
THE 2024
CYBER
AGENDA
govloop

Introduction

When it comes to cybersecurity, agencies at all levels face unprecedented challenges. The problem is two-fold: Malicious actors have become more adept at exploiting weaknesses, and the IT environment has become increasingly complex, making it harder to secure applications, data and services.

This guide is the first of our three-part 2024 series on the current cybersecurity landscape. We look at key cyber events and initiatives in 2023 that brought us to today's state of affairs, from high-profile cyber breaches to publication of federal standards that will guide public and private security efforts for years to come.

We explore issues of increasing importance, including supply chain security and the profound threat that quantum computing poses to encryption algorithms. A leader of the National Institute of Standards and Technology highlights key concerns and explains how her organization will help agencies turn policy guidance into daily practice. And we hear from industry partners who both understand agency challenges and are knee-deep trying to address them.

There are no guarantees that even the best protections will prevent a cyber intrusion, but there are ways to make attacks less likely. In this guide, we identify what they are.

CONTENTS

3 **2023 Timeline:** A Year of Guidelines, Hacks and New Visions

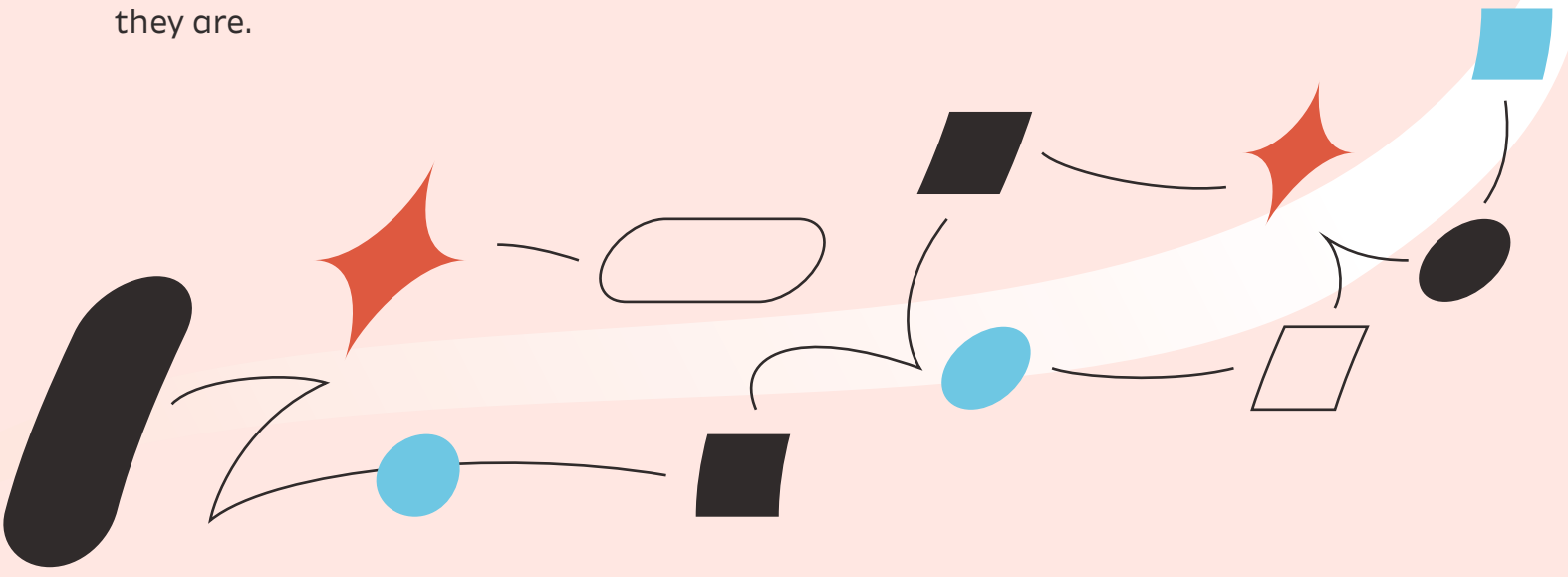
5 Protecting a Moving Target: Why Network Visibility Is the Foundation to a Strong Cyber Defense

