GovCIO MEDIA & RESEARCH

DeepDives

COMBATTING Ransomware

INSIDE:

SPONSORED BY

CYBERARK®

GovCIO MEDIA & RESEARCH

From the writer's desk

Kate Macri, Senior Staff Writer

Stemming the Ransomware Tide

U.S. Cyber Command and National Security Agency Director Gen. Paul Nakasone deemed ransomware a national security threat last year amid industry reports finding at least a 200% rise in ransomware attacks since 2019. For organizations seeking to combat ransomware, there is a seemingly endless deluge of proposed solutions and products.

One thing is certain: all organizations must maintain constant vigilance and diligently follow good cyber hygiene practices. Information-sharing and a zero trust approach to cybersecurity, which includes tools such as multi-factor authentication (MFA), privileged access management (PAM) and endpoint privilege management (EPM), can help.

Every organization will be hacked at some point, but learning how to curb certain threat vectors like ransomware will be imperative to limit losses and damages.

Table of Contents

Melissa Harris, Senior Staff Writer

Sarah Sybert, Staff Writer/ Researcher

Increased Cyber Defenses are the New Normal, Top Cyber Officials Say

CISA's Shields Up effort is here to stay as federal cyber leaders consider the future of cyber and national security.

BY MELISSA HARRIS

An enhanced cybersecurity posture is the status quo, federal cyber leaders said at the RSA Conference in June, adding they will leverage greater intelligence-sharing and collaboration, diverse skillsets and increased visibility to cultivate the new normal.

The sentiment follows growing acknowledgement that the rapid increase and frequency of cyberattacks since 2020 is not simply a symptom of physical conflicts or the global COVID-19 pandemic, but representative of the cyber landscape's "new normal."

CISA Director Jen Easterly, White House National Cyber Director Chris Inglis and NSA Cyber Director Robert Joyce.

Earlier this year, the Cybersecurity and Infrastructure Security Agency (CISA) launched the Shields Up campaign to build cyber resilience amid rising cyber threats stemming from the war in Ukraine.

Due to an emerging cyber landscape rife with cyber and ransomware attacks from nation-state actors and dark web ransomware-as-a-service offerings, Shields Up is here to stay.

"At the end of the day, we need to keep our shields up, because this message has actually resonated not just with the American people, but it's resonated with CEOs and business leaders who get that they need to empower their CISOs, which is one of the key recommendations we made on the Shields Up webpage, and ensure that there are the resources and the investments in place to be prepared to be able to not prevent, quite frankly, but to respond and recover effectively to mitigate risk," Easterly said during an RSA panel.

White House National Cyber Director Chris Inglis said the crisis in Ukraine was a clear indicator that U.S. agencies and industry partners need to work together closely to successfully identify and mitigate national cyber threats moving forward.

"It was clearly a declaration of a thunderstorm on the near horizon," he said, referencing recent Russian cyber threats. "What everybody wanted to

Photo Credit: GovCIO Media & Research Photo

Rob Joyce

Director, Cybersecurity Directorate, NSA

know was, when is what going to happen? … In order to determine that, we have to actually combine all of our insights, all of our capabilities, all of our authorities, because no one of us is probably going to see it for what it is."

Robert Joyce, Director of the Cybersecurity Directorate at the National Security Agency (NSA), said the intelligence community suspected malicious cyber activity would increase after Russia invaded Ukraine, further validating the need to double down on cybersecurity efforts across federal agencies and critical infrastructure sectors.

"We knew about real intentions, and that was the level of intel granularity," Joyce said. "It is hard to strike that balance of, we really do know that there is bad intent out there, but we may not know [specifically] where it's going to strike, and I really like the storm and lightning analogy, because it's very appropriate."

To maintain a heightened state of cyber defense, Easterly, Inglis and Joyce said it's essential to build trust across federal and private-sector stakeholders. Easterly said the Cyberspace Solarium Commission call to develop a Joint Cyber Planning Office, which CISA launched as the Joint Cyber Defense Collaborative (JCDC), will help her and her counterparts meet this goal.

"We want to be able to share that visibility so that we can identify those dots, connect those dots and drive down risk to the nation at scale, and we've been extending that since the war in Ukraine and started working together, planning together, implementing what we call and operational collaboration model where we're sharing information in near-real time," Easterly said. "It's starting to build momentum, but most importantly, it's starting to build trust."

CISA is considering the development of an advisory framework that will also determine scale and level of cyber threats based on national security agencies' intelligence information, Easterly added. This framework will help federal agencies consider a "more thoughtful way" of considering and communicating threats.

