HOW TO BUILD A CYBER-SAVVY WORKFORCE

govloop

carahsoft

Introduction

Recent advances in cybersecurity — such as the adoption of a zero-trust model and the emergence of artificial intelligence (AI) as both a threat and a solution — have only reinforced the importance of the cultural dimension to an agency's overall cyber posture.

That's the focus of this guide, the second of our three-part 2024 series on the cybersecurity landscape. We begin with a look at the key cyber-related events since our first installment in January. Employees need to understand the complexity of the threat landscape — and their role in their agencies' cyber defenses.

Consider zero-trust network architecture. Although zero trust is largely seen as a technological and policy challenge, agencies now realize they need to get buy-in from the workforce, because zero trust will affect how employees do their work. We hear from Steven Hernandez, Chief Information Security Officer (CISO) at the U.S. Department of Education, about how his department involved employees early on in zero-trust pilots.

In the same vein, agencies are stepping up their efforts to improve their employees' overall cyber literacy, providing training that aligns with specific responsibilities. Rodney Petersen, Director of the National Initiative for Cybersecurity Education at the National Institute of Standards and Technology (NIST), discusses this shift.

In our next installment in this series, we will focus on emerging priorities for 2025. But whatever the focus, you can bet that cyber culture will be part of it.

CONTENTS

3 2024: Agencies Adapt to Shifting Threat Landscape

5 Keeping Agencies Up and Running

7 Building Zero Trust Into the Supply Chain

9 How One Agency Wove Zero Trust Into Its Culture

11 How to Improve Security Through Modern Identity Management

13 An Open Source Platform Helps Achieve Zero-Trust Security

15 Building a Culture of Cyber Literacy

17 Securing Your Data: Beyond the Cloud

19 Making Sense of Malware

21 About and Acknowledgments

2024: Agencies Adapt to Shifting Threat Landscape

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

JANUARY

- The Cybersecurity and Information Security Agency (CISA) warns about unpatched vulnerabilities in a widely used virtual private network (VPN) tool.
- A Defense Department (DoD) official says that both the United States and its foreign adversaries were looking to AI to provide a cyber edge.

FEBRUARY

- CISA, the National Security Agency and the FBI report that state-sponsored cyber actors in China have been seeking to "pre-position themselves" to launch attacks against U.S. critical infrastructure.
- Introducing its new Federal Enterprise Operations Cyber Alignment Plan, CISA says it will help advance federal agency collaboration on cybersecurity, both in terms of sharing cyber-incident information and comparing cyber strategies.
- NIST finalizes a major update of its landmark Cybersecurity Framework, with a focus on extending its scope beyond critical infrastructure.

MARCH

- The Biden administration's fiscal 2025 budget request earmarks $13 billion for civilian cyber-related activity, a nearly 10% increase over 2024 spending levels.
- CISA drafts new rules that require critical infrastructure organizations to report cybersecurity incidents and ransomware payments.
- DoD establishes the Office of the Assistant Secretary of Defense for Cyber Policy, which will provide overall supervision of DoD policy for cyber operations.
- The Federal Risk Authorization and Management Program releases a plan for modernizing its approach to authorizing cloud services for government use.

APRIL

- Reports surface that Russian hackers had attacked water systems in several small Texas towns, which U.S. officials later confirm was part of a broader series of attacks in North America and Europe.
- NIST revises its digital identity guidelines to clear the way for agencies to adopt emerging multifactor authentication methods, such as syncable passkeys.
- The Biden administration issues National Security Memorandum 22, which provides CISA with clearer authority to oversee efforts to secure U.S. critical infrastructure.