6 **The 2024 Cybersecurity Agenda:** Urgency Drives Innovation

9 Simplifying Data Storage and Protection

10 **Government Interview:** Turning Cyber Policy Into Practice

12 Data Protection Builds Cyber Resiliency



2023 A Year of Guidelines, Hacks and New Visions

The release of the National Cybersecurity Strategy in March was just one of several efforts to put government agencies on better cyber footing. But the year also featured numerous incidents that reminded everyone why things need to change. Here is a sampling of the big headlines.

JANUARY

The Justice Department reveals that the FBI covertly infiltrated the Hive ransomware group in a monthslong effort to thwart $130 million in ransom demands by providing victims with encryption keys.

FEBRUARY

The U.S. Marshals Service suffers a security attack targeting sensitive information maintained by an agency that tracks fugitives.

82% of public-sector applications feature a security flaw, compared to 74% of private-sector apps.

MARCH

The Defense Department publishes a strategy for departmentwide cyber workforce management, including the use of standardized workforce analysis tools and processes.

The White House releases the National Cybersecurity Strategy, laying out a plan to create a "safe and secure digital ecosystem for all Americans."

APRIL

The Cybersecurity and Infrastructure Security Agency (CISA), in partnership with multiple U.S. and international organizations, publishes new guidelines for developing systems with security functions built in from the beginning, i.e., secure-by-design/secure-by-default.

The National Institute of Standards and Technology previews forthcoming guidance on post-quantum cryptography, that is, encryption methods that emerging quantum computers can't crack.

MAY

City employees sue Oakland, Calif., seeking damages after a data breach exposed personal information.

Cybersecurity has held a spot on the Government Accountability Office's "high risk" list for ***26 years.***

JUNE

Several federal and state agencies are among hundreds of organizations targeted by Russian hackers who exploited a flaw in a common application used to transfer data.

The gap between the number of cyber workers needed and the number available ***increased by 12.6%*** from 2022–2023

JULY

The White House publishes the National Cybersecurity Strategy Implementation Plan, identifying more than 65 "high-impact" federal initiatives aimed at making progress on goals detailed in the March strategy.

AUGUST

The Defense Advanced Research Projects Agency launches the Artificial Intelligence Cyber Challenge, a two-year competition that offers nearly $20 million in prize money to spur the development of AI-based tools that improve the security of critical infrastructure.

NIST releases a draft of the Cybersecurity Framework 2.0, expanding its scope beyond critical infrastructure and offering and adding cybersecurity guidance.

SEPTEMBER

CISA announces a new program through which it will provide local water utilities with free vulnerability scanning of internet-accessible systems.

In 2023, federal funding for the State and Local Cybersecurity Grant Program increased from ***$185M to $374.9M***

OCTOBER

CISA, the National Security Agency and industry partners provides developers and vendors with guidance on strengthening multifactor and single sign-on solutions, noting that "a significant portion of breaches" involve misused or stolen digital identities.

NOVEMBER

A new program from the Office of Personnel Management enables cyber employees to serve temporary assignments at other agencies, providing them with new learning opportunities that also will benefit their home agency.

DECEMBER

A Pennsylvania town reports that an Iranian cyber group hacked into one of its control stations and shut down a system that monitors water pressure data, while emphasizing the attack posed no risk to the water supply.

Harry Coker, Jr. is confirmed as the National Cyber Director, filling a post left vacant for most of the year.

Protecting a Moving Target: Why Network Visibility Is the Foundation to a Strong Cyber Defense

An interview with Jean Schaffer, Federal Chief Technology Officer, Corelight



Over the years, federal networks have become more complex. Cloud technology has replaced in-house infrastructure. Employees conduct work on their personal computers. And, thanks to the Internet of Things, a proliferation of "smart" devices connect to agency systems.

Agencies largely know about the equipment they manage, but the unmanaged devices are much harder to see and secure, said Jean Schaffer with Corelight, a network detection and response (NDR) platform that provides complete network visibility across hybrid and multi-cloud environments.