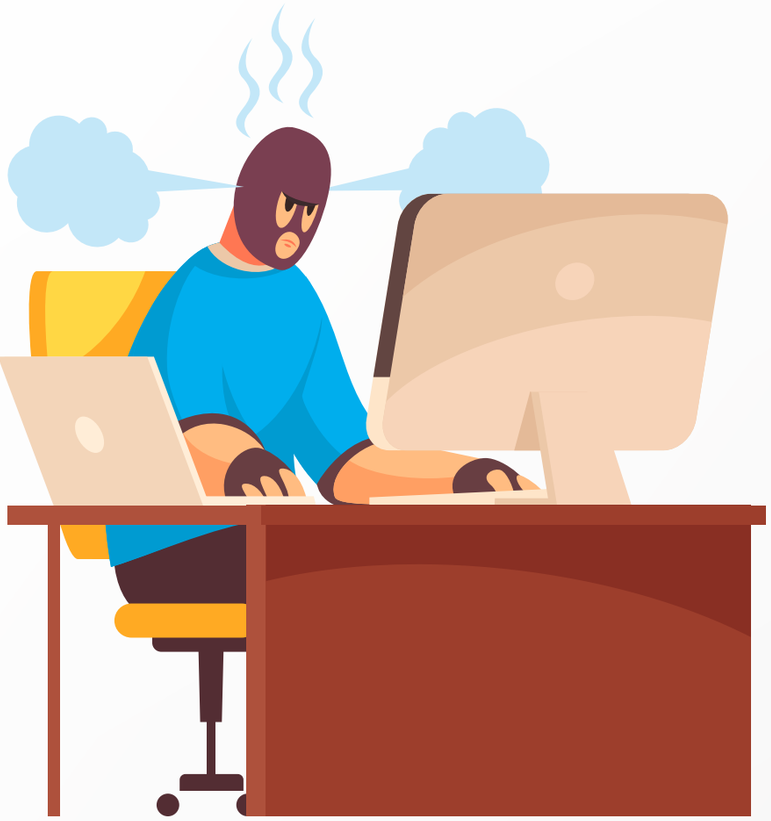
“It is hard to strike that balance of, we really do know that there is bad intent out there, but we may not know [specifically] where it’s going to strike, and I really like the storm and lightning analogy, because it’s very appropriate.”

— Rob Joyce, Director, Cybersecurity Directorate, NSA

GovCIO MEDIA & RESEARCH

DeepDives

Protecting Against a Ransomware Attack



MULTI-FACTOR AUTHENTICATION

the process by which a network verifies a user's identity before allowing access to the network. For example, after typing in a username and password to access the company cloud, a user may have to submit a six-digit code texted to their mobile phone before gaining cloud access.

ENDPOINT PRIVILEGE MANAGEMENT

the process of designating and restricting user privileges to only those needed for their jobs or certain job functions. When administrative privileges are widespread throughout an organization, bad cyber actors can more easily exploit them.

PRIVILEGED ACCESS MANAGEMENT

refers to administrators restricting and managing user privileges so as to limit their organization's attack surface, detect anomalous user behavior and mitigate and respond to cyber threats more quickly.

TIMED SESSIONS

the process of denying user access to applications and job functions after a designated period of inactivity to reduce the likelihood of a breach.

GovCIO MEDIA & RESEARCH

CYBERARK®

The Necessary Tools for Enabling End Point Security

Sophisticated security threats require modern methods in building cyber-resilient systems.

Andrey Pozhogin, Sr. Product Marketing Manager, Endpoint Privilege Security @ CyberArk, and an IT Security Expert

What is the importance of endpoint security when protecting against ransomware attacks?

Pozhogin Endpoint security is the organization's last chance to block ransomware before it deals damage. If you are at the point where your endpoint security is making the decision to block or allow a ransomware sample, quite a few of your defense layers have already fallen. They have already successfully touched the endpoint — they are in.

It means your organization has been targeted, it has been identified within vectors of attacks, and the attacker has made it all the way through email security, network security, sandboxes and so on.

The decisions your endpoint security team makes in the next moments is the difference between "just another day" and "the systems are down, do we have any backups?" Thus, a multi-layered identity-based endpoint security is an absolutely critical component of a defense-in-depth (DiD) approach.

> **“Adaptive and scalable security controls continuously fine tune the balance between convenience and security to ensure the user is not overly burdened with security processes while assessed risk remains at acceptable levels.”**
>
> **— Andrey Pozhogin, Sr. Product Marketing Manager, Endpoint Privilege Security, CyberArk**

How can Endpoint Privilege Management (EPM) lower ransomware risk while improving user experience and smoothing local IT operations?