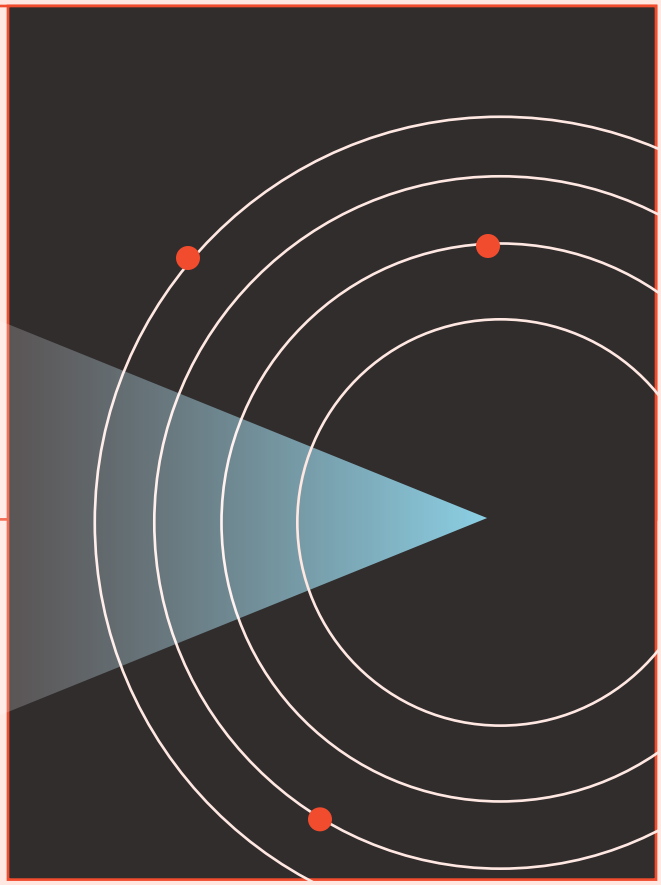
MAY

- U.S. officials detail how hackers sponsored by the North Korean government are taking advantage of flaws in a common email standard to launch phishing attacks.
- The Biden administration releases a new version of its National Cybersecurity Strategy Implementation Plan, detailing 31 new initiatives.

CYBER THREATS ON THE RADAR

Here are the top five trends driving federal cybersecurity efforts, according to the 2024 Report on the Cybersecurity Postures of the United States, released by the Office of the National Cyber Director in May 2024:

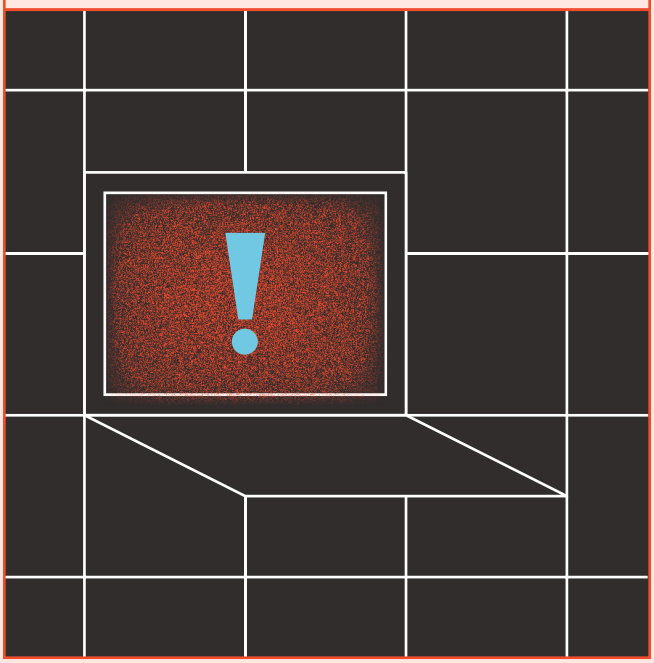
1. Evolving risks to critical infrastructure
2. Ransomware
3. Supply chain exploitation
4. Commercial spyware
5. Artificial intelligence



INFRASTRUCTURE SECTORS AFFECTED BY RANSOMWARE

In 2023, the FBI's Internet Crime Complaint Center (IC3) received **1,193 ransomware reports** from critical infrastructure organizations. Here were the top targets, according to the IC3's year-end report:

- Health Care/Public Health: **249**
- Critical Manufacturing: **218**
- Government Facilities: **156**
- Information Technology: **137**
- Financial Services: **122**
- Commercial Facilities: **87**



GAO: NATIONAL CYBERSECURITY STILL A WORK IN PROGRESS

Implementation of the Biden administration's National Cybersecurity Strategy, issued in 2023, is still incomplete, according to the Government Accountability Office (GAO).

In a February 2024 report, GAO said the federal government has **hit the mark in four areas:**

- Purpose, scope and methodology
- Problem definition and risk assessment
- Integration and implementation
- Organizational roles, responsibilities and coordination

But federal efforts have **fallen short in two others:**

- Goals, subordinate objectives, activities and performance measures
- Resources, investments and risk management

Keeping Agencies Up and Running

An interview with Jared Vichengrad, Head of Public Sector, Check Point



Government organizations have ample motivation to secure their networks, devices and infrastructure: Ransomware targets 58% of public-sector entities each year, and it costs them each more than $2 million, on average, to get up and running again. According to Jared Vichengrad, Head of Public Sector for Check Point, that's largely because agencies struggle with legacy systems.

"Public-sector organizations just can't buy the latest and greatest" technology, he noted. Budget restrictions, procurement obligations and workforce challenges heavily affect their abilities.

