GovCIO MEDIA & RESEARCH

OCTOBER 2024

DeepDives

Securing Data and BUILDING RESILIENCY

INSIDE:

SPONSORED BY

Commvault®

From the editor's desk

Amy Kluber, Editor-in-Chief

Preparing and Recovering from Security Incidents

Cybersecurity leaders consistently say organizations should be vigilant around data security breaches and be ready for when they inevitably happen.

In this issue, we delve into advancements in cyber resiliency within the federal government amid an evergrowing digital world. This includes a look at the standards around data backup and insight into rebuilding digital infrastructure especially in hybrid-cloud environments.

Plus, we look at the White House's recently unveiled plan to secure internet routing, a move aimed at fortifying the nation's cyber defenses. National Cyber Director Harry Coker urged agencies to adopt secure routing protocols and lead by example.

Federal agencies are also advancing cyber resiliency within the health care sector. Officials from the Department of Health and Human Services (HHS) and the Centers for Medicare and Medicaid Services (CMS) noted some of the programs and approaches organizations should take to protect sensitive health data from cyber threats.

Table of Contents

New White House Roadmap Looks to Secure Internet Routing

The plan outlines next steps in strengthening cybersecurity in the Border Gateway Protocol, a foundational part of the internet.

BY ROSS GIANFORTUNE

The White House released a plan to secure the Border Gateway Protocol (BGP), the data-routing framework that makes up much of the internet's data transmission foundation.

The Office of the National Cyber Director revealed the plan as part of the White House's National Cybersecurity Strategy Implementation Plan to secure the technical foundation of the internet. Called the Roadmap to Enhancing Internet Routing Security, it outlines fixing a key security vulnerability in the internet ecosystem. The original 1989 design properties, initially developed to facilitate quickly transferring data between computers, do not address cybersecurity threats and cyber resilience requirements of the modern internet.

"Internet security is too important to ignore, which is why the federal government is leading by example by pushing for a rapid increase in adoption of BGP security measures by our agencies," said White House National Cyber Director Harry Coker. "ONCD, along with our public and private sector partners, are guiding a risk-informed path forward toward our communal objective. We aim for this roadmap to mitigate a longstanding vulnerability and lead to a more secure internet that is vital to our national security and the economic prosperity of all Americans."

Coker expanded on the security concerns connected to the protocol and emphasized the call for the federal government to be leaders in security.