Pozhogin With CyberArk’s Endpoint Privilege Manager, an organization from day one can confidently defend against attacks by removing local admin rights, enforcing least privilege, and protecting the entire endpoint security stack from tampering. This will defuse most TTPs and prevent things like tampering with backup and logging agents, disabling shadow copies, wiping master boot record (MBR), exploiting a significant number of vulnerabilities and living-off-the-land (LotL) attacks.

Credential theft protection prevents attackers from compromising more credentials, elevating their privileges and moving laterally.

The Endpoint Privilege Manager also adds an additional layer of defense around sensitive data. Only designated content handlers are then allowed to even touch the data, so any high-risk or newly introduced software wouldn’t even be able to read the data.

The beauty of least privilege projects leveraging the right tools such as Endpoint Privilege Manager is that most operations involving elevation are completely automated and are transparent to the user. This helps significantly relieve the amount of user requests sent to the service desk. In addition, those operations are logged and provide a full audit trail for privileged actions.

How does Privileged Access Management (PAM) dovetail with zero trust principles, such as identity, credential and access management (ICAM), to boost cyber resilience to ransomware?

Pozhogin Federal officials have said ransomware is here to stay. With the pandemic leading to boosts in remote work, accessing data from mobile devices and widespread workforce changes, identity has quickly become the

new perimeter. Privileged access is a necessity. Under certain conditions, every identity has (some) privilege associated with it — an IT admin who needs to work on a server, a human resources official who has access to salaries, a financial analyst looking at the business.

Bad actors are thrilled with the attack surface expansion due to the explosion of identities with privileged access, so Privileged Access Management (PAM) is a necessity in defending against ransomware. A PAM strategy enforces the principle of least privilege to restrict account permissions to a minimum level. With CISA's recommended zero trust maturity model, determining advanced access requires least privilege controls to consider identity. Therefore, PAM enables zero trust by reducing the expanded attack surface of identity, through credentials control and access to sensitive information, ultimately preventing the spread of ransomware and boosting cyber resilience.

Can organizations maintain a strong cyber posture and limit ransomware exposure under a bring-your-own-device (BYOD) policy? If so, how?

Pozhogin Ransomware is a top-of-mind concern for most organizations. Ransomware is no different than any other malware that exploits poor foundational security.

Over 51% of respondents in CyberArk's Threat Landscape Report indicated that unmanaged identities represent the biggest security risk in today's hybrid/remote work environment. About 61% of respondents have identity-security controls in place for employer-assigned user devices, compared to 40% for employee-sourced or "bring-your-own-devices" user devices.

As ransomware evolves, new variants not only encrypt data and damage business continuity, but also lead to public data leaks of confidential information. CyberArk can secure both the endpoint where attacks often start, as well as the

Photo Credit: XXXXXXXXXXX

privileged credentials attackers leverage to move horizontally and vertically.

Using controls like multi-factor authentication, privileged credential rotation and session isolation, and removing local admin rights from endpoints, CyberArk is a trusted partner that helps any organization reduce the risks associated with ransomware attacks while protecting the user experience.

What is the role of adaptable and scalable security controls, such as adaptable multi-factor authentication (MFA), in a cyber strategy to protect against ransomware?

Pozhogin Adaptive and scalable security controls continuously fine tune the balance between convenience and security to ensure the user is not overly burdened with security processes while assessed risk remains at acceptable levels. Continuous and adaptive multi-factor authentication, while not sufficient for ensuring trust on the endpoints on its own, together with endpoint privilege security controls creates a formidable barrier in the path of ransomware. As an example — ransomware operators often rely on legitimate tools to establish foothold on the endpoint, set the stage for the attack, exfiltrate data and launch the payload (so-called “LOL” or “LOtL” attacks — live-off-the-land).

With identity-driven endpoint security, such as CyberArk Endpoint Privilege Manager and CyberArk Identity, we can selectively challenge the user based on the assessed risk of their action to MFA themselves. Let’s say the user is attempting to launch PowerShell with administrative privileges — this operation will allow the user to do pretty much anything on the endpoint, including disabling shadow copies, tempering with backup agents and altering logs. In this case, it is smart to ensure this is indeed your system administrator who’s launching the elevated PowerShell console and challenge them to MFA. Such MFA interventions, called “step-up” authentications, allow to significantly raise the security and defend against ransomware — all while maintaining system usability and user convenience.”

SECURE PRIVILEGE. STOP ATTACKS.

ACROSS THE ENTERPRISE
IN THE CLOUD
ON ENDPOINTS

Unsecured privileged accounts add risk to your business anywhere they exist— 100% of advanced cyber attacks involve them. Seamlessly protect privileged accounts across the enterprise— on premises, in the cloud and on your endpoints with CyberArk.