EDUCATIONAL IMPERATIVE

But continuous learning can help alleviate employee training gaps that pose cybersecurity risks. Vichengrad stressed the need for ongoing educational opportunities, including tabletop exercises, workshops, certifications and accreditations, conversations with industry experts, and training programs, such as those that Check Point offers.

Agencies also must think about the next generation of public-sector employees, he said. As cyberattacks take place with more frequency and intensity — and technology evolves almost daily, it seems — organizations must ensure that the next wave of government workers knows what it needs to do. One approach, Vichengrad said, is through Secure Academy, in which Check Point partners with higher learning institutions to provide comprehensive security education.

AI INNOVATIONS

It's nearly impossible to leave artificial intelligence (AI) out of an IT-related conversation, and with good reason. "We've seen AI adoption grow faster than any other technology out there," observed Vichengrad, "and AI is only going to become much more relevant in public-sector organizations."

Among other innovations, AI tools are transforming the cybersecurity world. For instance, Check Point's ThreatCloud AI scours the globe for cyber threats, and the company's Infinity AI Copilot relies on generative AI to provide real-time guidance and analysis during a security breach, so that agency staff can correct the problem.

"Our AI Copilot can assist security analysts by automatically correlating the data, suggesting remedies … and then predicting future threats based on … deep learning," said Vichengrad. The products leverage the capabilities of 50-plus machine learning engines, he added, and are included in Check Point's larger Infinity Platform, which unifies all security and management tools under a single dashboard.

BEST PRACTICES

At a basic level, agencies need a consolidated, enterprisewide approach to securing all their networks, Vichengrad said. "The cloud, mobile [devices], endpoints, the Internet of Things — it's not just one thing anymore," he explained. "We really have to look at optimizing the full environment to prevent any threats … and really consolidate the security architecture to reduce any management challenges, as well as reduce costs."

Additionally, Vichengrad believed agencies should pursue public/private partnerships because although private entities such as Check Point don't perform daily organizational tasks, "we really know the challenges and pain points that [agencies] are dealing with, and we're there to help."

"We're all customers of the state that we live in, the city, the federal government [and] the schools, and are really [about] making sure that [those entities] have the expertise and resources to keep running," he said.

CHECK POINT™
PUBLIC SECTOR

Driving the future of cyber security

Check Point's Infinity Platform adopts AI to predict and prevent threats to your organization



AI - Powered.
Cloud- Delivered.

checkpoint.com/infinity

Building Zero Trust Into the Supply Chain

An interview with Josh Bressers, Vice President of Security, Anchore



Zero-trust strategies involve more than just verifying user identities and controlling access. Successful zero trust also means securing applications across the agency.

"The intent of zero trust is [that] you have two things that are each trusted, communicating over an untrusted channel," explained Josh Bressers of Anchore, whose software composition analysis platform helps secure public-sector applications and automate compliance with government security standards. "But if you have an untrusted channel, one trusted device and one untrusted device, there's no trust."

ENTER THE SBOM

After some dramatic supply-chain breaches in which hackers exploited vulnerabilities in commonly used software to attack all users of those applications, the government has emphasized the SBOM — software bill of materials.

The intent of the SBOM is to uncover all the pieces of software used in the modern DevSecOps environment, Bressers said. "There are cases where [the vendor] may not even know what's in their application." Without this insight, there is no trust.

The software in our environments is dynamic. "As soon as you start running it, your people [start] making changes to it. Has the software changed itself? There's software that downloads data off the internet and starts running it," he cautioned.

Keeping track of what's actually running on your system "is surprisingly more difficult than we wish it were," Bressers said.

Anchore also works with federal software factories including DoD's Platform One and the Navy's Black Pearl to verify an application's compliance with regulations and standards.

These software factories represent foundations for modern DevSecOps. Focusing on SBOMs, vulnerability detection and policy enforcement means the developer can remediate findings before the Authority to Operate stage, speeding up the process.

SPEEDING UP REACTION TIME

"Another piece of the security puzzle is that there's an enormous amount of information [about vulnerabilities] that we're subjected to constantly. It can be hard to figure out which of these things actually matter," said Bressers.

For example, the Cybersecurity & Infrastructure Security Agency (CISA) maintains a Known Exploited Vulnerabilities Catalog — KEV. "Vulnerabilities on the KEV list should be treated as the most serious vulnerabilities in your infrastructure." Without automation, there's no way we can understand what software is in use, and what vulnerabilities affect it.

