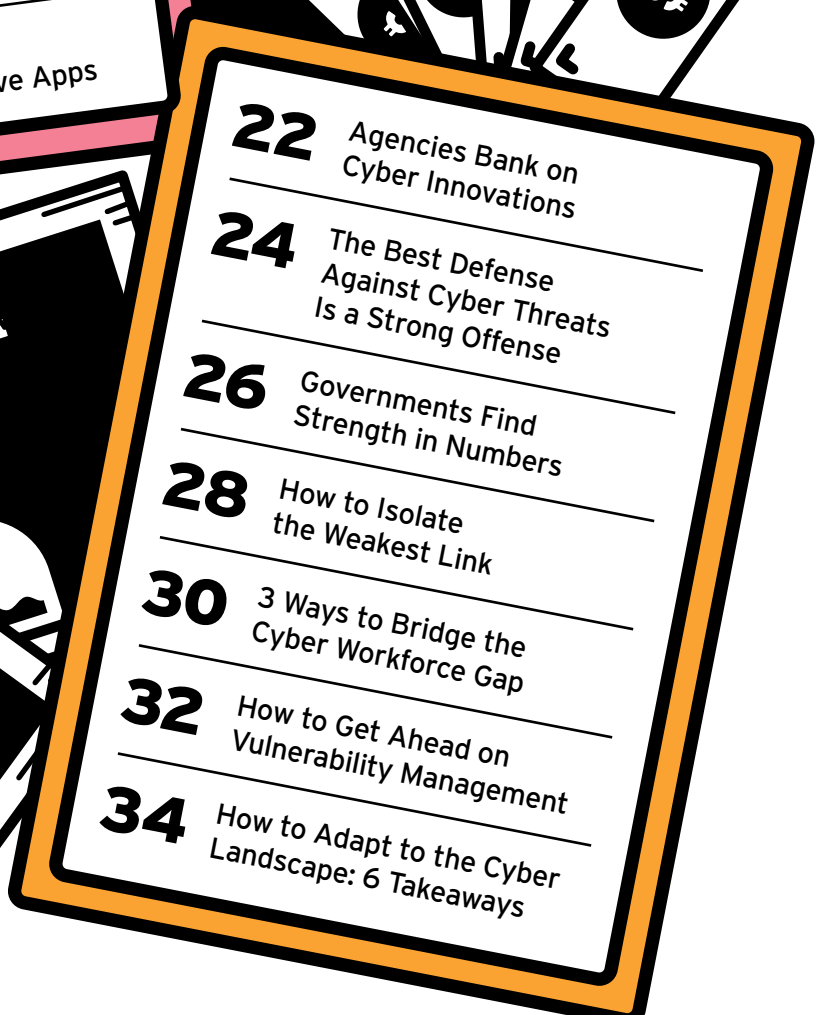
What they can do, however, is become more adaptive. This guide will look at how agencies can improve their ability both to anticipate threats and to change tactics as new threats emerge. Specifically, we highlight activity in three key areas: automation (including the use of artificial intelligence), training, and intergovernmental collaboration.

At the heart of this guide is a breakdown of the recently released National Cybersecurity Strategy, which will shape federal efforts in the years to come and provide a model for state and local governments to follow.

No doubt that strategy will evolve as the cyber landscape continues to evolve. But maybe, just maybe, the ongoing work highlighted in this guide will help bring some change for the better.

Table of Contents

- 
- 4** Mapping the Cyber Threat Landscape
 - 8** A Proactive Cyber Strategy
 - 10** What You Need to Know About the 2023 National Cybersecurity Strategy
 - 16** Zero Trust: What It Is, and Why It Matters
 - 17** 5 Ways to Tackle Cybersecurity
 - 20** How to Address the Risks of Cloud-Native Apps

- 
- 22** Agencies Bank on Cyber Innovations
 - 24** The Best Defense Against Cyber Threats Is a Strong Offense
 - 26** Governments Find Strength in Numbers
 - 28** How to Isolate the Weakest Link
 - 30** 3 Ways to Bridge the Cyber Workforce Gap
 - 32** How to Get Ahead on Vulnerability Management
 - 34** How to Adapt to the Cyber Landscape: 6 Takeaways

Mapping the Cyber Threat Landscape

Cyber experts often emphasize that there's no silver bullet for improving the security of government systems. The problem is not that technology always falls short. Instead, it's that the cyber threats are so varied and always evolving. Here is a look at the current threat landscape, based on recent cyber-related news and events.

A High-Level View

According to the 2022 (ISC)² Cybersecurity Workforce Study, the global cyber workforce has reached 4.7 million workers, but that still leaves 3.4 million positions unfilled. In the United States, the number of unfilled jobs stands at about 410,000, a 9% increase over 2021. As Fortune points out, these shortages are good news for cyber wages – and bad news for government agencies competing for talent.

Shadow IT – that is, technology that the IT department does not approve or manage – continues to be a bugaboo. In February 2023, for example, the Defense Department's inspector general found that “DoD personnel are downloading mobile applications to their DoD mobile devices that could pose operational and cybersecurity risks to DoD information and information systems.”

Another persistent problem: Agencies aren't applying patches to known vulnerabilities. A recent study by Tenable Research found that many organizations were falling victim to attacks that exploited well-known vulnerabilities, including some dating to 2017. In 2021, the Cybersecurity and Infrastructure Security Agency (CISA) debuted a catalog of nearly 300 known, exploited vulnerabilities; that list now stands at around 900.



The federal government has increased efforts to improve the security of the software supply chain. Beginning in September 2023, software vendors must attest that they are using secure development practices identified by the National Institute of Standards and Technology. But recent media reports suggest the deadline might be elusive.

Just the sheer volume of remaining work can be daunting. In a January 2023 report, the U.S. Government Accountability Office notes that its auditors have made 712 recommendations to federal agencies since 2010, 21% of which have not been implemented. “Until these are fully implemented, federal agencies will be more limited in their ability to protect private and sensitive data entrusted to them,” the report states.





Specters of a Cyber War

On Feb. 20, 2022, with the Russian invasion of Ukraine seen as imminent, New York Gov. Kathy Hochul said the state was strengthening its cyber defenses against possible Russian state-sponsored attacks against public institutions and critical infrastructure.

On Feb. 25, the day after Russian invaded Ukraine, Texas Gov. Greg Abbott directed the state's departments of Information Resources and Public Safety "to use every available resource to safeguard the state's critical infrastructure and to assist local governments and school districts with their needs."

Around the same time, CISA issued an advisory warning about an Iranian state-sponsored threat group known as MuddyWater, which was conducting cyber espionage and other malicious cyber operations targeting government and private-sector organizations worldwide. MuddyWater was a subordinate element within the Iranian Ministry of Intelligence and Security, according to CISA.

Meanwhile, in March 2022, cybersecurity firm Mandiant reported that a state-sponsored threat group in China had successfully hacked the defenses of six state governments in the United States during a 13-month stretch. The group exploited a well-known vulnerability called log4j.

In April 2022, two months after the invasion began, the United States and four other countries issued a joint cybersecurity advisory warning that Russian state-sponsored cyber actors could target critical infrastructure both within and beyond the region. The joint advisory provided links to more information about known threat groups.

Non-Traditional Tech Gets Targeted

In April 2022, GAO said the Department of Homeland Security urgently needed to improve the security of the nation's critical infrastructure, with a focus on the vulnerability of operational technology (OT) – that is, hardware and software used to control industrial equipment. "Water treatment facilities, power plants, and other critical infrastructure assets are increasingly connected to computer networks and the internet," the report states. "Recent cyber incidents targeting pipelines and other facilities underscore the need for effective cybersecurity to protect this infrastructure."

Also in April 2022, CISA warned that "certain advanced persistent threat actors" have developed the ability to gain access to multiple industrial control systems and related OT that could be used to disrupt critical infrastructure, especially in the energy sector.

A July 2022 report raised similar concerns about public transportation. A study conducted by the Mineta Transportation Institute and San Jose State University noted that public transit relies on external vendors to deliver services and provide critical technologies. Although advanced technologies have brought many improvements, they also have introduced new risks for agencies to mitigate, including ransomware.

In March 2023, the U.S. Environmental Protection Agency issued a memo urging states to include cybersecurity assessments as part of their regular audits of water systems. In a press release, EPA noted that a recent survey found that many public water systems "have not adopted basic cybersecurity best practices and are at risk of cyber-attacks."

Ransomware's Persistent Threat

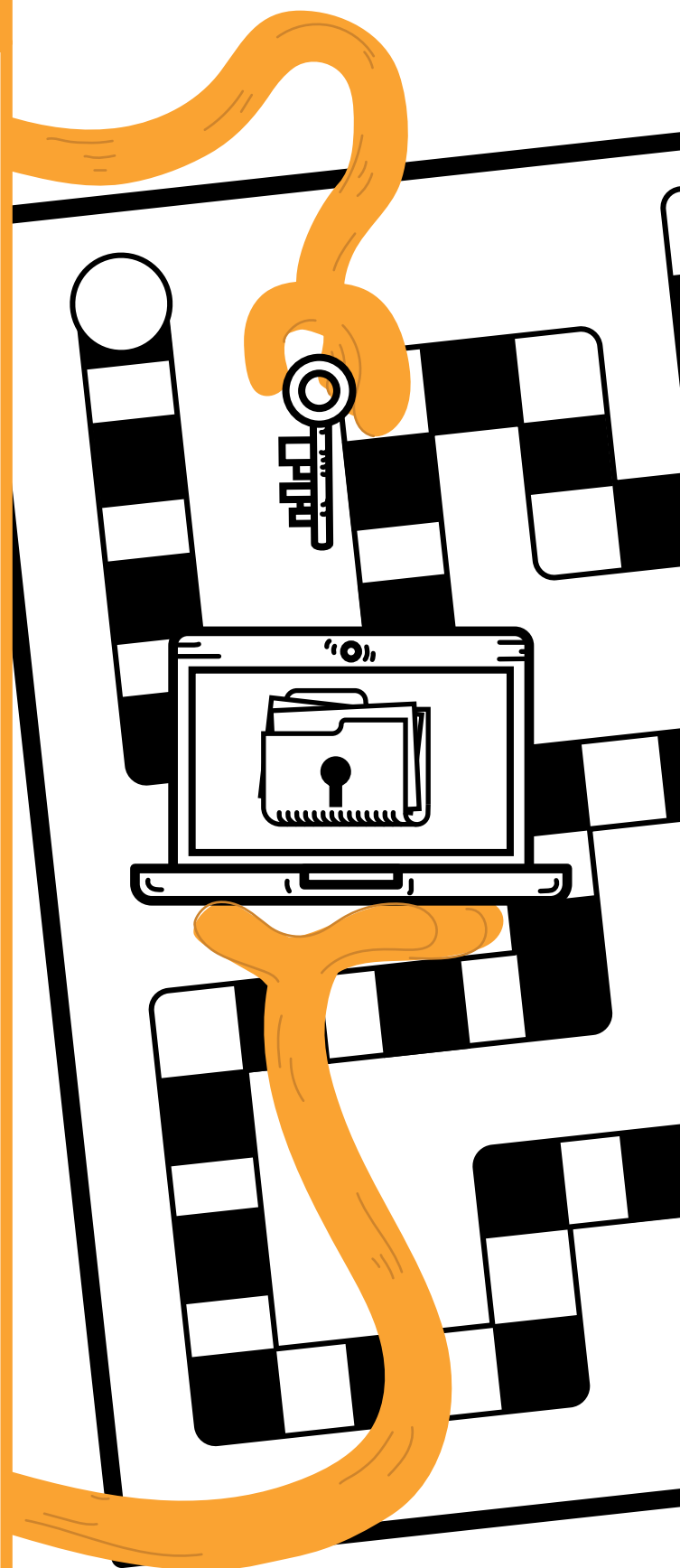
State-sponsored malicious actors in North Korea are targeting health care, public-sector agencies and critical infrastructure organizations, according to a [February 2023 advisory](#) that CISA and other agencies issued. The revenue generated goes toward supporting North Korea's various national objectives, including cyber operations against the United States and South Korea, CISA reports.