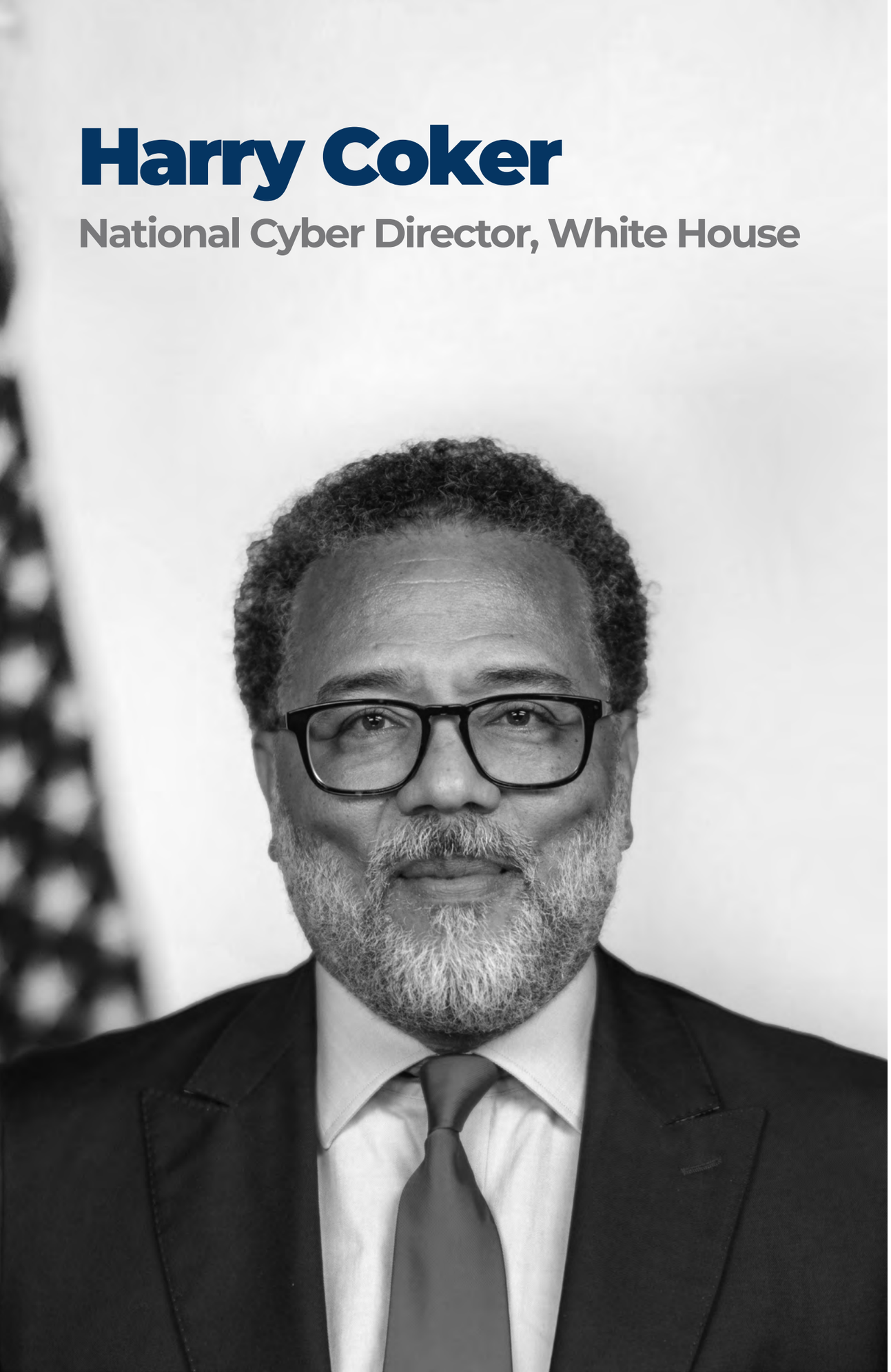
"We've had instances where internet traffic has been rerouted accidentally and maliciously by our nation-state actors. This is going to help address that problem," said Coker during the 2024 Billington Cybersecurity Summit. "It's

White House National Cyber Director Harry Coker, Jr. speaks at the Billington Cybersecurity Summit in Washington, D.C.

Photo credit: C-SPAN

Harry Coker

National Cyber Director, White House



certainly not going to fix it all, but this is a case where the federal government is going to lead by example. By the end of this calendar year, we'll have 60% of our internet space with registered address capabilities."

The roadmap outlines 18 recommendations that include:

- Instructing the Office of Management and Budget to create guidance for agencies to bring forward security measures soon.
- Directing the State Department to engage international partners.
- Partnering between the government and industry to monitor data moving through networks and build risk management frameworks for network operators.
- Taking the National Institute of Standards and Technology with coordinating government efforts to "standardize, and foster commercialization" of BGP security.

NIST Director Laurie Locascio highlighted the agency's role in creating standards for industry operators.

"NIST has a long history of working collaboratively with industry to design, measure, and standardize technologies that make internet protocols more resilient and secure," said Locascio. "This roadmap establishes a clear plan of action to expedite the adoption of current, commercially viable BGP security technologies while highlighting the need for further research and development of additional solutions."

ONCD also said it is partnering with the Cybersecurity and Infrastructure Security Agency to establish an Internet Routing Security Working Group to develop resources to advance cybersecurity recommendations contained in the roadmap.

"We're going to have a joint private sector, public sector working group to address a path forward," Coker said.

“Internet security is too important to ignore, which is why the federal government is leading by example.”

— Harry Coker, National Cyber Director, White House

GovCIO MEDIA & RESEARCH

DeepDives

Preparing Organizational Data for Incident Response

The National Cybersecurity Center of Excellence at the National Institute of Standards and Technology (NIST) developed a set of suggestions to buttress organizations to prepare for breaches that affect data and systems.