"Visibility really is about understanding anything and everything that's touching your networks, including your workflows in the cloud, so you can get your arms around what needs to be protected," Schaffer said. A comprehensive, dynamic view — not a snapshot in time — is necessary to identify your high-value assets, the "crown jewels you really want to protect," she explained.

A CORE NEED

In August 2021, the Office of Management and Budget released Memorandum 21-31, establishing federal requirements designed to increase government's network visibility before, during and after a cybersecurity event. "The memo requires agencies to understand what is happening down at their network and endpoint layers and to maintain a record of that information in a way that can contribute to their overall security defense," Schaffer said.

Corelight helps organizations comply, passively monitoring all their network traffic and creating logs that memorialize the behavior and detect both known and behavior-related threats (e.g., anomalous logins). "What Corelight does really well," she said, "is stitch together [an agency's] logs so it's easy for defenders to understand the context of what's happening and get that true picture quickly."

The platform is a foundational tool that helps agencies build effective cybersecurity programs, Schaffer added.

TRUE STORY

Corelight data makes a real-world difference. The 2020 Solar Winds SUNBURST attack, which affected more than 40 federal agencies and thousands of other entities worldwide, is a prime example. FireEye's threat research team discovered the supply chain attack using Zeek, Corelight's core technology, to detect the novel threat in Solar Winds' environment.

"Without those detailed logs, they said they couldn't have identified [the attack] as quickly ... or how the attacker entered the supply chain," she said.

OPTIONS

Corelight fills network visibility gaps left by endpoint detection and response (EDR) and security information and event management (SIEM) solutions. Sensors can be installed anywhere Linux can, whether as a physical appliance, software or virtual appliances available for several cloud platforms, such as Amazon Web Services, Azure, GCP, VMware, and Hyper-V. Corelight can also be installed on customer-managed Linux to take advantage of existing agency-owned hardware, regardless of vendor.

Government and its industry partners are "doing this dance with our adversaries every day," in which malicious actors pose new threats that agencies and industry try to detect and remediate, Schaffer said. Knowing about everything traversing your network is the foundation of a strong cyber defense.

corelight
FEDERAL, LLC

The 2024 Cyber Agenda: Urgency Drives Innovation

In the past three years, the federal government has increased its efforts to advance cybersecurity technology and strategy. The Biden administration laid out its agenda in the May 2021 Executive Order on Improving the Nation's Cybersecurity (EO), then offered a more sweeping vision in the March 2023 National Cybersecurity Strategy.

Although cyber innovations will come largely from industry and academia, the federal government is attempting to bolster those efforts by offering technical guidance best practices, spearheading public/private collaboration and, in some cases, making financial investments.

Here are some of the key issues on the current cyber agenda.



Strengthen Software **Supply Chain Security**

WHAT'S AT STAKE

Whether developed in-house or procured from the commercial market, every major application includes countless open source and commercial software components. The problem is that agencies often can't identify all those components or their source, i.e., the software supply chain. Subsequently, an application might contain numerous vulnerabilities that might not be discovered until it's too late. For example, in 2021, malicious actors exploited a vulnerability in Log4j, a popular open source component, to infiltrate systems across the public and private sectors.

WHAT'S BEING DONE

The Biden administration has made software supply chain security a pillar of its efforts to improve cybersecurity nationwide and in the federal government. These are some current initiatives:

- As part of its May 2021 EO the administration is pushing for widespread adoption of **software bills of material** (SBOMs), which detail the software components of applications.
- CISA, which has taken the lead on advancing the use of SBOMs, has published numerous resources, including the **Software Bill of Materials (SBOM) Sharing Lifecycle Report** and **Securing the Software Supply Chain: Recommended Practices Guide for Customers**.
- The General Services Administration plans to develop a contract through which agencies can **buy supply chain risk management tools and services**.