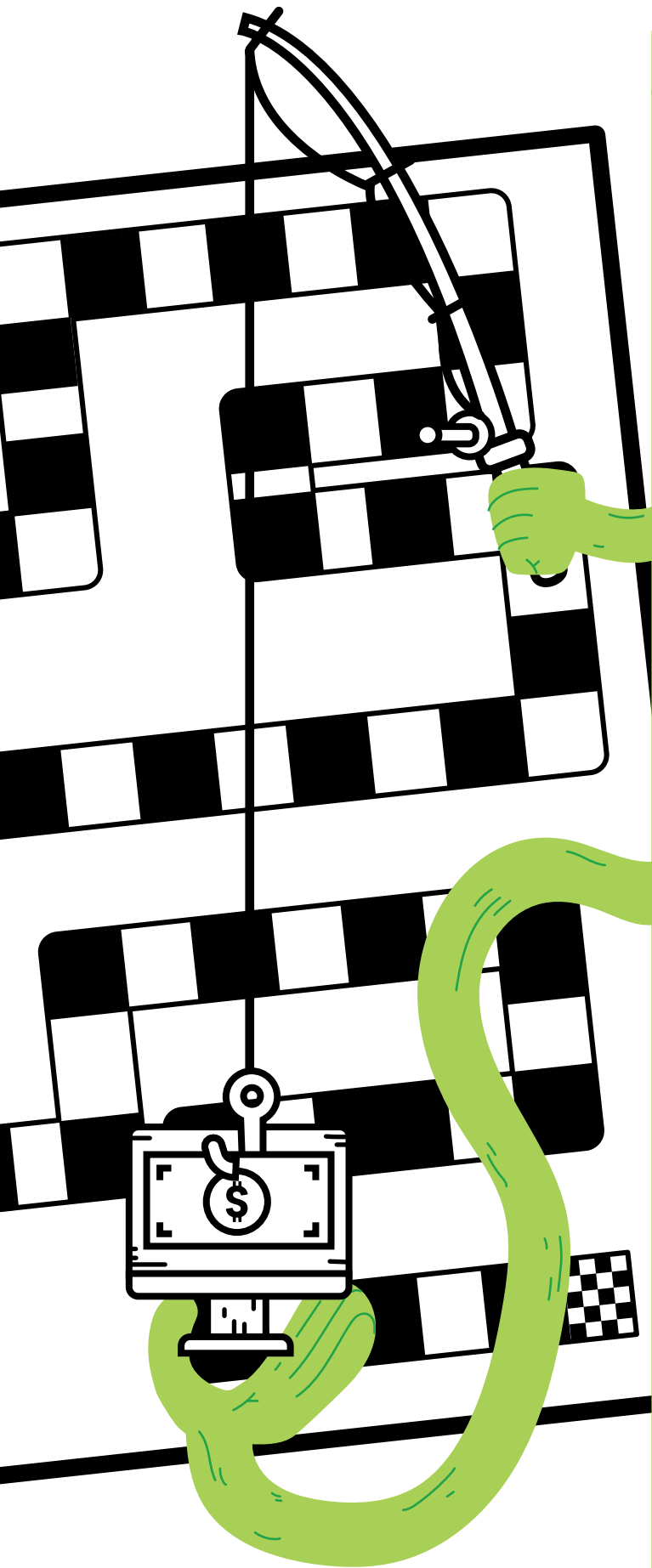
CISA also has noted that ransomware has become more of a commercial enterprise, with criminal groups turning to independent "[cybercriminal services-for-hire](#)" to do their work. Additionally, some ransomware groups now offer ransomware-as-a-service, making it easy for smaller groups to carry out attacks.

Experts warn that malicious actors are using more sophisticated tools that are increasingly difficult for their targets to defend against. For example, some are using a tactic known as [intermittent encryption](#). Rather than encrypting everything, they might encrypt every other 16 bytes, explains BleepingComputer, a security-focused media site. The encryption process takes half the time but effectively renders the file useless.

In some cases, attackers threaten to or actually publish stolen data as a way to coerce organizations to pay up. That was the case in a [recent attack](#) against the city of Oakland, California. In early March 2023, weeks after the attack, the hackers started posting online employees' personal information, such as names, addresses, and driver's license and Social Security numbers.

But the news is not all bad. Early this year, the U.S. Justice Department announced that the FBI has [hacked the systems](#) of the Hive ransomware group, which had been responsible for more than 1,500 attacks worldwide. In the process, the FBI captured more than 300 decryption keys for Hive victims who had been under attack, and another 1,000 keys for previous Hive victims.





The Cost of Human Folly

Each year, a study confirms what cyber experts always say: The weakest link in most cyber defenses is humans. Purposefully or accidentally, human action is a contributing factor in 82% of data breaches, according to Verizon's [2022 Data Breach Investigations Report](#). "As long as organizations continue to perceive and treat cybersecurity as a technical challenge, we will continue to lose this battle," wrote a cyber expert at the SANS Institute in a [blog post](#) about the report.

What motivates people to be more attentive to security? According to a [2022](#) study published in the journal *Computer and Security*, the answer is fear. Specifically, the study found that employees who have a better understanding of the risks and ramifications of security problems are more likely to adopt good cyber practices. That said, the researchers also noted that employees who experience a strong sense of belonging are more likely to become good "stewards of the organization's resources."

In March 2022, NASA's inspector general (IG) recommended that the agency expand its program for detecting insider threats from only classified systems to all systems. But the IG highlighted an important caveat: "On-going concerns including staffing challenges, technology resource limitations, and lack of funding to support such an expansion would need to be addressed prior to enhancing the existing program," [the report states](#).

Bad actors continue to develop new ways to fool even the most well-intentioned employees. For example, according to a [recent advisory](#) from the Multi-State Information Sharing and Analysis Center, employees at two federal agencies downloaded remote monitoring and management software after receiving emails that appeared to come from their agencies' help desks. The software enabled cybercriminals to access the users' systems and steal personal data.



A Proactive Cyber Strategy

An interview with Kevin E. Greene, Public-Sector Chief Technology Officer, OpenText Cybersecurity

opentext™ | Cybersecurity

Government often plays catchup to threat actors rather than tracking their activity early in the attack life cycle. But according to Kevin E. Greene with OpenText Cybersecurity, it is time for government agencies to become more forward-leaning, especially considering the new National Cybersecurity Strategy (NCS), which underscores the need to disrupt threat actors.

“Part of what the NCS emphasizes is taking a more proactive approach with cyber defense, actively hunting for early warning signals associated with threat actor behaviors to adapt and evolve cyber defenses to disrupt their campaigns,” he said.

Early Warning Signals

Unlike indicators of compromise, which are forensic clues discovered after a cyberattack happens, early warning signals detect an adversary’s preparations before the initial access phase of the attack life cycle.

For instance, an agency could use what we call global adversary signals and analytics to detect reconnaissance activities to gather information threat actors use to plan and execute their initial access for a cyberattack, Greene said.

Early warning is “basically creating an inspection shield looking for signals coming in and out of what we call a covered space [routable IP addresses] to detect compromised behaviors and suspicious communications to known infrastructure controlled by threat actors or infrastructure supporting compromised assets and resources, and using that ... to hunt for these signals in [security information and event management], XDR/EDR telemetry and drive better planning [and] repurposing of cyber defenses to be more resilient against cyberattacks,” he said.

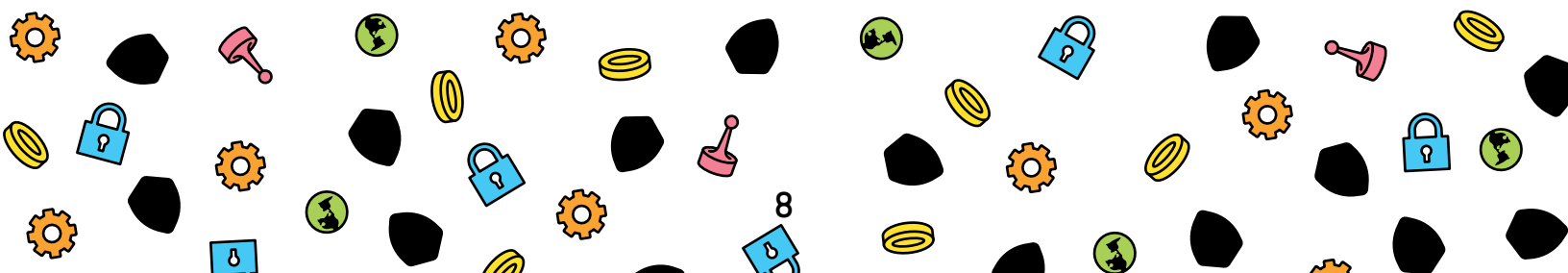
Zero Trust

If you work from the zero-trust premises of “never trust, always verify and assume compromise,” it is essential to incorporate good identity management hygiene and visibility into daily operations, Greene said. It forces users to pay greater attention to little things because “you can never take subtle notification alerts for granted,” he explained.

By leveraging mission-specific threat intelligence, government agencies can take what is considered a threat-informed defense approach to formalize their zero-trust strategies and make the right investments to mature their zero-trust architecture. But “at the center of everything is protecting the sensitive data, whether it’s in use, in motion or at rest,” he said.

For organizations that must do a lot, but with limited resources, adopting a proactive cyber stance can be difficult.

“Government is a little risk-averse, but I think we have to try new things, because some of the things we’re so used to are just not keeping pace with threat actors,” Greene said.



Take a proactive approach to cyber defense

Achieve greater cyber resiliency with a fundamental zero trust approach.

- **ENHANCE** cyber resiliency to deliver mission and business value
- **ANTICIPATE** disruption and minimize impact
- Continuously **EVOLVE** cyber capabilities to keep pace with threat actors
- **ADAPT** to new and emerging threats targeting the mission

What You Need to Know About the 2023 National Cybersecurity Strategy

When the Biden administration released its eagerly awaited National Cybersecurity Strategy (NCS) in March 2023, the big news was its requirements for potentially increased regulatory oversight and for the private sector to step up.