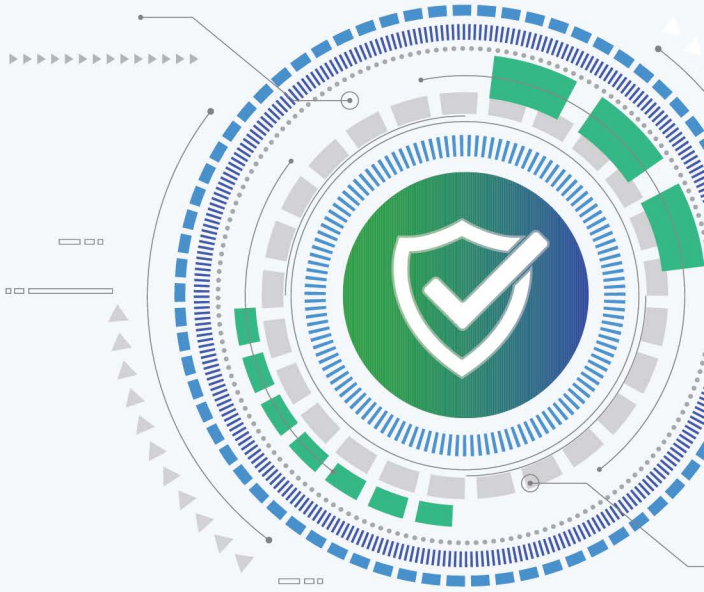
"The first step, the only step and the thing we haven't done yet is understanding what we have," Bressers said. "Having the ability to create an SBOM for our environments is the foundation of a modern DevSecOps program."

A platform such as Anchore Enterprise helps by generating an SBOM of an agency's whole system that's searchable and scannable, Bressers said.

The Log4j exploit, discovered in 2021, compromised countless public- and private-sector systems. Defending against the attack required knowing where the Log4j utility was used. According to Bressers, an Anchore customer was able to identify all its uses of that code in about six minutes. "A lot of other organizations were spending months just figuring out where it was," he said.

anchore

Anchore secures your software supply chain with confidence.



Software Composition Analysis for containerized applications

Generate and manage SBOMs

Detect and fix vulnerabilities

Automated government and industry compliance

Remediation and reporting

Trusted By

U.S. Customs and Border Protection

America's Navy

U.S. Department of Defense

U.S. Air Force

U.S. Army

Ministry of Defence

Australian Government Defence

Learn more: **www.anchore.com**



How One Agency Wove Zero Trust Into Its Culture

*An interview with **Steven Hernandez**, CISO and Director of Information Assurance Services, Department of Education*



The U.S. Department of Education has plenty of incentive to instill a zero-trust philosophy across its enterprise, even without needing to comply with the White House's Executive Order on Improving the Nation's Cybersecurity or the ensuing federal strategy for implementing zero-trust architectures. Because of the nature of the department's work with students and their families, the agency holds personally identifiable information (PII) and other sensitive data on about 28% of the population.

"When we looked at zero trust, a big selling point was that we're protecting about a third of this nation's PII and financial information," said Steven Hernandez, the department's Chief Information Security Officer and Director of Information Assurance Services. His office mapped its zero-trust implementation plans using the Cybersecurity and Infrastructure Security Agency's Zero Trust Maturity Model, and set about raising awareness and educating users departmentwide.

Many agencies have some of the foundational capabilities of zero trust in place already, such as Identity, Credential and Access Management (ICAM). "What zero trust calls us to do is take all of these capabilities to the next level. That's not a technological solution," said Hernandez. "Zero trust is a cultural journey as much as a technological one."

At the department, the change began with buy-in from high-level officials who convinced deputy secretaries and other senior leaders that they had a vested interest in zero trust's success. "There were lots of briefings, one-on-ones, phone calls and personal conversations," Hernandez said. "Leadership buy-in is a foundational pillar."

OPEN COMMUNICATION IS KEY

In taking the program enterprisewide, Hernandez and his team held regular cyber risk briefings and provided notice that training sessions or system tests were coming. They also wove zero trust into the standard user-awareness training that all department staff receive.

Opening lines of communication was the secret sauce that made the education program work. "We decided that we're going to communicate until people tell us it's too much," Hernandez said. "And they never did."

For example, his office issued an early call about new pilot programs and recruited volunteers to test them. Word spread from the volunteers to their colleagues, who also became interested in zero trust's advantages and offered to participate. "We originally planned for 50 to 60 people to take part in the pilots and wound up with hundreds," Hernandez said. "And we got great feedback from the training."