Reverse the Gains of **Ransomware Gangs**

WHAT'S AT STAKE

Ransomware continues to bedevil the public sector, with hackers targeting organizations that deliver essential services such as public safety, hospitals, schools and local government. Often, when organizations refuse to pay up, hackers retaliate by dumping the data on the web. That is how it played out for Oakland, California, which was the victim of an attack in early 2023. Eventually, city employees, whose data was exposed, filed a class-action lawsuit against the city.

WHAT'S BEING DONE

The federal government is working with organizations across the public and private sectors to undermine ransomware gangs. Here are some current initiatives:

- CISA has teamed with the FBI, the National Security Agency (NSA) and the Multi-State Information Sharing and Analysis Center to provide new guidance on **how to detect, prevent, respond to and recover from ransomware attacks**.
- As mandated by the National Cybersecurity Strategy, the State Department is working with the Joint Ransomware Task Force (co-chaired by CISA and the FBI) to develop an **"international engagement plan"** aimed at shutting down safe havens and cooperating on transnational cybercrime.
- CISA has launched the **Ransomware Vulnerability Warning Pilot Program**, which aims to help critical infrastructure organizations identify and mitigate vulnerabilities before they can be exploited.

Close the **Cyber Workforce Gap**

WHAT'S AT STAKE

Even as the global cyber workforce is now larger than ever, "the demand for skills still far exceeds the supply," according to a November 2023 study by ISC2, an association for cybersecurity professionals.

That gap means federal agencies face stiffer competition for cyber talent: More than half say staffing challenges make it difficult to improve their response to cybersecurity incidents, according to a December 2023 report from the Government Accountability Office.

WHAT'S BEING DONE

The Biden administration plans to explore ways to expand the capacity of two cyber workforce programs that have proven effective so far:

- The **CyberCorps Scholarship for Service**, which provides scholarships for up to three years of cyber-related studies in exchange for an equal amount of time of work in government
- The **DoD Cyber Scholarship Program**, a similar program that offers scholarships to improve both recruitment and retention efforts

States are also getting creative to expand their cyber talent, according to a 2023 survey of state chief information officers. Two popular tactics include offering hybrid or remote work and working with K-12 and/or higher education to recruit cybersecurity workers.

Prepare for **Quantum-Era Hackers**

WHAT'S AT STAKE

The race is on: Can researchers develop encryption tools that can withstand attack by quantum computers before quantum computers enter the mainstream? Mathematics is the key. Current encryption approaches work because to crack them, you need to solve complex mathematical equations that are beyond traditional computers' power. But quantum computers are expected to provide enough firepower to crack many widely used encryption algorithms. It's an "emperor has no clothes" scenario.

WHAT'S BEING DONE

The federal government, which is leading the advancement of quantum computing, is accelerating efforts to develop what has been dubbed post-quantum cryptography (PQC). Here are some of the initiatives underway:

- As part of an update to the Federal Cybersecurity Research and Development Strategic Plan, federal agencies will **partner with academia, manufacturers and the technology industry** to spur more R&D work.
- The National Institute of Standards and Technology has published three draft standards for **quantum-resistant encryption tools**, which are expected to be finalized in 2024.
- CISA, NSA and NIST are encouraging organizations to begin **planning their migration to PQC**, especially if they manage critical infrastructure.

Above all, the Biden administration believes the federal government can drive advances in cybersecurity by leading by example. "The private sector should follow the government's model in preparing its own network and systems for our post-quantum future," states the National Cybersecurity Strategy.

Simplifying Data Storage and Protection

An interview with Chris Sprague, Principal Technologist, Pure Storage



No organization is immune to cyber breaches. Bad actors with ample creativity and technical resources can pierce even strong cyber defenses. But there are strategies that make effective cyberattacks less likely and that protect data on which government depends.

"Breaches will happen. It's a matter of if, not when," said Chris Sprague with Pure Storage, which delivers forward-thinking security and data protection via a cloud experience. Agencies must practice good cyber hygiene, be prepared to mitigate fallout from a cyber event, and follow federal guidance as it evolves, he said.