One major goal of the strategy is to shift responsibility for security away from individuals and small organizations – including state, local, tribal and territorial governments – to those “most capable and best-positioned...to make our digital ecosystem secure and resilient.” That’s primarily the federal government and cloud and infrastructure vendors.

But government has plenty to do under the new guidelines. For starters, NCS calls for accelerating modernization, specifically transitioning from legacy systems to the cloud and speeding up adoption of zero trust.

Specifics of implementation won’t be available until later this year, but here are some ways each pillar may affect you. The key takeaway is that you’ll be collaborating, coordinating and sharing information with other agencies, the private sector and even international allies as never before.

Big Picture

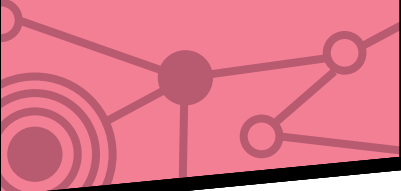
“Next-generation interconnectivity is collapsing the boundary between the digital and physical worlds, and exposing some of our most essential systems to disruptions.”

The strategy is designed to drive what it calls two fundamental shifts:

- **Rebalance the responsibility to defend cyberspace.** In short, individual users have been left to their own devices, making them weak links that malicious actors can exploit to access larger organizations.
- **Realign incentives to favor long-term investments.** The idea is to find “points of leverage,” or areas where small investments or “minimally invasive actions” could get everyone working toward building for “future resilience.”

Soundbite

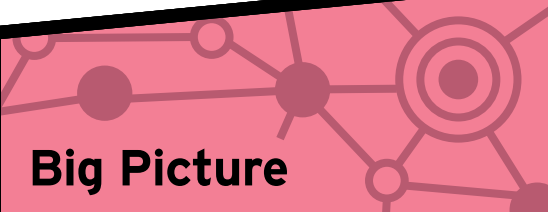
“Our goal is a defensible, resilient digital ecosystem where it is costlier to attack systems than defend them, where sensitive or private information is secure and protected, and where neither incidents nor errors cascade into catastrophic, systemic consequences.”



Pillar 1: Defend Critical Infrastructure

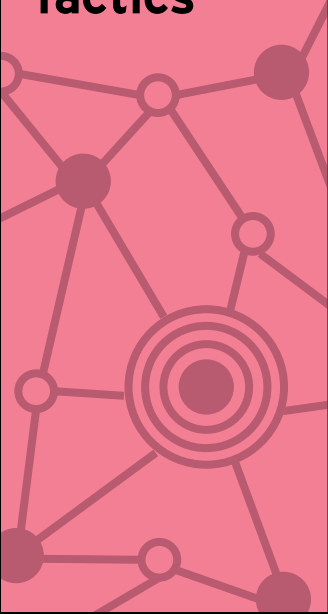
This pillar raises the minimum cybersecurity requirements in critical sectors, such as energy, nuclear, water, aviation and some high-priority manufacturing, whether public or privately owned.

Agencies, especially Sector Risk Management Agencies (SRMAs), will need to coordinate more tightly with CISA and operators of critical infrastructure systems and assets.



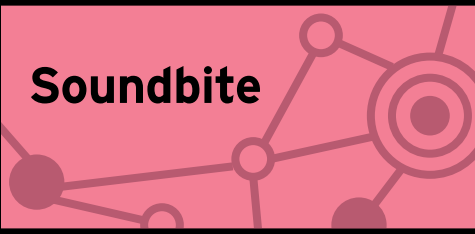
Big Picture

“We aim to operationalize an enduring and effective model of collaborative defense that equitably distributes risk and responsibility, and delivers a foundational level of security and resilience for our digital ecosystem.”



Key Tactics

- **Regulate, but carefully.** The administration plans to work with Congress to establish “minimum cybersecurity requirements” and to “mitigate related market failures.”
- **Broaden public/private collaboration.** The goal is to create a “trust-based ‘network of networks’” of cyber defenders, enabling “collective and synchronized action.”
- **Coordinate cyber centers.** Various agencies have cyber centers intended to support organizations managing critical infrastructure. But everyone could benefit from coordinated intelligence collection, analysis and partnerships.
- **Update the National Cyber Incident Response Plan.** ‘Nuff said.
- **Strengthen federal defenses.** In planning for better defenses in the long term – including the adoption of zero-trust principles – feds can serve as “a model for private sector emulation.”



Soundbite

“The American people must have confidence in the availability and resilience of this infrastructure and the essential services it provides.”



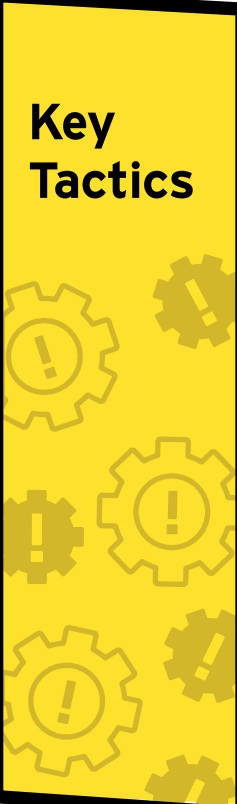
Pillar 2: Disrupt and Dismantle Threat Actors

This pillar is about undertaking large-scale efforts to attack the attackers. This means using all the tools of federal government – from law enforcement to diplomacy – to go after malicious cyber actors.



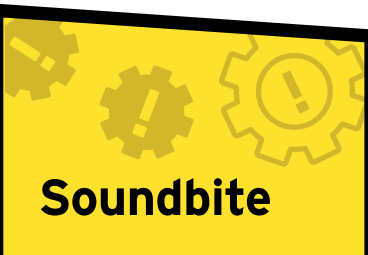
Big Picture

“Our efforts will require greater collaboration by public and private sector partners to improve intelligence sharing, execute disruption campaigns at scale, deny adversaries use of U.S.-based infrastructure, and thwart global ransomware campaigns.”



Key Tactics

- **Coordinate disruption campaigns.** Numerous agencies are involved in such campaigns, including the Justice Department and other law enforcement agencies and DoD. The plan calls for both technological and organizational platforms to support coordinated efforts.
- **Public/private collaboration.** In the same way, agencies should increase their work with private-sector organizations in areas such as threat hunting.
- **Share more and share quickly.** Information sharing with the private sector is a common practice, but it needs to happen at a greater scale and in a timelier fashion.
- **Defend against foreign actors.** Key IT services often go through foreign-based providers, which makes it difficult to identify malicious actors. Better visibility is needed.
- **Prioritize ransomware.** Ransomware can't be beat on a case-by-case basis. The plan envisions a multipronged effort focused on international cooperation, greater investigative efforts and crackdowns on digital money laundering.



Soundbite

“The United States will use all instruments of national power to disrupt and dismantle threat actors whose actions threaten our interests.”

Pillar 3: Shape Market Forces to Drive Security and Resilience

The focus here is carrot and stick – using federal buying power and regulations to push vendors toward best practices. This pillar is the core of NSC's commitment to shifting responsibility for breaches and their consequences away from individuals and small organizations and onto the private sector.

Big Picture

"To build the secure and resilient future we want, we must shape market forces to place responsibility on those within our digital ecosystem that are best positioned to reduce risk."

Key Tactics

- **Create accountability around data.** The plan calls for legislation that provides clear limits on how data can be used and how it should be protected.
- **Create accountability around software.** The plan also calls for legislation to establish liability for vendors developing products or services that are not secure.
- **Focus on IoT security.** The internet of Things encompasses sensors, baby monitors, industrial control systems and other devices connected to the Internet – many of which have few or no security features.
- **Use the power of the purse (1).** Through infrastructure-related grants programs, the federal government can stipulate the adoption of sound cybersecurity design, development and practices.
- **Use the power of the purse (2).** In the same way, good cybersecurity can be enforced through the procurement process.
- **Stabilize the cyber insurance industry.** Catastrophic cyberattacks can overwhelm programs designed to help organizations recover from attacks. The administration would like to explore options for providing a backstop.

Soundbite

"In too many cases, organizations that choose not to invest in cybersecurity negatively and unfairly impact those that do, often disproportionately impacting small businesses and our most vulnerable communities."

Pillar 4: Invest in a Resilient Future

A resilient future demands an upgrade from the no-longer-reliable past. The structure of the internet is getting old, and everything built on top of it is subject to its underlying vulnerabilities.

Big Picture

“The Federal Government must leverage strategic public investments in innovation, R&D, and education to drive outcomes that are economically sustainable and serve the national interest.”

Key Tactics

- **Secure the foundation.** The internet is built on an aging, vulnerability-riddled infrastructure. It's time for a major clean-up.
- **Spur more research.** Federal agencies and labs should prioritize cybersecurity research, with a focus on such areas as AI, industrial control systems, cloud infrastructure and encryption.
- **Prepare for quantum threats.** Quantum's massive power is expected to render many current encryption techniques useless. Research on new techniques needs to begin now.
- **Secure clean energy.** Many emerging clean energy solutions rely on automated, interconnected systems that are vulnerable to attack unless security solutions are developed.
- **Secure digital identities.** Many data breaches and fraud cases are possible because there is no foundation for creating strong, verifiable digital identities for use in online transactions. The federal government should support efforts to fill that gap.
- **Build the cyber workforce.** There are hundreds of thousands of unfilled cyber positions across the public and private sectors – and that's just in the United States. NCS calls for the development of a National Cyber Workforce and Education Strategy that draws on lessons learned and best practices from other countries.

Soundbite

“As we build a new generation of digital infrastructure...and prepare for revolutionary changes in our technology landscape brought by artificial intelligence and quantum computing, the need to address this investment gap has grown more urgent.”

Pillar 5: Forge International Partnerships to Pursue Shared Goals

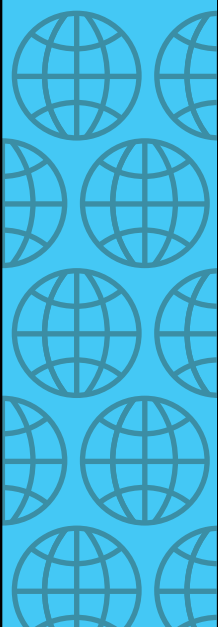
In addition to Pillar 2's emphasis on using international ties to thwart cyberattacks, NCS is intended to forge a cyberspace community that expects and rewards responsible behavior and makes it both isolating and expensive for states to engage in hostile cyberactivity.

Big Picture



"To counter common threats, preserve and reinforce global Internet freedom, protect against transnational digital repression, and build toward a shared digital ecosystem that is more inherently resilient and defensible, the United States will work to scale the emerging model of collaboration by national cybersecurity stakeholders to cooperate with the international community."