Federal Certifications and Compliances Include:

- DoD UC APL
- Common Criteria Certified
- NIST SP 800-53 / -171 / -82 / -63
- NERC-CIP
- DHS CDM Phase II Privilege Management Solution
- Army Certificate of Networthiness (CoN)
- Available on DoD Cyber Range
- HSPD-12
- In Evaluation for NIAP

CyberArk.com

CYBERARK®

Feds Tackle Growing Ransomware Risks With Zero Trust

Cyber organizations are adopting zero trust and access management solutions to combat new ransomware threats.

BY SARAH SYBERT

The commander of the U.S. Cyber Command and director of the National Security Agency (NSA), Gen. Paul Nakasone, declared ransomware a national security threat in 2021 following compromises to critical infrastructure and key resources. The SolarWinds and Colonial Pipeline attacks, along with virtual network expansions, have forced organizations to build a stronger cybersecurity infrastructure to better detect security risks.

Recent progress in zero trust and privileged access management (PAM) solutions are helping combat these evolving ransomware threats, especially amid what's called ransomware-as-a-service (RaaS), a subscription-based model that enables affiliates to use already-developed ransomware tools to execute their attacks. With these types of models, bad actors and adversaries do not have to be well versed in ransomware in order to use the tools for attacks.

This contributes to as much as a 200% rise in ransomware attacks in the past two years in the U.S., according to a 2021 report from Delinea.

The shift from "vertically oriented" threat actors, who make and then attack organizations using their own bespoke ransomware, to the RaaS model where one group builds the ransomware and then leases the use of that ransomware out to specialists has changed the threat landscape and increased scale and number of attacks.

In 2022 and beyond, the RaaS business model will continue to dominate

the threat landscape for ransomware attacks, according to another report from Sophos. This model enables ransomware developers to continue to improve the attack vector and increase attack intensity, without slowing attacks.

"We've already seen these RaaS threat actors innovate new ways to break into progressively more well-defended networks, and we expect to see them continue to push in this direction in the year to come," the Sophos report said.

As cyber threats become more prevalent and sophisticated, the Biden

Photo Credit: Christiaan Colen / flickr

administration is directing agencies to improve defenses to prevent, disrupt or mitigate attacks. The White House Executive Order on Improving the Nation's Cybersecurity takes a holistic approach to securing networks, requiring agencies to shift toward zero trust architectures and adopt advanced security solutions.

PAM solutions are key here. By enforcing "least privilege" principles, organizations can prevent credential harvesting and lateral movement, reducing attacker dwell time and making it more difficult to use ransomware tools. Plus, PAM policies enable security teams to identify the attack entry point, understand what's happened, help remediate and ultimately protect restored data — the end goal of any zero trust approach.

"Least privilege is one of the many essential components of zero trust," DLT Chief Cyber Security Technologist Don Maclean said during a GovFocus earlier this year. "All human systems and users only have the privilege they need to do their jobs. I've been involved in least privilege exercises, and what you find is, often, with the hurry to get things done, excessive privileges are given and you don't want to sit there and parse out what they don't need. Once people have privilege, they feel privileged and important. Rescinding those privileges becomes an exercise in human management and knowing what they actually need to do their jobs. That's just one example of the types of cultural things that will be difficult in implementing a zero trust program."

The NSA recently released guidance for embracing a zero trust approach, noting these "principles can better position [cybersecurity professionals] to secure sensitive data, systems, and services."

NSA's 2021 Cybersecurity Year in Review outlined how NSA worked to prevent and eradicate threats to critical systems over the past year. One of the agency's top highlights was working with partners, through its Cybersecurity Collaboration Center, to respond to national-level threats, like SolarWinds and

“We want to be able to share [cyber threat landscape] visibility so that we can identify those dots, connect those dots and drive down risk to the nation at scale, and we’ve been extending that since the war in Ukraine and started working together, planning together, implementing what we call and operational collaboration model where we’re sharing information in near-real time. It’s starting to build momentum, but most importantly, it’s starting to build trust.”

— Jen Easterly, Director, CISA

multiple ransomware attacks on U.S. critical infrastructure.

“While many of our mission successes must remain classified, I’m proud that we can showcase how NSA Cybersecurity helps contribute to securing the nation in this report,” said Rob Joyce, NSA’s cybersecurity director, according to a press release. “The successes really show the value NSA cybersecurity delivers through its foreign threat intelligence insights, partnerships and expertise.”

NSA worked collaboratively to analyze cyber threats and share insights through its foreign signals intelligence about the cyber criminals profiting from ransomware and their infrastructure. The agency alongside U.S. Cyber Command and other government and industry organizations pursued the actors, capabilities and finances driving global threats.

“Throughout the effort, NSA ensured that its threat intelligence was disseminated at the lowest possible classification level, so that it generated outcomes,” the report said.