PATH TO PROTECTION

Continuous protection requires a multilayered approach. It involves physical security — guarding access to buildings and the hardware within — and network security, which includes segmenting data and managing its travels, Sprague said. Data encryption is essential, as are backups, particularly if they're immutable, inalterable snapshots in time.

Similar to photographs, **snapshots** reflect the moment they're taken. If a cyberattack, human error, or another circumstance results in data theft, deletion or corruption, a snapshot can quickly restore what's lost, said Sprague.

An agency also must be able to **replicate** snapshots offsite. "My snapshot is protecting my data from being changed," he explained, "but now, that replication protects me in case, let's say, an earthquake happens and I lose a building. We want both of those [capabilities] in tandem."

Pure Storage provides them, Sprague said. It also offers a third layer, called **SafeMode**, that automatically keeps deleted snapshot data in a "bucket," similar to a Windows recycle bin, that's purged after a set period of time.

Ransomware attacks often occur because a hacker stole a network administrator's credentials. With SafeMode, an administrator cannot delete snapshots; backups are safe even if hackers invade an administrator account. That feature differentiates Pure Storage from competitors, he noted.

TRUST AND COMMUNICATION

Sprague said that when agencies need their backups, they want a platform that allows for rapid recovery; with Pure Storage, recovery can take just minutes. The technology promotes and supports cyber resilience and zero-trust principles, integrates with new and existing infrastructure, and conserves space and electricity, he said.

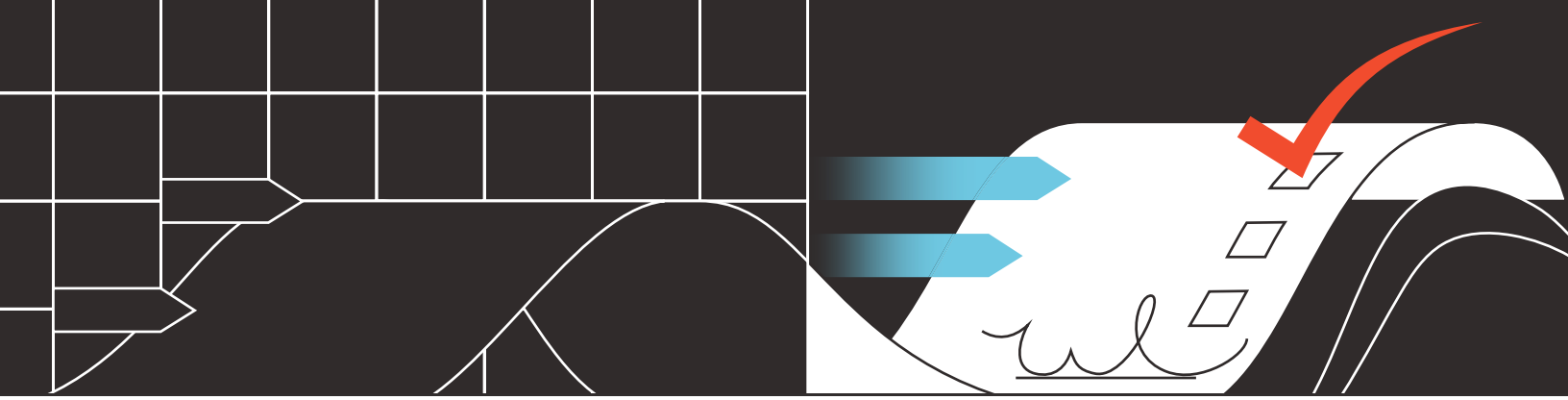
That helps agencies maintain business operations. And with extensive data at its disposal, government must be diligent about security.

"If agencies fail to protect their data, there's a high risk of data breach, which could lead to severe and wide-ranging consequences," Sprague said. "It could mean outcomes like reputational damage, which would erode the public's trust, to things like financial loss, identity theft … all the way up to national security threats [and] interruption to our critical infrastructure." Officials could be held criminally liable.

Intra-agency communication is vital after a breach, he said. "A lot of times in IT, when we have a problem, we put our heads down and try to fix it, and we don't necessarily communicate with the business side about what's going on." But open dialogue promotes transparency and constituent trust.