Key Tactics



- **Build coalitions.** Global internet freedom requires global solutions. The United States plans to build on and extend existing mechanisms (e.g., the Quadrilateral Security Dialogue) for collaborating across borders to respond to malicious activity.
- **Exchange subject-matter expertise.** The State Department is expected to coordinate a whole-of-government effort to share expertise and insights with cyber officials in other countries.
- **Give a helping hand.** U.S. cyber officials can help other countries respond to and recover from significant cyberattacks. The administration will establish policies for determining when such assistance is in the national interest.
- **Reinforce global norms.** When state-sponsored attacks occur, the global community, with leadership from the United States, should respond, both in terms of statements of condemnation and "meaningful consequences."
- **Secure global tech supply chains.** Today's technology infrastructure is built on hardware and software produced by an international supply chain, and that business model comes with risks that must be addressed. Ultimately, the goal is to build supply chains that "flow through partner countries and trusted vendors."

Soundbite



The United States will pursue these goals "while recognizing the need to work with partners to thwart the dark vision for the future of the Internet that the [People's Republic of China] and other autocratic governments promote."

Conclusion

Not all changes will happen quickly; NCS has a decade-long timeline. Plus, several of its provisions – notably, increased regulation of private players and funding – call for legislative action. The divided Congress almost guarantees compromise and possible blocking of some key points. Nonetheless, this strategy provides the blueprint for a stronger, more resilient and more secure digital future.

Zero Trust: What It Is, and Why It Matters

Traditionally, organizations took a moat-and-castle approach to network security: Anything within a network's perimeter was deemed safe, while external infrastructure and activity raised cybersecurity concerns.

But that approach has proven costly and insufficient as cyber criminals devise new schemes to invade our networks and traditional on-premises systems become more scattered and diffuse.

So, the federal government, some local governments and much of the private sector now are transitioning to a zero-trust architecture. It essentially turns traditional cybersecurity on its head.

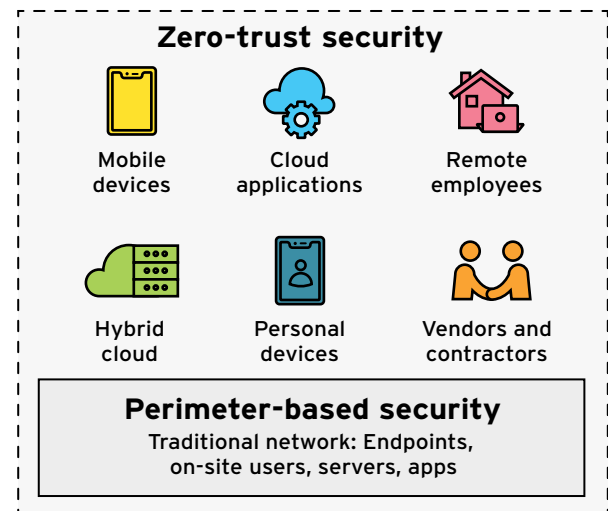
Rather than worry about perimeters, zero trust by default denies people access to enterprise information. Users are granted limited access based on their roles and responsibilities, and no one or device is implicitly trusted.

The framework relies on multi-factor authentication, encryption, and continuous monitoring and verification, among other features. Transitioning to a zero-trust architecture can be costly, though, and it takes time.

But it's critical. "Incremental improvements will not give us the security we need," said the Administration in a May 2021 executive order. "Instead, the Federal Government needs to make bold changes and significant investments in order to defend the vital institutions that underpin the American way of life."

"A transition to a 'zero trust' approach to security," the EO continued, "provides a defensible architecture for this new environment."

Zero trust vs. perimeter-based security



Source: [TechTarget](#)

Steps to build a zero-trust network

Network teams are largely responsible for deploying and configuring the elements that make up a zero-trust network. But security teams should also be involved in developing the overall zero-trust architecture.



STEP 1

Identify users and devices that attempt to connect to the network

Tool used:
Identity and access management



STEP 2

Set up access controls for application, file and service access

Tool used:
Next-generation firewall to create microsegmentation



STEP 3

Deploy tools to continuously monitor the network and device behavior

Tool used:
Network detection and response, AI for IT operations



STEP 4

Evaluate remote access to ensure proper security and authentication

Tool used:
Remote access VPNs

Source: [TechTarget](#)

5 Ways to Tackle Cybersecurity

Cybersecurity is a perpetual battle. As soon as agencies shore up their defenses, a new type of attack arises. But the [2021 Executive Order on Improving the Nation's Cybersecurity](#) has done much to give the good guys an edge. In addition to making "prevention, detection, assessment, and remediation of cyber incidents...a top priority and essential to national and economic security," the order calls for specific actions, including implementing zero-trust architectures, removing barriers to threat information sharing and improving threat detection.



"It's pretty amazing because for the first time in a lot of years, we're really transforming what cybersecurity is across the federal government and how we're handling things," said Amy Hamilton, Senior Cybersecurity Adviser, Policy and Programs, at the U.S. Department of Energy.



Bo Berlas, Chief Information Security Officer (CISO) at the U.S. General Services Administration, is optimistic about public-sector cybersecurity, too. "I can tell you from an agency perspective, we have a clear vision and a detailed plan that is really focused around executing against a set of challenges that we have," Berlas said. "That's a really great place to be."

So, just how are agencies tackling this persistent problem? Here are five ways.



1. Zero Trust

The concept of zero trust "assumes no implicit trust granted to assets or user accounts," providing a strategic opportunity to fundamentally change agencies' approach to cybersecurity, Berlas said. That change involves moving away from traditional perimeter-based security to "applying security with a focus on the data, with a focus on the device, with a focus around the user, and making sure that we not only validate that access initially, but do so on a continuous basis," he said.

One way GSA is doing that is through microsegmentation – dividing networks into segments and applying security controls to each. As a result, about 98% of users no longer connect over virtual-private networks, but over secure access and secure edge technology. "We've facilitated direct migration of roughly 30 to 40 buildings towards this microsegmentation model for more readily securing [operational technology/the Internet of Things]. We're focused around getting to roughly 500 buildings over the next three years."

Berlas cautions that some employees mistake zero trust as agencies not trusting them. "That really couldn't be any farther from the truth," he said. "It's about providing the right access at the right time."

2. Artificial Intelligence

Since OpenAI's launch of ChatGPT in November 2022, talk about AI has been at an all-time high, but AI in general has a role to play in cybersecurity because of its ability to pick out patterns – and anomalies – faster than humans can.

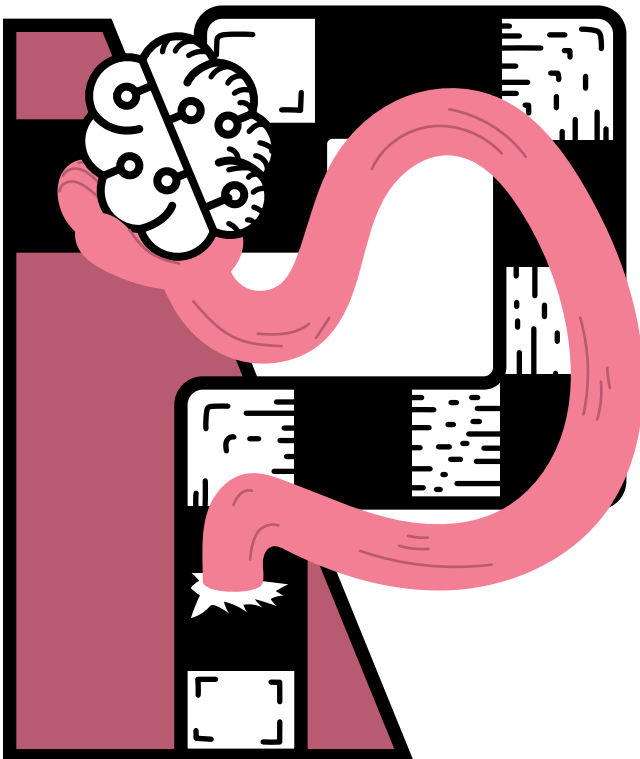
Consider how it could thwart phishing attacks by detecting when someone has clicked on a phishing link in an email, for example – something that at least one person at 86% of organizations has tried to do.



AI algorithms “help identify abnormal behavior, whether it’s an account or some other service running on the network,”

said Russell Marsh, Cyber Operations Director in the National Nuclear Security Administration’s Office of the Chief Information Officer (CIO).

“I would like to see us get to the point where AI and machine learning help us get more proactive,” he added, such as being able to identify IP-based protocols before they’ve gone all the way through to attack or before bad actors can broaden their account privileges across the network.



3. Information Sharing

Cyber threats don’t affect one organization alone, but rather government agencies at all levels. That’s why it’s helpful for officials to share information on what suspicious activity they’re seeing and lessons learned from past attacks.



For example, when threats of cyberattacks by Russia intensified in 2022, Jeremy

Wilson, Deputy CISO for Texas, used partnerships with CISA, the U.S. Homeland Security Department, and others to request dedicated sessions to understand the threat.

“We collaborate with other states as well,” Wilson said. “When you have those opportunities to kind of collaborate and share threat intelligence and talk about concepts, to me, that’s where the relationship really happens.”

He also pointed to the Texas Information Sharing and Analysis Organization, which had more than 1,500 members as of January 2022 and allows them access to intelligence and educational opportunities, plus information sharing.

4. Backups



In today's hyper-digital world, backups almost seem archaic, but they still play an important role, particularly in recovery from cyberattacks, said Gerald Caron, CIO and Assistant Inspector General for IT at the U.S. Department of Health and Human Services' Office of the Inspector General.

"If you want to be able to keep operations going, you've got to be able to restore," Caron said, adding that IT managers must regularly check backups for effectiveness and security. "Cloud technologies help a lot with that now because now you can set those to sync with those folders and basically your backup will be in the cloud. You're still able to work offline because you saved it to your local computer. When you get hooked back up, any changes you made will sync."

Fast recovery is crucial for many government agencies. For some, "it can mean life or limb if the right data isn't available to the right people at the right time," Caron added. "You want to recover as best as possible, but you don't want the same thing just reoccurring, so have a good plan, have good roles and responsibilities, [and] make sure that you recover in a proper fashion. Don't just...reboot and put things back online."



5. Tech Literacy

The biggest threat to cybersecurity is human error. And as technology advances and becomes more complex, the risks rise. To combat it, agencies must train employees, regardless of their job titles, to be more tech literate.



"When you don't understand or you don't know, you tend to have the most resistance" to change, said Cindy Good, a Program Manager at the Office of Financial Innovation and Transformation at the Bureau of the Fiscal Service at the U.S. Treasury Department. "Couple that also with the culture, or the mindset, of not wanting to change. Those are pretty big barriers, where even in instances where we've gotten the technology to deploy, we're finding it very difficult to scale at large."

One example is blockchain, which Good said could revolutionize the agency's financial services operations. "But the full benefits of that have not been realized just because there's limited stakeholder acceptance," she said. "So, there's the education piece, and also the adoption of it."

One way that the agency encourages change is by measuring how many pilot programs and proofs of concept it has completed. "We're also measuring how we are embedding these into our processes," she said.



How to Address the Risks of Cloud-Native Apps



An interview with Benjy Portnoy, Vice President, Global Solution Architects, Aqua Security

Software developers and malicious actors both love cloud-native applications, but for very different reasons.