> ***"We decided that we're going to communicate until people tell us it's too much.***
>
> ***And they never did."***
>
> *– Steven Hernandez*

MAKING YOUR CASE

Selling employees on zero trust's advantages takes some marketing, he noted. For instance, Secure Access Service Edge (SASE) technology, one of the technological pillars of zero trust — along with Security Orchestration, Automation and Response and enterprisewide ICAM — replaced VPNs by performing the same type of tasks, but far better.

So, rather than downplaying the change, Hernandez's team emphasized what SASE did differently, providing encrypted tunnels via the internet and carrying out zero trust at the endpoint instead of within the network. "This is a game-changer," he said. "We don't trust the network — that's one of the core tenets of zero trust."

The department also emphasized other advantages of the switch to SASE, such as reduced downtime and other interruptions, and increased efficiency. "What used to take weeks or days now takes us hours or minutes," Hernandez said.

In addition, it was important to recognize staff who contributed to the transition. When Hernandez briefed the department secretary on the progress with zero trust, he made sure to call out program-level leaders, including people outside the security teams. "When we build champions, they become champions for us," he explained.

How to Improve Security Through Modern Identity Management

Insights from Bryan Rosensteel, U.S. Federal Chief Technology Officer, Ping Identity



To be efficient and effective, government agencies need interoperable systems that securely connect employees, constituents and partners to the resources they need across the enterprise. But many agencies rely on a patchwork of legacy Identity Credential and Access Management (ICAM) systems, and that creates security gaps and provides an uneven user experience.

Those individual ICAM systems might work well with some applications, but they lack the interoperability needed to support key capabilities such as federated single sign-on and zero-trust network access, said Bryan Rosensteel, Ping Identity's U.S. Federal Chief Technology Officer. The company's solutions make digital experiences secure and seamless for all users.

With a modern system, agencies can overcome legacy approaches' limitations and gain greater flexibility and more granular controls around identity management.

Here are three concepts that are key to modern identity management.

FEDERATED IDENTITY MANAGEMENT

To ensure seamless access to their ever-expanding landscape of applications, agencies need a unified approach to identity management. Federated identity management (FIM) enables diverse users to access networks, applications and resources using a single set of credentials. In FIM, a third-party identity provider stores user credentials and authenticates users across organizations.

This approach "will greatly reduce what that user needs to remember," Rosensteel said. It will also provide IT teams with greater visibility into network activity: With authentication-logging in one place, "they can better understand what's going on," he added.

POLICY-BASED ACCESS CONTROLS

Agencies are looking to technology to seamlessly implement access policy, especially as they roll out zero-trust security. To do that, they need identity management to be rooted into centralized policy engines.

Policy-based access control helps here. It uses policies to determine user access privileges, putting additional criteria on top of user role and associated permissions, providing finer-grained control. This makes it possible to shift from role-based access control to attribute-based access control.

Role-based controls consider who you are and what you do at the organization, while attribute-based controls may add, for example, "the context of how you're coming in," Rosensteel said. That becomes especially important given the rise of mobile devices and remote connectivity. And attribute-based solutions may also consider user-behavior analytics. "We can start plugging those into our authentication and authorization engines," he said.

CENTRALIZED POLICY MANAGEMENT

In a heterogenous IT landscape, agencies need a way to create and implement policy across all their applications, APIs and data. To that end, they can move away from application-specific authorizations and instead adopt centralized policy management.

In a modern identity management system, "federation allows me to have centralized authentication and to abstract that away from the application," Rosensteel said. This ensures both enhanced security and the ability to meet regulatory requirements efficiently.

Many in government recognize the need to modernize ICAM. With a platform that empowers organizations to easily orchestrate secure identity experiences, "Ping Identity can help accelerate that adoption," Rosensteel said.

PingIdentity®

“IDENTITY is Mission-Critical & Ping Identity Has You COVERED”

- FedRAMP High, DOD IL5, Air-gapped, and Hybrid solutions available
- Adaptive Authentication and Dynamic Authorization for ABAC enablement
- Phishing-resistant MFA, SSO, and Access Management anywhere in your environment

pingidentity.com | @pingidentity

An Open Source Platform Helps Achieve Zero-Trust Security

An interview with Jeremy Wilson, CTO – North America Public Sector, EDB



To meet mission needs, federal agencies must interact with databases containing everything from personal records to geographical information to law enforcement data. It's imperative that these databases comply with the White House zero-trust security mandate. Yet implementing zero trust in legacy database management systems has proven to be problematic.

"A zero-trust model includes supporting tools such as identity and access management, data loss protection, analytics, network security, etc.," said Jeremy Wilson, EDB's CTO – North America Public Sector. "Legacy databases often can't interoperate and integrate with these technologies."