INTEGRATE THE APPROPRIATE STORAGE TECHNOLOGIES INTO THE OPERATION.
Organizations need to incorporate cloud storage, removable media storage, automated data backup and local hard drive storage into plans.

KEEP A SET OF SYSTEMS COMPLETELY DISCONNECTED FROM THE ORGANIZATION'S NETWORK.
Maintain an offline or a separate firewalled network with recovery data in the event of an incident.

CONSIDER ALTERNATIVE STORAGE.
Maintain physical diversity capabilities for recovery site in case the primary facility is unavailable for activities.

PREPARE A "GO BAG" FOR RECOVERY.
Keep a copy of critical data like passwords and security keys in a secure and accessible location to speed recovery in the event of data loss. Physical paper copies of some information may be necessary.

Source: NIST

GovCIO MEDIA & RESEARCH

PARTNER INTERVIEW

Commvault®

A SaaS Approach to Rapid Cyber Recovery

What are some of the challenges in rebuilding digital infrastructures after a data breach or ransomware attack?

Ansari Although many organizations now back up their data, they do not protect the blueprint for how that flowed across the organization. They need a plan to recover that blueprint first before restoring it. This challenge is even greater in our hybrid cloud and on-premise environments to ensure how a cloud data center supports the flow of business data.

Commvault Cloud takes a blueprint of the cloud data center as well as the data and stores it so it is pristine. That way after an attack, we can restore on demand the cloud blueprint into a new environment that never existed before. The likelihood that a cyber presence remains is now zero because we restore back to the state before it was present. We re-establish the environment based on the blueprint prior to the attack, then populate it with clean data from backup files in the right order and then test it to make sure it is valid. We provide automation and consistency to that entire process.

(ctd.)

Govind Rangasamy
Founder and CEO, Appranix

Kashif Ansari
Senior Director of Sales Engineering, Commvault

This approach also has financial advantages because the organization does not have to pay for that new environment until it is set up.

What are some of the use cases for Appranix's AI-driven automated solution and Cloud Time Machine in enhancing data recovery?

Rangasamy The hybrid cloud environments present in most organizations are complicated because of the distributed nature of the cloud applications themselves. These application environments are made up of several of these interconnected cloud services, and some of the services will have data in several different databases.

The second problem is that these environments change quite a bit because of the promise of cloud agility. That means the organization can change and release new features and satisfy customer requirements quickly.

A third problem is that because cloud architecture allows for creating accounts, organizations can virtually segment different parts of their infrastructure so that development and production are in separate accounts.

Even though the environments are getting more complex, Recovery Point Objectives (RPO) are shrinking.

Appranix's AI-driven automated solution and Cloud Time Machine ensures you don't have to write the scripts and worry about cloud-native language. Commvault Cloud is continuously discovering and protecting all the cloud resources, the dependencies and the data together so that you can rewind to an earlier point in time if something such as a cyberattack were to happen.

With Commvault Cloud, restoring an environment that used to take up to 72 hours can be done in about 32 minutes, according to a recent Appranix study.

Looking ahead, what advancements do you anticipate in the field of automated data recovery?

Ansari Over the next few years, we're going to see more workloads go to the cloud. In the public sector, some applications and data will stay on-prem, and some will go to the managed service providers (MSP) or a third-party cloud provider.

"After an attack, we can restore on demand the cloud blueprint into a new environment that never existed before."

— Kashif Ansari, Senior Director of Sales Engineering, Commvault

So where does the liability of the data lie and how do we manage it?

We are seeing a consolidation of automation tools in the market. We are in the business of helping customers recover and prevail against ransomware and other cyber threats. You are seeing us and our peers integrate with more security vendors like Palo Alto and CrowdStrike.

We want to encourage every organization to test their environments continuously. With Commvault Cloud, they can do that without disrupting their production. That takes away the pain associated with testing.

Testing continuously is going to simplify life in the long run. If you have tested, you can trust your environment and be confident that the process works. As long as the process works, you can focus on delivering the mission.