Developers understand the many benefits of using cloud-native applications, including architecture, agility, flexibility and scalability.

Nefarious actors are increasingly exploiting the fact that traditional security solutions aren't equipped to manage the growing threat landscape in cloud-native environments, especially with technologies such as containers, Kubernetes, functions and pipelines.

Attack services are increasing, said Benjy Portnoy of [Aqua Security](#), which specializes in cloud-native security. "We see not just a significant increase in the volume of attacks that are specifically targeting cloud-native technologies like Kubernetes, Docker, etc., but also in the sophistication of these attacks, such as the evasion techniques being used," he said.

To provide robust security of cloud-native applications, Portnoy said, federal government agencies must address three key areas: people, processes and technology.

Fill the Knowledge Gap

Agencies need their security teams to have both the knowledge and the tools to secure cloud-native applications, said Portnoy. For example, what are serverless functions, and what are the ramifications for application security? What are common causes of Kubernetes misconfigurations, and how can they be exploited by malicious actors?

But agencies also need their developers to understand the risks involved and how to mitigate them during the development process.

"How do we foster that collaboration between security teams and the developers to ensure that the entire application lifecycle has the relevant processes and security controls in place?" he said.

Revisit Traditional Processes

Many core cyber defense processes built with traditional technologies in mind don't address the risks with associated cloud-native applications.

One challenge is that cloud-native applications typically are built using containers, providing a specific function that can scale as needed. This can pose a problem when it comes to a process such as incident response, said Portnoy.

"Typically, containers are ephemeral by definition, sometimes around for just minutes or hours," he said. "By the time a breach has been discovered, it's likely that the particular container that was used in this breach will no longer exist, making incident response and containing the attack a challenge."

Use Cloud-Native Tools

Automation is essential. One of the main reasons organizations adopt cloud-native methodologies is the speed with which they can develop, deploy and scale applications. Without automation, security risks will not be addressed, or mitigation efforts will gum up the works.

To address the complexity of this environment, Aqua created a Cloud Native Application and Protection Platform (CNAPP). Aqua's platform stops cloud-native attacks from code to cloud and back, identifying risks early in the application lifecycle while protecting production workloads from attack.

"Our platform was built to help organizations address the risks and gain visibility into the threats they face throughout the entire application lifecycle, ensuring that security teams understand the context of an attack so they can prioritize and remediate the highest risks to the business," Portnoy said.





we stop cloud native attacks. Guaranteed.

Secure your Agency's Software Supply Chain

Speed Cloud Compliance

Simplify Runtime Protection

About Aqua:

Aqua Security stops cloud native attacks across the application lifecycle and is the only company with a \$1M Cloud Native Protection Warranty to guarantee it. Aqua helps the U.S. Federal Government reduce risk while building the future of their agencies.

The AquaPlatform is the industry's most integrated Cloud Native Application Protection Platform (CNAPP), protecting the application lifecycle from dev to cloud & back. Aqua Security's CNAPP helps U.S. Federal Government agencies address, comply and execute on Executive Order (EO) 14028, OMB M-22-09, and various binding operational directives including BOD 23-01. We rapidly and securely transform cloud native adoption agencywide. Aqua is headquartered in Boston, MA.

For more information, visit us at <https://www.aquasec.com/solutions/federal> or contact us: aquasec-federal@aquasec.com or 866-436-204

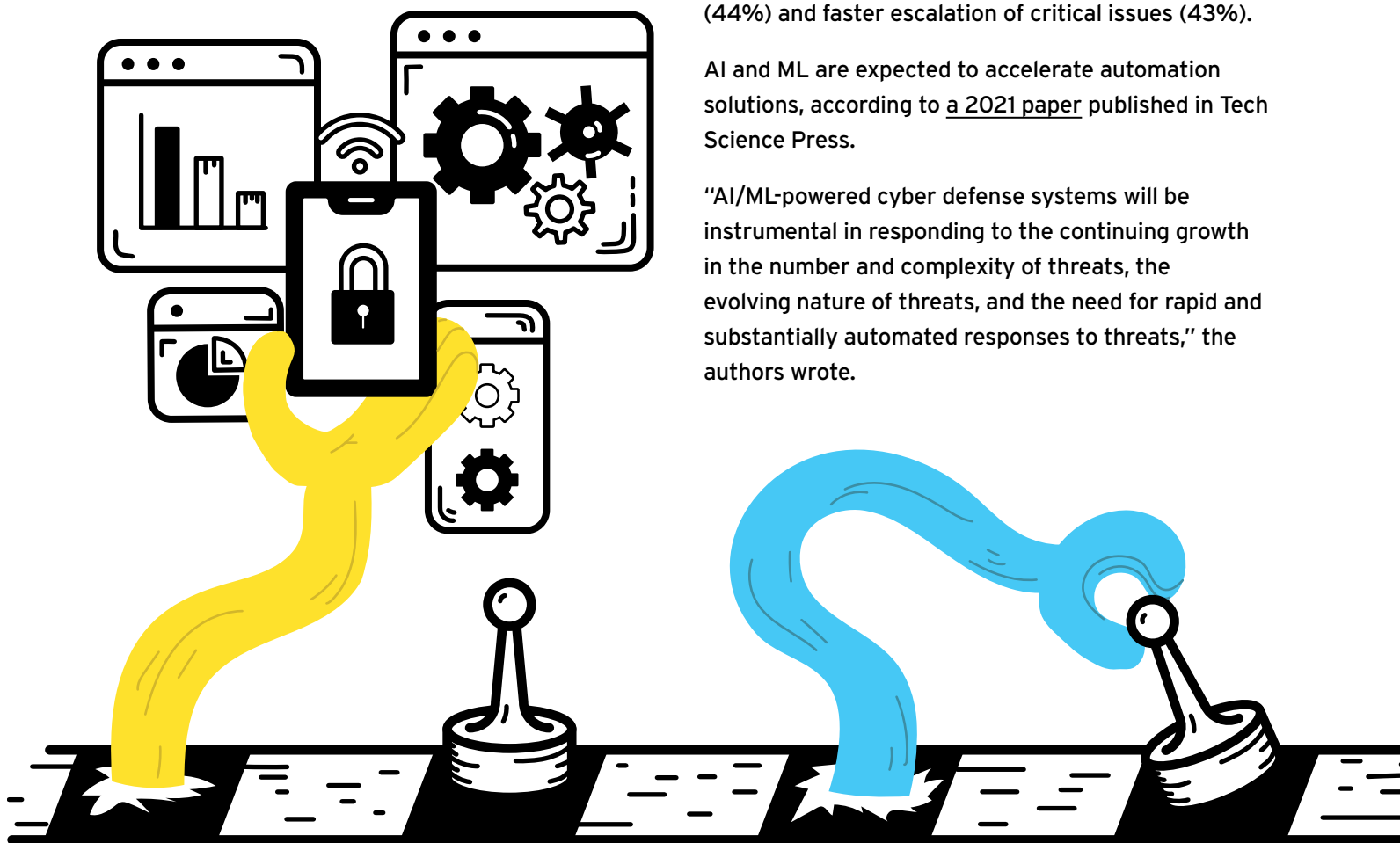


Agencies Bank on Cyber Innovations

Malicious actors are coming up with new tools and tactics faster than agencies can adapt. You might call it the cyber innovation gap.

This challenge has been a long time in the making. As the National Cybersecurity Strategy puts it, “public and private investments in cybersecurity have long trailed the threats and challenges we face.”

That said, both government and industry have been developing new solutions for addressing the cyber threat landscape, building on emerging solutions for automation, AI and machine learning (ML).



Cyber Accelerators

The goal is to help organizations get out of reactive mode, in which they play catch-up with malicious actors. Automation makes it possible for security teams to identify and adapt to potential threats and vulnerabilities, and to respond more effectively when attacks occur.

Increasingly, organizations are adopting security orchestration, automation and response (SOAR) platforms, which simplify the process of coordinating, automating and executing key security functions, such as vulnerability management, incident response and threat intelligence. SOAR platforms typically come with playbooks, providing users with basic approaches to common tasks.

In a recent survey by the Enterprise Strategy Group, 49% of respondents said automation improved their mean-time to respond, while 44% said it improved incident prioritization. Other benefits include more quickly isolating assets in the event of an attack (44%) and faster escalation of critical issues (43%).

AI and ML are expected to accelerate automation solutions, according to a 2021 paper published in Tech Science Press.

“AI/ML-powered cyber defense systems will be instrumental in responding to the continuing growth in the number and complexity of threats, the evolving nature of threats, and the need for rapid and substantially automated responses to threats,” the authors wrote.

Advancing the State of the Art

CISA is spearheading the development of numerous cyber automation solutions. Here are some of its flagship projects:

- **The Cyber Analytics and Data System (CADS)**, highlighted in the Biden administration's fiscal 2024 budget request, is intended to help security teams make more effective use of advanced analytics to identify, detect and prevent or mitigate emerging threats, according to a budget document. CADS will provide tools for ingesting and integrating cyber-related data, as well as for coordinating and automating the analysis of that data.
- **The CISA Advanced Analytics Platform for Machine Learning (CAP-M)** (formerly known as CyLab) is a virtual collaborative research environment in which CISA's cyber experts can test ideas for using data to tackle cybersecurity problems. CAP-M can run on-premises and on a multi-cloud platform. CISA will share lessons learned from its research with partners across government, industry and academia.
- **The Advanced Data Analytics and Machine Learning Technologies Program** is focused on using data to assess risks across cyber, physical and blended cyber-physical environments – a major concern when it comes to critical infrastructure. As part of its mission, the program is intended to build the foundation for using AI. Activities include developing representative datasets for AI training, providing computational testing capabilities and assessing emerging analytic tools.

Worrying About Quantum

NCS identifies quantum computing as a high-priority concern.

Quantum computing uses subatomic particles to run a massive number of calculations in parallel. "This means quantum computing may revolutionize our ability to solve problems that are hard to address with even the largest supercomputers," according to the U.S. Department of Energy's primer on the topic.

All that compute power has cyber experts worried. Traditional encryption techniques essentially are just difficult math problems. But future quantum computers might not find them so difficult, QuantumXchange explains.