To comply with zero-trust requirements, federal agencies should look to modernize, Wilson said. A commercial open source database management system empowers them to bring to bear the tools of zero trust across their mission-critical data estate.

"A modernized platform will include open interfaces that allow for integration with these zero-trust technologies," Wilson said. Such a solution "will be able to accommodate a wide range of technologies and standards in order to meet the zero-trust requirements."

OPEN SOURCE BENEFITS

An open source approach here comes with certain inherent security benefits.

When agencies leverage Postgres, a powerful open source database management system, "one of the advantages from a security perspective is transparency. Since a 'worldwide community' is working together, inspecting the source code 24x7x365, there are typically fewer bugs, and what is discovered is remediated quickly," Wilson said.

A commercial open source solution will take this even further, deploying additional security tools to automate the inspection and discovery of vulnerabilities, so they can be remediated immediately.

"EDB commercializes open source Postgres and builds an enterprise model around it to further enhance security for regulatory compliance," he said.

SPECIAL ATTENTION TO SECURITY

In fact, security is a top focus for EDB, whose products are developed specifically to support national security requirements and other highly regulated areas of government.

"Compliance and security are very stringent in these areas, and so we adhere to specific security standards," Wilson said. Some of those include the Federal Information Processing Standard (FIPS) for encryption, and Security Technical Implementation Guides (STIGs), which hardens the database.

The enterprise model incorporates role-based access control, which supports zero trust by limiting what users can see and do within the database. "We've incorporated all of these security measures that meet the government standards, and they are built into the enterprise model," Wilson said.

The U.S. Army, for example, benefits from EDB's decades of PostgreSQL experience supporting a wide range of missions, including modeling and simulation, satellite communications, research initiatives, and biometric identification. The service has relied on EDB for its robust enterprise database functionality and as an alternative to costly legacy vendors, Wilson said. From a security standpoint, they use EDB Postgres Advanced Server, which provides enhanced security features such as FIPS encryption and DISA STIGs.

With a modern, open source database management system, federal agencies can meet mission needs, while ensuring zero-trust security across this key piece of IT infrastructure.


EDB
Postgres® for the AI Generation
Learn how EDB empowers government organizations with their Zero Trust journey
enterprisedb.com

Building a Culture of Cyber Literacy

*An interview with **Rodney Petersen**, Director of the National Initiative for Cybersecurity Education, NIST*



Improving their employees' cybersecurity awareness has been a longtime focus of government agencies. The changing cyber threat landscape, with attacks becoming ever-more frequent and sophisticated, has put a finer point on what employees need to know. The goal now is not just cyber awareness, but cyber literacy — the ability to function safely in online environments with a clear understanding of what constitutes safe behavior.

For agencies, that means regularly connecting with employees to provide education and training that align with their jobs and to update them on new threats and attack techniques. In addition, agencies can sharpen the focus of mandatory annual cyber awareness training to form a foundation for cyber literacy.

"The annual training, at least as it's being done by our agency, is very effective [for] not only sharing tips, information and resources, but assessing that the employees actually understand the content and can apply it in the right way," said Rodney Petersen, Director of the National Initiative for Cybersecurity Education (NICE) at NIST. But achieving cyber literacy among the workforce requires agencies to exceed that baseline.

CYBER LITERACY:

The ability to function safely in online environments with a clear understanding of what constitutes safe behavior.

Train Regularly

"Annual training is not enough," Petersen said. "It has to be reinforced throughout the year."

NICE, which originated in 2008, focuses on helping government agencies, the private sector and academia build their cybersecurity workforces from within. Part of its initial focus was preparing federal workers to handle cybersecurity challenges, and it now coordinates with cyber education programs such as those that CISA and the Federal Information Security Educators run.

Another role NICE plays is promoting an integrated ecosystem of cybersecurity education. In the current threat climate, that means bringing about a cultural change in which cyber literacy is interlaced with daily aspects of work.

Foundations of Cyber Literacy

"The main message is that **cybersecurity is everyone's job**," Petersen said. "It's not just the job of the CIO, CISO or the people doing technical work, but it's everyone across the enterprise."

There are three general levels of cybersecurity education: training for all, for the many, and for the few. The first level applies to all users, including the general public, and the third area is NICE's focus — that is, people who will make cybersecurity their career.

Cyber literacy falls into the second category — and applies to all agency employees, including "people who have specialized access to data and systems and may need specialized training to administer systems securely," Petersen said.

To be cyber literate, employees need regular updates and education plus annual and job-specific training. For instance, security teams can issue alerts about new phishing campaigns or other attacks to keep employees apprised of current threats. "We look at phishing especially because some of the messages can be really targeted," he said.