Photo Credit: Mer_Studio/Shutterstock

Commvault®

FedRAMP™

ANYTHING LESS THAN FEDRAMP® HIGH IS...LESS.

SCAN QR CODE
TO LEARN MORE

How Health Care Leaders Should Plan for Building Cyber Resiliency

Policy leaders recommend health care organizations implement tools like encryption and multi-factor authentication to protect their data.

BY NIKKI HENDERSON AND AMY KLUBER

Federal health leaders are strategizing how health care organizations can build and budget for cyber resiliency as the attack landscape and need for data security grow.

"Resiliency costs money. … You can't just plug in a new system and say that you are now resilient," said Keith Busby, acting CISO and director of the Information Security and Privacy Group at the Centers for Medicare and Medicaid Services (CMS), during a recent webinar. "You don't need to throw out everything that you've done. You just need to look at it from a different angle and look at some of the best practices that have been around for years."

The Department of Health and Human Services (HHS) released its cybersecurity strategy last year outlining four pillars of action to strengthen resilience through voluntary health care and public health sector cybersecurity performance goals (HPH CPGs). The goals incentivized organizations to develop resiliency and also expanded cybersecurity services within HHS' Administration for Strategic Preparedness and Response (ASPR).

Cmdr. Thomas Christl, director of the Office of Critical Infrastructure Program within ASPR, noted the goal for the 2023 HHS roadmap was to provide consolidated, actionable guidance recommendations in a simplified manner.

"This is going to cost money, and so HHS is looking at how can we incentivize entities to implement those practices. There's mention of upfront investment programs as well as incentives to continue to advance the practices within an entity," he said during the webinar. "What do we already have in place? Existing brands, programs or collaborative agreements or cooperative

Photo Credit: MUNGKHOOD STUDIO/Shutterstock

agreements, where else might we need to grow?"

The comments come amid an overhaul at HHS in which cybersecurity and tech policy and strategy functions are moving to ASPR and the renamed Assistant Secretary for Technology Policy and Office of the Coordinator for Health IT (ASTP/ONC).

"Cybersecurity, data and artificial intelligence are some of the most pressing issues facing the health care space today," said HHS Secretary Xavier Becerra in a statement. "For decades, HHS has worked across the organization to ensure appropriate and safe use of technology, data and AI to advance the health and well-being of the American people."

Tips for Cyber Resiliency

There are several things health care organizations should prioritize to increase data security and resilience. One priority is having good data inventory.

"As an organization, you need to be able to know where your data is and who you're giving it to, and so I think finding a way to do that is important, and you're only going to do that through relationship building through collaboration with the business side of the house," said Busby.

Busby added multi-factor authentication and encryption are basic security controls organizations should implement.

Christl added that cybersecurity should also be a part risk management approaches.

"Everything relies on it, and it can't just be an afterthought. Work it into exercises. Have specific exercises for cybersecurity. The preparedness supports resilience and recovery," said Christl. "Also try to truly understand the first, second, third-level contingencies, and make sure you have plans to address those contingencies as much as possible. Then the most important part of all of this is that once you think you've understood those, talk with the people and have the conversations that go back to the contracts and resilience." (ctd.)

ARPA-H Programs Tackle Resilience

Christl cited efforts the Advanced Research Projects Agency for Health (ARPA-H) launched including its new Universal PatchinG and Remediation for Autonomous DEfense (UPGRADE) program and its Digital Health Security Initiative.

Christl said he's also collaborating with the Cybersecurity and Infrastructure Security Agency (CISA) to help organizations understand what resources they have.

"They have free, scalable services that entities can sign up for to help get information on where they might be vulnerable," said Christl. "They also have a health care and public health sector cybersecurity toolkit. We're working with them to make sure that they're speaking the right language for the health care sector, that they're engaging effectively so that as many people as possible become aware of these resources and that they're going to be taking advantage of them."

"Resiliency costs money. … You can't just plug in a new system and say that you are now resilient."

— Keith Busby, Acting CISO and Director of the Information Security and Privacy Group, CMS