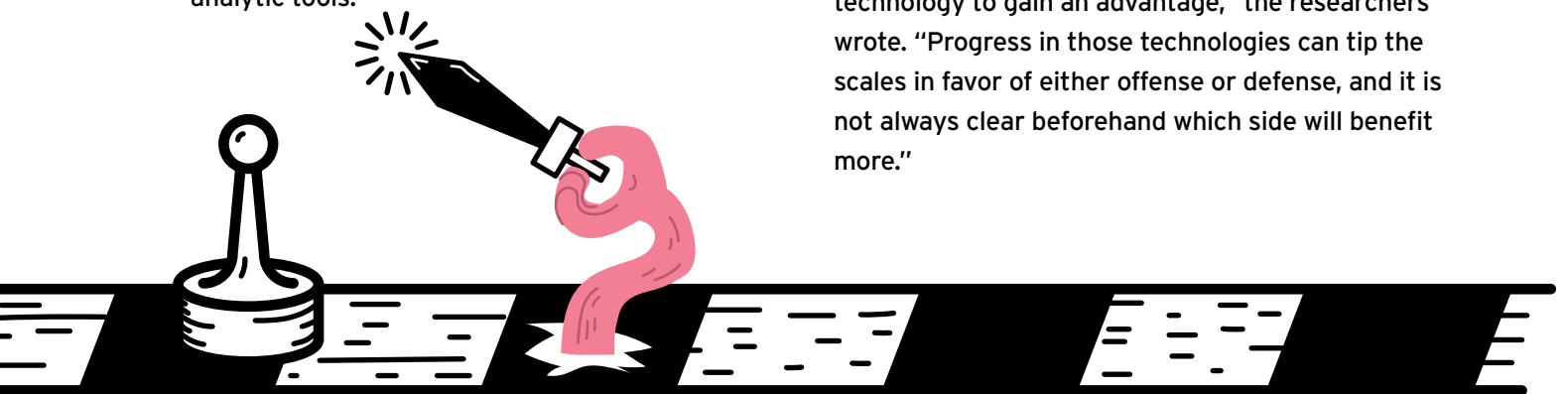
NCS calls for the federal government to plan a transition to quantum-resistant cryptography environments and to determine how to ensure cryptography's continued evolution.

A Double-Edged Sword

Cyber experts have similar worries about AI and ML. Although this technology will play a critical role in strengthening cybersecurity, it doubtless will also fuel efforts to crack those defenses.

For example, cyber criminals are expected to use emerging AI-based chatbot solutions to devise much more convincing phishing emails, leading more unsuspecting users to click on malicious links, according to a report from the Center for Security and Emerging Technology.

"Cybersecurity is a constant battle between attackers and defenders who try to leverage advances in technology to gain an advantage," the researchers wrote. "Progress in those technologies can tip the scales in favor of either offense or defense, and it is not always clear beforehand which side will benefit more."





The Best Defense Against Cyber Threats Is a Strong Offense

An interview with Marty DeConcilis, Vice President, Federal Sales and Engineering, Fidelis Cybersecurity



In today's highly contested cyber environments, agencies must be faster and smarter than even the most sophisticated adversary. Retroactive analysis and periodic scans aren't enough. And even with the best tools, you must assume that attackers will – or already did – find their way in. Only a proactive cyber defense will help you stop attackers early enough in the kill chain so that threats don't become costly incidents. In other words, you need to put your cyber defenders back on the offensive.

"A proactive cyber defense is essential to winning the war against cyber threats," said Marty DeConcilis of Fidelis Cybersecurity. "The first step is to fully understand your environment, so that you can be prepared to detect, distract and defeat whatever comes next."

Here are three strategies for proactive cyber defense.

Understand Your Cyber Terrain

You must understand your environment better than your attacker. That means having visibility into all traffic, and ongoing risk prioritization. Only then can you identify potential attack vectors, isolate issues and resolve problems before they escalate.

"Once you have automated systems that continuously discover, analyze and map your cyber terrain, you can put that intelligence to use and stay ahead of adversaries," DeConcilis said.

Follow the Data

Addressing cyber threats requires strong data loss prevention (DLP). But in today's hyper-connected environments, traditional DLP can't keep up. True data protection requires a continuous understanding of data access and movement throughout your network – which is called network DLP.

"Real-time insight is essential to quickly detect and investigate threats and prevent sessions that violate policies," said DeConcilis. "You need deep, contextual analysis of data movement in real time to spot and stop risks."

Outmaneuver the Attackers

Post-breach technologies that put you back in control of your environment, including deception and active threat detection, are imperative to cyber resilience. Deception technology changes the attack surface and lures attackers into a contained area of your network. Active threat detection works in conjunction with DLP and deception to correlate alerts and provide strong, actionable conclusions about active threats. This means fewer false positives and faster response times.

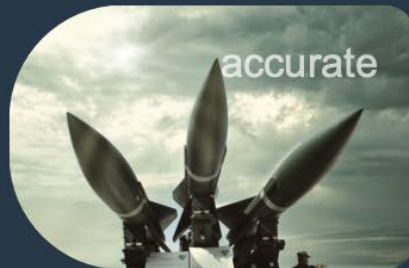
"With deception in place, defenders can hunt, detect and defend with great speed and confidence. And active threat detection provides high-confidence conclusions about attacks, including attack stages and the tactics, techniques and protocols in use," DeConcilis said. "Together, these solutions help stop active threats and prevent re-engagement."

Fidelis Elevate is an eXtended Detection and Response (XDR) platform designed for proactive cyber defense. It automates security operations across traditional network architectures and extends seamless security controls into the cloud, across all network ports and protocols, and out to endpoints.

With patented Deep Session Inspection and in-line decryption, Fidelis Elevate catches DLP risks other tools miss, providing content with rich context. Fidelis Elevate includes built-in deception and game-changing active threat detection. This platform delivers cyber resilience that gives defenders strategic advantages over evolving threats.



Detect, Respond and Neutralize Threats Faster



Governments Find Strength in Numbers

Increasingly, government leaders recognize the need to approach cybersecurity in the same way they approach public health: There must be a holistic network in which the well-being of individuals, or individual systems, depends on and benefits the well-being of others.

Like viruses, cyber threats succeed by finding a vulnerability before moving on to overwhelm the larger population. The more they succeed, the longer they stay in circulation, putting everyone at risk.

It is in our best interests not only to share resources and expertise, but also cyber intelligence, to create a more complete picture of the threats in the digital ecosystem. Forewarned is forearmed.

Collaboration is inherent in the National Cybersecurity Strategy. “By working in partnership with industry; civil society; and State, local, Tribal and territorial governments, we will rebalance the responsibility for cybersecurity to be more effective and more equitable,” the strategy states.

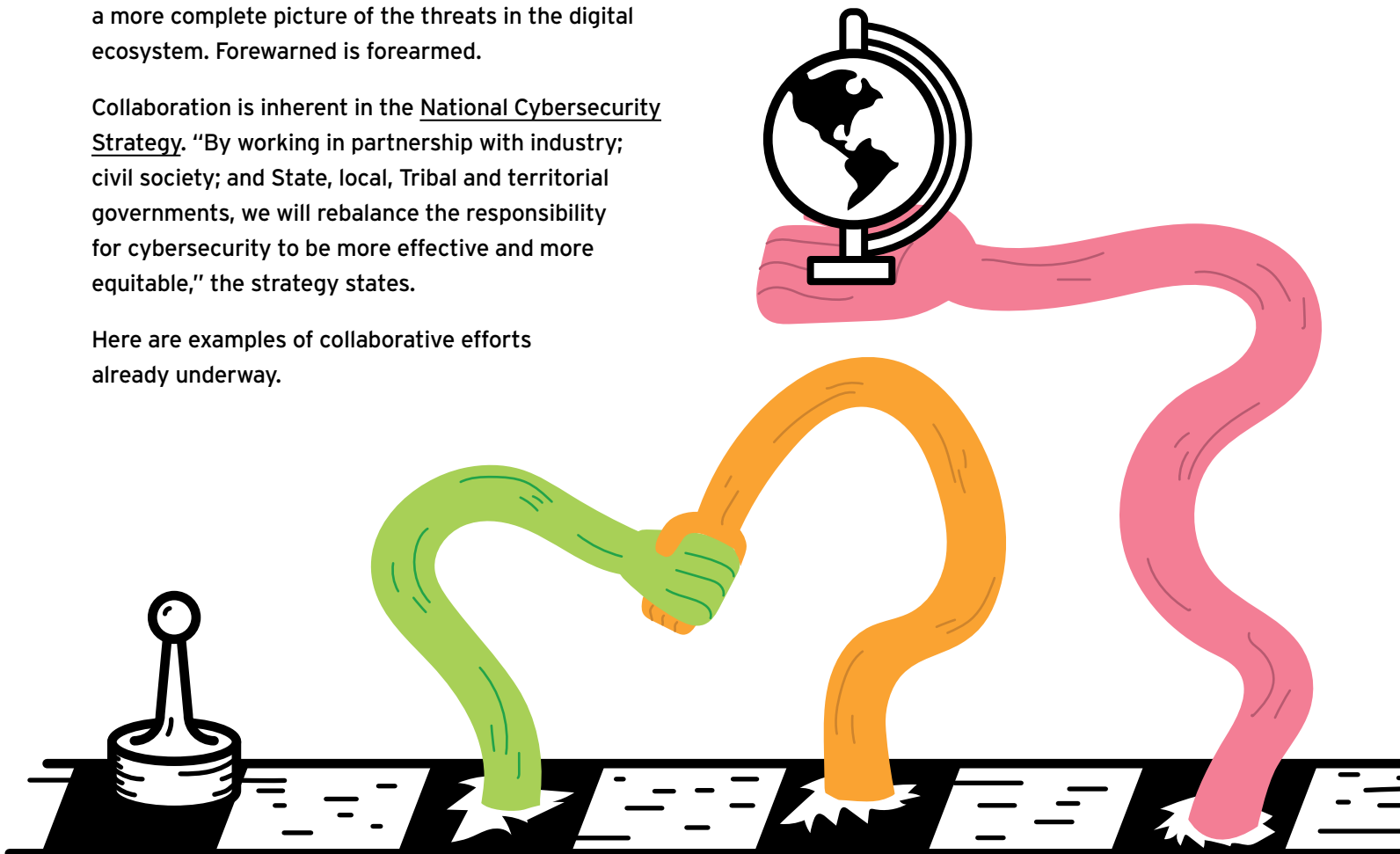
Here are examples of collaborative efforts already underway.

CISA Coordinates a National Effort

The federal government has collaborated with state governments on cybersecurity over the years. But the National Defense Authorization Act (NDAA) of 2021 institutionalized those efforts by creating a network of state coordinators under CISA's purview.

The goal is for each state to have a federal, on-the-ground cyber expert. These coordinators will work with public- and private-sector organizations, providing advice, supporting preparation, incident response and mediation efforts, and connecting those organizations with federal resources.

“Cybersecurity for state and local governments is just as important as efforts at the federal level, and frequently, they lack the resources, technical know-how, and situational awareness to secure their systems, or respond in the event of an attack,” said former Sen. Rob Portman (R-Ohio), one of the original sponsors of the bill incorporated into the NDAA.



DHS Extends Funding to Local Agencies

Federal efforts also can help spur collaboration within states. That's the hope for the State and Local Cybersecurity Grant Program and Tribal Cybersecurity Grant Program, as part of the Bipartisan Infrastructure Law.

With a historic \$1 billion, the program funds agencies for four years to address risks and strengthen security, particularly for critical infrastructure. CISA and the Federal Emergency Management Agency will approve state plans, with committees comprised of cybersecurity representatives from counties, cities, towns, public education and public health. States are required to distribute at least 80% of the funding to local and rural communities and 3% to tribal governments, for new and existing programs.

At a 2022 conference of the National Association of State Chief Information Officers, state participants were asked what a successful State and Local Cyber Grant Program would look like. One of the hallmarks of a good program, they said, was that it would "[break] down barriers between state and local government and foster 'an inertia of collaboration'."