Where to Start

In developing cyber literacy programs, agencies can draw from many resources. NIST's Special Publication 800-50, released in final form in October 2023, spells out the steps for designing, developing and implementing an awareness program.

CISA outlines the four basics of online safety — **recognizing and reporting phishing**; using **strong passwords**; using **multifactor authentication** on any site an agency offers, whenever possible; and **updating software** promptly, even automatically. The National Cybersecurity Alliance expands on that with other advice, such as using secure Wi-Fi and ways to recognize suspicious links.

NICE also coordinates with the National Cyber Workforce and Education Strategy, which promotes foundational cyber skills for all employees, in addition to supporting the pursuit of careers.

Ultimately, Petersen said, developing cyber literacy depends on making it part of an agency's culture through persistent, consistent messaging.

Securing Your Data: Beyond the Cloud

An interview with Jeff Reichard, Vice President, Solutions Strategy, Veeam



Agencies often transition to the cloud to close security gaps, but the cloud itself poses unique risks. In fact, in the last five years, some of the largest cybersecurity breaches were tied to cloud permission issues that allowed anyone to access protected data.

"There's been a tendency to mistake the operational resiliency and uptime capabilities of cloud environments, the ability to fail services over from one region to another ..., for data protection," said Jeff Reichard, with Veeam, which provides software solutions that strengthen data resiliency. But the cloud offers protection against downtime, not data deletion.

"The shared responsibility model for all kinds of cloud services ... leave[s] the mandate for data backup and regulatory compliance in the hands of the data owner," he said. "It's not the cloud service [provider], it's you."

DANGER IN THE CLOUD

Organizations that suffered ransomware attacks in 2023 lost considerably more data in the cloud than in data centers or home offices, according to Veeam survey results. Two case studies offer profound examples of what can go wrong, Reichard said.

Earlier this year, an Australian pension fund managing the investments of 600,000 educators — with $125 billion of assets under management — lost all its cloud-stored data due to an administrative error. The mistake deleted the fund's entire tenant account, which also deleted the fund's cloud data at remote sites, said Reichard.

The fund might have been forced to "cobble together from multiple disparate data sources what people had in their life savings and their retirement accounts," he explained. "And the reason they're not in that position — the sole reason — is because they had a backup out of the cloud."

In the U.S., a large city began repatriating data from the cloud to on-premises systems, Reichard added, and ultimately lost data affecting 17,000 criminal cases. The city wasn't as fortunate as the retirement fund: It lost everything. "It turned out," he said, "they thought they had a backup of the data they were repatriating, and they didn't."

BACKUP THE RIGHT WAY

So what is the answer? First, identify the highest-impact data you have and steadily back it up, Reichard advised. Second, make sure you have immutable backups of your data, wherever it lives. In other words, if an adversary breaches your environment and compromises all your administrator credentials, do you have data copies that will survive?

Veeam solutions, which are deployed on U.S. Navy ships, offer what Reichard calls "radical resilience." That falls into three categories: data security, delivering multiple layers of protection; data recovery, providing multiple ways to restore data whenever and wherever you need it; and data freedom, so you're not tied to specific platforms or file formats, he explained.

"In the old days, we knew [not to] keep all of our backup data and replicated data in the same data center because then you're vulnerable to a power outage or flood or tornado," Reichard said. "It is the same with cloud resources."

Ransomware Trends 2024:

US Federal Government Executive Summary

Read Now



Making Sense of Malware

An interview with Dr. Arun Lakhotia, Chief Technology Officer, UnknownCyber



Cybercrime is today an organized industry. It has individuals and businesses specializing in different stages of cyber-attack. There are scouts that identify lucrative targets, programmers to develop malware, infrastructure providers to deliver malware at scale, call centers with social engineering specialists to extort ransom, and ecommerce sites to connect various buyers and sellers of various goods and services.

At the center of most cyberattacks is malware, a piece of software. Thanks to GenAI bad actors can create and obfuscate malware at scale. Thus, today's malware threat is so significant largely because the hacking industry is organized and is using automation.

"You have more players in the game [and] more industrialization of the attack," explained Arun Lakhotia with UnknownCyber, which helps agencies detect and respond to computer viruses and malware that they otherwise would overlook for days or months.

SO MUCH TO SCREEN

Antivirus and sandbox technologies have not kept pace with the sheer number of machine-generated code obfuscations, said Lakhotia, who also is a computer science professor at the University of Louisiana at Lafayette. Thus, obfuscated malware is detected by endpoint detection and response systems weeks and months after it has bypassed antivirus defenses and infected its targets.