"Things [like trust] erode much faster than they build up," Sprague observed.

PURESTORAGE®



Turning Cyber Policy Into Practice

*An interview with **Cheri Pascoe**, Director, National Cybersecurity Center of Excellence*



Executive orders, frameworks, and acts of Congress tell agencies what their cybersecurity goals should be, but generally leave implementation details to other entities. The National Cybersecurity Center of Excellence (NCCoE), a component of the Commerce Department's National Institute of Standards and Technology (NIST), fills that need — developing actionable, standards-based guidance that helps agencies turn cyber concepts into reality.

Cheri Pascoe, NCCoE Director since last August, reflected on the center's strengths, challenges and 2024 priorities.

STRENGTH: COLLABORATIVE MODEL

"We describe ourselves as a collaborative hub, an applied cybersecurity laboratory," Pascoe said, where NIST cybersecurity experts partner with industry, academia and other government entities to tailor standards to the needs of specific sectors. The NCCoE guidance shows agencies how to adapt commercially available technology for their own purposes.

"We work with [our partners] hand in glove, or hands on keyboard," she explained. Once NCCoE decides to start a project, one or two NIST staff will team up with four or five of the center's contract staff, and then 15 to 20 collaborators from across industry and government also sign on, she said.

"You're basically taking one or two staff and turning [the project] into a large group of people," Pascoe added. "That kind of combination of expertise in both standards and technology is very rare, and so we're able to do some really cool things."

Although each group focuses on solving a single cybersecurity challenge, NCCoE's collaborative model also fosters product improvements and personal relationships.

Other governments may offer informal feedback on projects under development. And beyond project-specific work, NCCoE meets regularly with an industry advisory group to discuss current challenges and anticipate future concerns; maintains various communities of practice; and engages in local outreach.

CHALLENGE: PRIORITIZING ISSUES

The greatest NCCoE difficulty, and one that Pascoe aims to address in 2024, is deciding which issues to pursue. "It can take a year to develop a consortium, [and] it can take a couple of years to develop guidance," she said. "So really the biggest challenge is making sure that we can identify what challenges are coming … so that we're ready with guidance at the right time."

And faced with a limited budget and a vast number of cybersecurity issues, the center must develop guidance with broad potential. "Sometimes that's hard because we'll have different sectors come to us and say, 'This is a really big challenge for [us],' but it's not … applicable to other sectors, [so the center] might have to decline taking on that project," she said.

Created roughly 10 years ago, NCCoE has ended projects midstream when collaborators realized that pending guidance would have limited impact. "We really do have to be flexible in pivoting as we delve deeper into an issue, making sure we're addressing the right needs," noted Pascoe.

2024 PROJECTS

Of course, some NCCoE projects are rather pre-ordained. The center in 2024 will help specific sectors implement the NIST **cybersecurity frameworks**, including helping agencies transition from the initial NIST Cybersecurity Framework to the 2.0 iteration scheduled for release in February.

NCCoE also will continue its effort to help organizations develop **secure software**, as called for by the National Cybersecurity Strategy. At this stage, the center is working with global software development organizations to break down how agencies can implement the NIST Secure Software Development Framework.

And for the past five years, the center has been working with more than 20 vendors to build **zero-trust** architectures for its own systems. Currently, NCCoE is sharing its more than 1,000-page internal guidance with fellow agencies, Pascoe said.

But NIST is one of the world's top agencies for developing encryption standards, she noted, and so NCCoE in 2024 will prioritize helping agencies transition to new NIST cryptography standards. That will help agencies prepare for the potentially devastating threat of **quantum computers**.

"We're identifying tools to help organizations identify where there's vulnerable cryptography," said Pascoe, "and then help them make risk-based decisions about what you replace first."

NCCoE also will dig more deeply into **supply chain security**. "It's difficult enough to oversee the security of your own organization, let alone somebody else's," she said. "Over the last couple of years, [people] have really started to gain some recognition of just how important that issue is."