States Create Cyber Fleets

Federal support and direction are essential, but states also need to run their own cyber defense vessels.

In February 2022, New York Gov. Kathy Hochul established the Joint Security Operations Center (JSOC) to unite local, state and federal response efforts and data collection. It includes businesses that operate critical infrastructure, plus DHS, Emergency Services, the New York State Police, the Metropolitan Transportation Authority, the Port Authority of New York and New Jersey, and other entities.

Qualified personnel from across New York staff JSOC, which is headquartered in Brooklyn, both in person and virtually. Officials expect the center's central view of threat data to make it easier to detect and respond to emerging threats and to accelerate remediation efforts.

Other states, such as Illinois, North Carolina and Utah, have established similar task forces that include their state's emergency management agencies, police, the National Guard and infrastructure partners.

Cyber Care on the Global Landscape

But a holistic approach needs to go beyond the public sector.

With that in mind, Congress created the Joint Cyber Defense Collaborative (JCDC) in 2021 for public- and private-sector partners worldwide. The collaboration involves service providers, infrastructure providers, cybersecurity experts and researchers who can share information, decrease threats and build defense plans to serve the global community.

Every government agency, business and nonprofit is part of our cyber landscape. That means that each entity's level of security is tied to the next, in more ways than we can imagine. As the JCDC website says, "No one entity can secure cyberspace alone."



How to Isolate the Weakest Link

An interview with Mike Rider, Senior Solutions Engineer, Menlo Security



If you think about it, there's a fundamental disconnect between the concept of zero trust and the approach traditional security technology takes.

As employees browse the internet or open email, legacy solutions scan the content for potential threats before allowing access. That's not zero trust. That's "innocent until proven guilty."

If you take zero trust seriously, you will treat all content as if it's malicious, whether you detect a threat or not.

That's the mindset behind isolation technology, said Mike Rider of Menlo Security, which provides browser- and email-based isolation solutions.

"With isolation, our default approach is that all content is malicious, and we treat it as such (i.e., never trust it)," Rider said. "Never let the end user have access to it, but instead, always deliver to them a safe, sanitized version."

How It Works

Think about going through airport security. Imaging technology and metal detectors scan every person and their bags. If a system detects something suspicious, security officials pull that person and their bags aside for greater inspection. That's how traditional security tools work.

Now, imagine if every person and every bag were automatically subject to the highest level of scrutiny. That's how isolation technology works.

Browser isolation routes web traffic through a cloud-based remote browser where all content can be activated in a safe environment. If nothing malicious is present, the content is passed on to the end user.

Agencies can take a nuanced approach to restrict browsing. Some websites might be blocked fully, and others might be accessible, but in view-only mode. Menlo Security's solution enables agencies to create granular policies that define who can access what type of file in what mode.

Security at Speed

Of course, if airport security worked the same way, no one would make their flight. But that's not a problem with isolation technology, said Rider.

For example, when the Defense Department (DoD) adopted browser isolation, users saw a 50% reduction in load times of web content, according to the Defense Information Systems Agency.

That's because under its old approach, security scans happened at the department's internet access points, which led to bandwidth congestion. Moving security to the cloud eliminated those chokepoints.

Although DoD is a unique environment, most agencies should expect the performance of browser isolation to be on par with their standard internet connection, Rider said.

Isolating the Human Factor

A 2021 global study by IBM found that 95% of successful attacks or breaches involved human error. It's just human nature, Rider said: No matter how much training people receive, they are bound to click on links or visit sites that they shouldn't.

With isolation technology, "users can freely navigate the web and make mistakes, which they will do, without bringing risky content into an organization," Rider said.





Cloud Security Platform Powered by an Isolation Core™

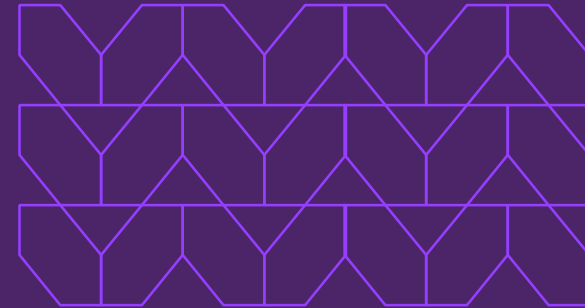
Empowering organizations with the essential Internet security platform they need to eliminate threats and protect productivity.

What's stopping malware?

The work-from-anywhere policies necessitated by the global pandemic have created more flexibility for the world's workers, but an unwanted result was an increase in security vulnerabilities. With the broader range of ways that people are connecting to enterprise networks every day, the concept of a secure perimeter is officially obsolete.



menlosecurity.com/federal 29



Three things to know:

While recent work-from-anywhere policies have created more flexibility for the world's workers, they have also led to increased security vulnerabilities, as the browser is still the most common attack vector.

Menlo Security adopts a Zero Trust approach to this security challenge through its Isolation Core™ technology, which prevents attacks from reaching users in the first place by moving the browsing process off the desktop and into the cloud,

Menlo Security consolidates all Secure Web Gateway (SWG) capabilities—including CASB, DLP, RBI, proxy, sandbox, FWaaS, and private access—into an end-to-end single cloud-native platform. The platform also integrates with SD-WAN to provide an integrated Secure Access Service Edge (SASE) solution. It is also extensible via an API framework and features a single interface for policy management, reporting, and threat analytics across all the consolidated services.

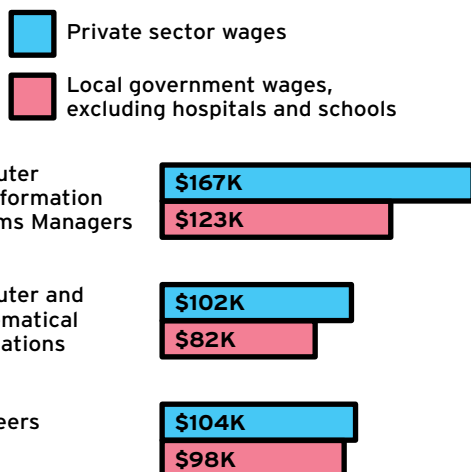
3 Ways to Bridge the Cyber Workforce Gap

Implementing the new NCS will take many technical professionals at a time when an estimated 40,000 to 45,000 public sector cyber positions are going unfilled and 69% of state and local human resources officers are reporting an IT-hiring crunch.

Despite a Federal Cybersecurity Workforce Strategy that's been in place since 2016 and a Federal Cyber Workforce Management and Coordinating Working Group dating from 2019, governments continue to struggle to find enough qualified cyber personnel. That's partly because they're competing with a private sector that's short an estimated 710,000 professionals – and can pay more.

Tech workers earn more in the private sector than in local government

Average salaries for tech workers in U.S. dollars.



Source: Michael Brady/Smart Cities Dive

Better Balance and Benefits

Government may be able to capitalize on recent layoffs at major tech firms – but salary remains a stumbling block.

Although agencies may not be able to compete with industry on pay, other benefits also matter – especially to younger workers.

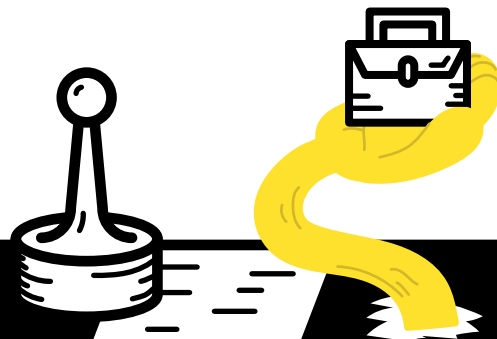
Public-sector jobs can attract new talent by offering:

- Student loan repayment
- Hybrid and remote work
- Health care, financial and other benefits
- An important mission

At the National Science Foundation (NSF), an agency that's competing for scientists, doctors and others who can make more money in the private sector, flexibility can be a deciding factor, explained Wonzie Gardner Jr., Office Head and Chief Human Capital Officer for NSF's Office of Information and Resource Management.

"Work-life balance is so important to millennials," Gardner said, speaking at a recent GovLoop virtual event. "Remote work, hybrid work, supporting new parents – these are key for both recruiting and retention."

And don't forget the agency's mission. It's what distinguishes a government career from one in the private sector. Many people seek meaning in their work – and those are the people you're looking to hire. Emphasize how their role contributes to the agency's overall goals.



Seek Talent Early and Often

Accelerate your hiring pipeline and tap into it early. That means internship, fellowship and other programs that catch workers early in their careers, or even while they're still in training.

One such program is the Office of Personnel Management (OPM)'s CyberCorps "Scholarship for Service," which recruits young professionals in IT, industrial controls, and security for federal, state, local, tribal and territorial governments. The scholarships, for up to three years of undergraduate or graduate study, require recipients to work in government for the same number of years that they received the aid.

Cities and states reach out to local institutions in various ways. For instance, Kansas City, Missouri works with local universities by hiring graduate students to help with city projects, and the students can stay on after graduation if they choose. Washington, D.C., has a pilot program that trains inmates for Amazon Web Services Certified Cloud Practitioner certification, giving them a chance at better jobs when they're released. The key is to be creative and take advantage of local resources.

You can also reduce barriers in the hiring process – for instance, by adopting OPM's 45-day hiring model and replacing academic requirements with skills-based ones. For federal agencies seeking cyber talent, OPM has the Cybersecurity Hiring Resource Hub, which brings together information on incentives and expedited application processes.

Grow Your Own

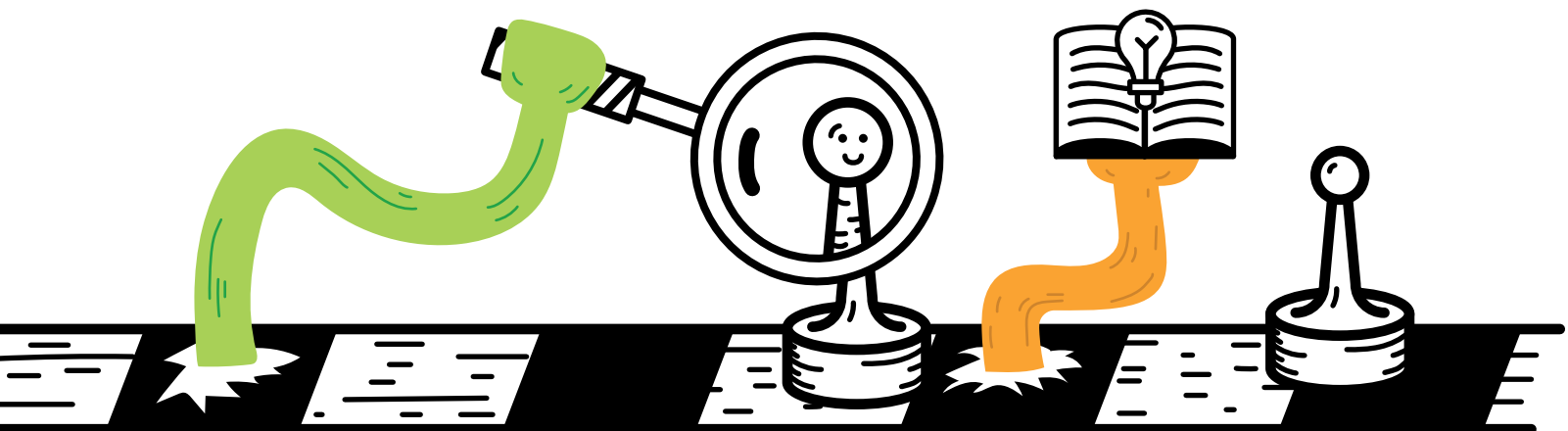
Finally, there's the option of developing your own internal tech pipeline. Employers – both public and private – have drastically reduced what they spend on training since 2000. That needs to change.