You can think of antivirus software like Transportation Security Administration (TSA) screenings at the airport, he said. "Loads of people are coming through, and [TSA] needs to check and say, 'Hey, is this good, is this bad' all day long.... And they can't hold up everyone. They must [decide] quickly." Much as if TSA slows down it can bring an airport to a crawl, so also any sluggishness of the antivirus can make a computer useless.

Thus, if a program looks suspicious the current technologies issue an alert — like a TSA machine beeping when a suitcase needs extra attention — so that a human can investigate. But that shifts the work to people, he said, and alert fatigue becomes a problem.

MALWARE GENETICS

What's called semantic malware analysis — UnknownCyber's specialty — is more effective and less burdensome, said Lakhotia. Rather than look at superficial patterns, which hackers can easily manipulate, a semantic approach analyzes the instructions in the code that make it do what it does. In effect it is like looking at the genetic make up of a person instead of their fingerprint or facial profile.

That allows UnknownCyber to recognize machine generated variations of malware. "We are like 23andMe for malware," said Lakhotia, "We identify not just one malware but all its progeny as well." Thus, using UnknownCyber an agency can extract genome of the adversaries targeting them to defend even against malware that has not yet been written.

Malware may seem like an insurmountable challenge, said Lakhotia, but "we tamed the problem ... to a point where you can manage it with modest resources [and] without significant training."

govloop UNKNOWN CYBER

Incident Response

UNKNOWN CYBER LAB FORWARD

UNKNOWNCYBER RESPONSE

PROACTIVE CAPABILITY FORWARD



Capability:
Cyber protection teams at incidents need a portable capability to do rapid reverse engineering and forensic analysis to identify and attribute otherwise unknown threats through code. This rapid analysis also returns hunting and protection signatures in minutes. Increased capability at point of incident allows teams a time and information advantage to find, fix, and finish the adversary earlier. UnknownCyber's deployable instance places this capability forward so OCO and DCO teams can act faster by upskilling their team through automation. This saves time and provides the victim network owner the situational understanding and tools necessary to take-action, with custom countermeasures immediately available to pivot to a proactive defense. Benefits include earlier updates of running estimates, earlier cueing of intelligence assets, and actionable information from which to build the intelligence picture.

Automation:
From Unpacking to Attribution UnknownCyber provides deep code analysis capabilities automatically at incident without waiting for a lab to complete a manual investigation. Gain an asymmetric advantage, shorten investigations, and shift malware development costs to the adversary by defeating reused code.

About our tech:
UnknownCyber is an In-Q-Tel Portfolio Company. Our core technology was developed during DARPA's Cyber Genome Project and is available to be contracted through SEWP. Our many unique innovations automate the capability to analyze the evolution of code and identify novel variants of malware rapidly at scale. Our capability has been independently validated by MIT's Lincoln Labs and a Fortune 500 SOC which demonstrated UnknownCyber's ability to detect new threats before any other global threat intelligence.

KEY BENEFITS

- Find unknown malware before the rest of the world
- Attribute from Code: Type/ Family/ APT
- Automatically generate bytecode based YARA to Hunt and Harden
- Harden with matched IoCs
- Triage Risk on match score
- Associate past attacks to identify campaigns and evolution of polymorphic variants
- OCO tool comparison

Learn more at: www.unknowncyber.com Contact: info@unknowncyber.com

ABOUT CARAHSOFT

Carahsoft Technology Corp. is The Trusted Government IT Solutions Provider®. As a top-performing GSA Schedule and SEWP contract holder, Carahsoft serves as the master government aggregator for many of its bestof-breed technology vendors, supporting an extensive ecosystem of manufacturers, value-added resellers, system integrators and consulting partners committed to helping government agencies select and implement the best solution at the best possible value.

Visit www.carahsoft.com, follow @Carahsoft, or email sales@carahsoft.com for more information.

Click here to pre-register for the third installment of our 2024 cyber guide series.

Read our first installment — regarding the cyber threats and mandates of greatest concern to your agency — by clicking here.

govloop carahsoft

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 Anchore, Carahsoft, Check Point, EDB, Ping Identity, UnknownCyber and Veeam for their support of this valuable resource for public-sector professionals.

CONTENT TEAM

Candace Thorson, Managing Editor

John Monroe, Director of Content

Lauren Walker, Senior Staff Writer

Susan Kirby-Smith, Senior Staff Writer

DESIGNERS

Kaitlyn Baker, Senior Creative Manager

Kelly Boyer, Motion Design Team Lead