The center will continue its **artificial intelligence** and **ransomware** initiatives, among others. And because organizations asked NCCoE for help regarding data use and security, the center will advance its new project, launched in 2023, on **data file applications**.

"We're always listening and trying to really see the true challenges organizations are facing and see if we have the right expertise to … spin up a consortium to tackle [them]," Pascoe explained. "Cybersecurity is not just an IT issue, it's a business issue. It's a concern that needs to be addressed throughout [an] organization, at multiple levels."

NCCoE invites people from different backgrounds and disciplines to participate in its work by commenting on NCCoE resources and joining its communities of interest (COIs), among other options. Further details, including draft and final NCCoE publications, an events calendar, and a COI sign-up form, are available at www.nccoe.nist.gov. Technical expertise is not required.

Data Protection Builds Cyber Resiliency

An interview with Richard Breakiron, Senior Director for Strategic Initiatives, Federal Sector, Commvault



Feeling overwhelmed by growing needs for cyber protection? Each hour brings a new tale of bad actors and cyber breaches. Cybersecurity does not have to be difficult, especially if agencies follow federal standards, such as those developed by the National Institute of Standards and Technology.

Standards create the basis of security controls on which everyone can rely, said Richard Breakiron with Commvault, which provides agencies with comprehensive, intuitive, enterprise-level data management solutions. "Many people say cybersecurity is hard, and while complex to get started, establishing effective cybersecurity becomes easier once there's a culture of understanding that standards are the fundamental linchpins to the way you do business," he said. "That awareness demystifies the building of a cybersecurity foundation."

It starts with the simple things, much like driving a car, he said: Everyone knows to buckle their seatbelts and use their directionals before turning. These essential security and safety practices become second nature.

THE FUNDAMENTALS

The first step: Identify what you have, said Breakiron. Then prioritize your most important data, develop a data protection strategy, monitor your security measures once implemented, and respond to an attack when it occurs. Backups allow agencies to recover compromised data, he said, but even backups are cyber targets.

"You need to have a copy that is literally immutable. When an event occurs, you need to bring back that clean copy," he explained. Today's ransomware targets include operational backups, which are stored locally on a computer or network and designed for data recovery after power outages and human error, to maintain operational resiliency. Immutable backups can undermine a ransomware attack.

USING DATA

Data is the lifeblood of agencies today, turning ideas into tangible, potentially income-generating resources — therefore, protection of the data and the process to access it becomes pivotal. Yet data protection, Breakiron noted, "has gotten exponentially harder in the last 20 years [thanks to] the internet and the volume, variety and velocity at which data moves." Ensuring that data is always available to an organization, as Commvault does, "is the ultimate cyber backstop."

A comprehensive approach to data management, security and restoration includes the immutable, air-gapped backups. Agencies also must be able to retrieve data at a granular level, Breakiron said. Storing data with metatags allows you to later access only that file, saving time and expense, rather than extracting data you don't need.

RESILIENCY

Commvault Cloud sends automated, AI-generated cyberattack alerts upon detecting an unknown data source. This technology saves and quarantines the unknown data, then notifies a human response team, Breakiron said.

Sometimes the new source is innocent: An employee joined the organization and someone forgot to notify others. But as the state of Colorado discovered, the source could be nefarious — a server stood up by adversaries planning a cyberattack.

"At Commvault, uing NIST standards, we deliver a data-resilient foundation to ensure cyber resiliency for agencies," Breakiron said.

COMMVAULT

govloop

ABOUT GOVLOOP

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

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

govloop.com | @govloop

Click here to pre-register for the next two installments in our cyber guide series!

THANK YOU

Thank you to Commvault, CoreLight and Pure Storage for their support of this valuable resource for public-sector professionals.

CONTENT TEAM

Candace Thorson, Managing Editor

John Monroe, Director of Content

Susan Kirby-Smith, Senior Staff Writer

Lauren Walker, Senior Staff Writer

DESIGNERS

Kaitlyn Baker, Senior Creative Manager

Kelly Boyer, Senior Motion Designer