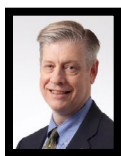
Developing good training programs can open your options. You can bring in new hires who have the potential to learn needed skills once on board, rather than hold out for people already trained. And use vendors' professional services to train employees on specific technologies and applications.

Taking advantage of the Federal Rotational Cyber Workforce Program, under which cyber employees work at other agencies for six months to a year, can help tech staff learn new skills.

You can also think of "rotations" to the private sector as a way to upgrade skills. According to NSF's Gardner, younger tech workers are unlikely to stay with the same employer for their whole career, so they might not stay in a government job for life. But you can entice them to return to government after time in the private sector by promoting a workplace that meets their needs for flexibility and work-life balance.

"Talent that we want is going to learn skills in different places," Gardner said. "We say the best employee is one that can go from one agency to another, and the best employee [now] is one that can go out of government into industry and later come back in."





How to Get Ahead on Vulnerability Management



An interview with Bill Harrod, Chief Technology Officer, Public Sector, Ivanti

At some point, security becomes all about the math.

Every device you connect to the network becomes another potential security vulnerability. And the more vulnerabilities you have, the harder it is to sort out what to tackle and when.

That's always been the case. What's new is how the devices have proliferated over the last several years, in large part because of remote and now hybrid work.

"Think about it: There are, maybe, several hundred thousand potential vulnerabilities on a network," said Bill Harrod at Ivanti, which provides risk-based vulnerability management solutions. "Where do you go first? How do you do the patching to keep up with zero-day attacks and critical security vulnerabilities?"

Map Your Threat Landscape

The first step toward answering that question is to identify those vulnerabilities.

It's not enough to know what devices are on the network. You also need insight into the status of every device: Is it compliant with your security policies? What software does it run, and exactly what components are part of that software? Is that software up to date on its patches? Have security controls been altered? And so on.

The next step is to understand the risk involved. Every misconfigured system, outdated software or missing patch represents a vulnerability. But to what extent is that vulnerability likely to be exploited, and what damage might be done?

That discovery process must be continuous as new devices are connected, the status of existing devices changes (e.g., new patches must be applied or software must be updated) and new threats emerge.

Change the Equation

Back in the days when networks had a relatively stable number of devices, the security team tended to keep tabs on vulnerabilities using a spreadsheet. But with the proliferation of connected devices, "trying to manage it with a spreadsheet is just a losing proposition," Harrod said.

Here are three areas in which automation can change the equation:

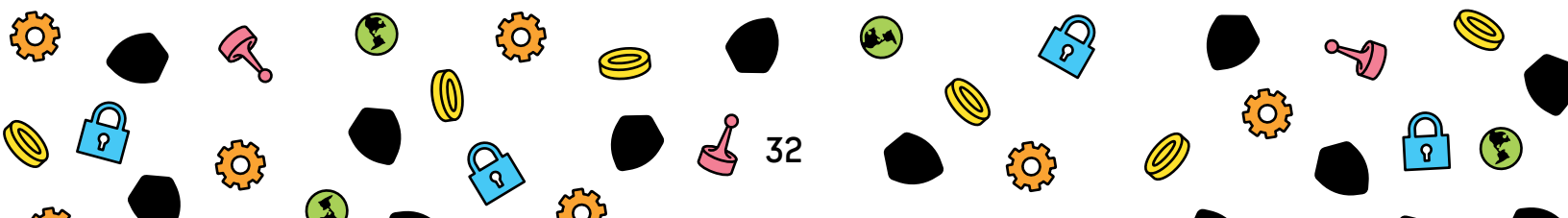
- Identifying and assessing devices and other IT assets in real time, including all hardware and software on premises, in the cloud and at the edge
- Correlating that inventory with threat intelligence and other security data to prioritize remediation efforts
- Testing, deploying and validating patches, and ensuring that patch deployments have minimal impact on your employees and system workloads

Keep the Employee in Mind

If security had one objective – to protect systems and data – you could just lock users out of the network and call it a day. But the real goal, said Harrod, is to "make it as easy as possible for people to do their jobs and be secure at the same time."

In fact, he said, a 2022 survey by Ivanti found that 40% of respondents would consider changing jobs if they couldn't access the tools they need, such as a mobile device.

Ivanti provides risk-based vulnerability management and related tools that enable organizations to provide that user experience without compromising security, Harrod said.



Ensure peace of mind, everywhere your business works.

Our security solutions provide the highest barrier you can get against threats, giving you the power to protect your business—everywhere.

■ Ivanti Discovery

Make your IT, and your user experiences, more efficient and secure with real-time visibility of your assets.

■ Ivanti Unified Endpoint Management

Automate deployments, personalize user workspaces and fix issues quickly, everywhere.

■ Ivanti Zero Trust Access

Deliver secure, streamlined user experiences with zero trust access for any application or device.

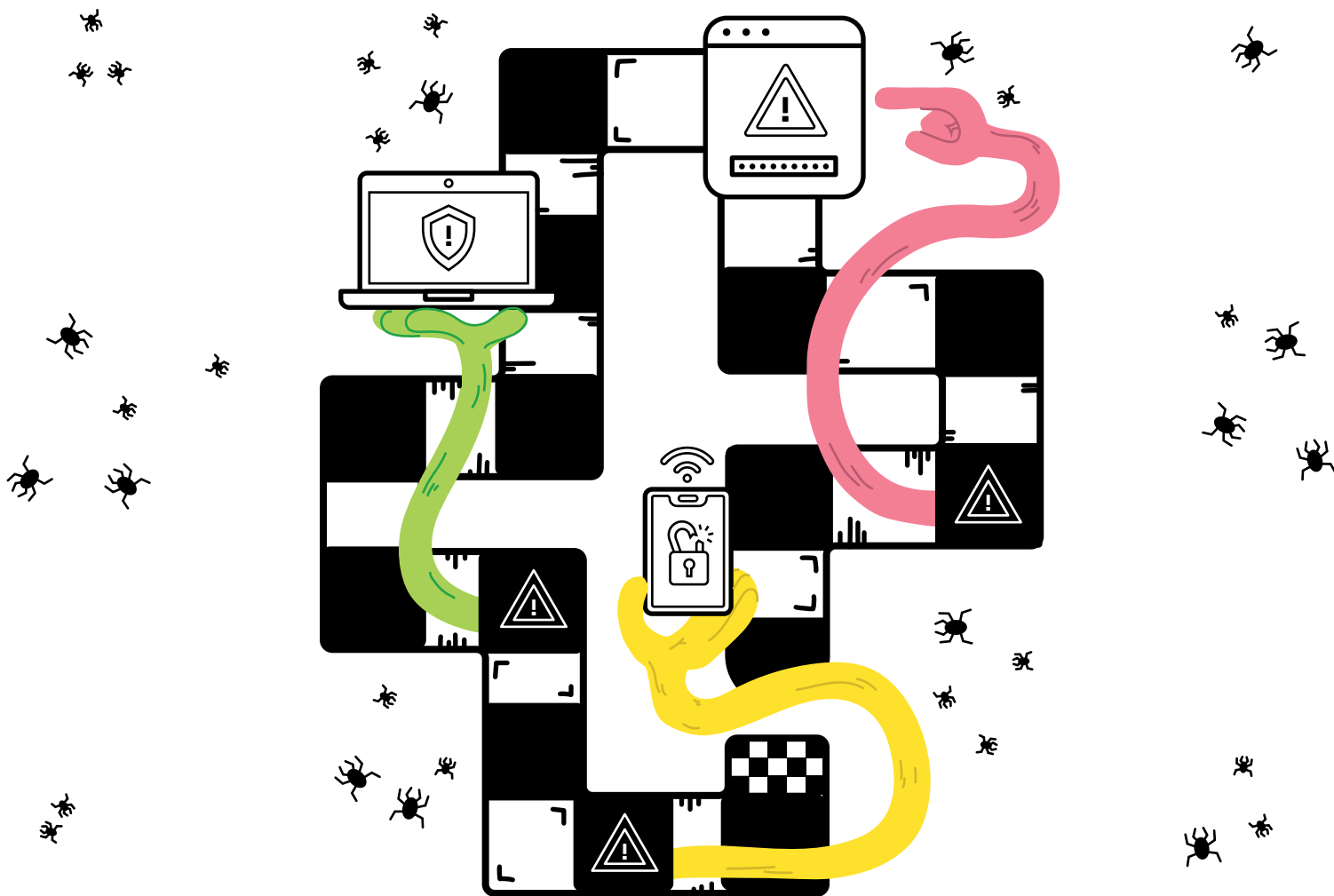
■ Ivanti Risk-Based Vulnerability Management

Move from detection of vulnerabilities and weaknesses to remediation in minutes – not months.

■ Ivanti Patch Management

Efficiently prioritize and remediate the vulnerabilities that pose the most danger to your organization.





How to Adapt to the Cyber Landscape: 6 Takeaways

Here's the bottom line: There's no such thing as an immutable defense. Good security is adaptive security. Here are some key takeaways on how to improve your cyber agility.

Automate. Given both the volume and velocity of tasks, there's no way that cyber experts can keep pace with threats without automation.

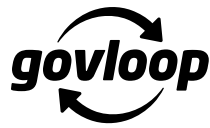
Build the cyber workforce. Build it every which way: Recruit young talent, upskill existing staff and hire seasoned professionals. Whatever it takes.

Keep tabs on CISA. The cyber agency is spearheading the development of advanced cyber strategies and solutions. Follow its lead wherever possible.

Don't go it alone. Collaborate with other agencies or organizations to build cyber intelligence and develop cyber best practices.

Get serious about zero trust. Zero trust has become a bit of a buzz word, but it remains one of the best approaches to securing applications and data.

Secure non-traditional tech. Any device that's hooked up to the internet is at risk. The problem is that many IoT-type devices do not come with security features, leaving your network vulnerable.



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.

Thank You

Thank you to Aqua Security, Fidelis Cybersecurity, Ivanti, Menlo Security, and OpenText Cybersecurity for their support of this valuable resource for public sector professionals.

Authors

John Monroe, Director of Content

Lauren Walker, Senior Staff Writer

Susan Kirby-Smith, Senior Staff Writer

Candace Thorson, Managing Editor

Stephanie Kanowitz, Contributing Writer

Designer

Marc Tom, Junior Graphic Designer