FEDInsider

Adapting Advanced IT and Zero Trust For The Federal Government

Civilian agencies are modernizing systems, adopting zero trust and also considering the user experience when enhancing cybersecurity government-wide.

The pandemic forced federal agencies to modernize IT quickly, as they migrated to hybrid and multi-cloud environments to support remote workers and adopted digital services to keep up with customer demand. These trends continue, yet also increase the need for stronger cybersecurity to protect endpoints and data.

The Office of Management and Budget's (OMB) Federal Zero Trust **memo** is intended to bolster federal cybersecurity, improve risk assessment and help agencies improve lagging security practices. Thought leaders from government and industry spoke at recent **FedInsider webinars** to discuss the intersection between IT modernization progress and enhanced cybersecurity.

The Pandemic's Impact on Cybersecurity

Teleworking wasn't an entirely new concept to the government, yet the size and scale of telework once the pandemic hit was what Dr. Gregory Edwards, chief information security officer for FEMA, called an "explosion." For the expansiveness of an organization like FEMA, this was a big undertaking for collaboration and security.

"We had to begin to understand it and take a little more risk. And then we had to expedite some of the major projects we had in place, one of those being a network monitorization, speaking to the capacity that we could extend ourselves to the edge. And we also had an identity program that we had to expedite," Edwards said.

That element of accessing networks from home created a new realm of security worries that agencies and industry partners had not fully considered before. "All this remote work and remote access coming into our organizations had to go through new networks, and we weren't necessarily mapping those out," said Brian Dennis, principal technologist for the public sector at Akamai. "We had to make sure that everyone began to understand that cybersecurity is not just one person's job in an organization, it is everyone's job."

FEMA has since adopted a tailored secure-by-design approach; one that is built around the organization's engineering lifecycle process requirements so that new capabilities have security baked in from the start. FEMA is also looking toward advanced cyber capabilities, like micro-segmentation, zero trust, complete network visibility and machine learning to help fill in the gaps.

Getting Started With Zero Trust

The strategic goals in OMB's memo align with the Cybersecurity and Infrastructure Security Agency's five pillars: identity, devices, applications and workloads, network and data. "You have to think about devices and how they are handled. And then think about your network and how you handle traffic going across that network," said Tony Lauro,

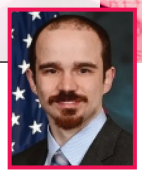
Featured Experts:

- **Dr. Gregory Edwards**
  Chief Information Security Officer, FEMA

- **Brian Dennis**
  Principal Technologist, Public Sector, Akamai

- **Jennifer Franks**
  Director, IT & CS Team, U.S. GAO

- **Wayne Rodgers**
  Zero Trust Lead, United States Department of Education

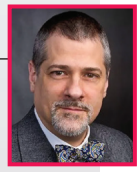


- **Tony Lauro**
  Director of Security Strategies, Akamai Technologies

- **Conrad Bovell**
  Branch Chief, CS Advisory & Strategy, OIS/OCIO/OS, Dept. of Health & Human Services

- **Randy Wood**
  Senior Vice President, North American Sales, Akamai

- **Jonathan Feibus**
  Chief Information Security Officer, NRC



- **Beau Houser**
  Chief Information Security Officer, U.S. Census Bureau

- **Dave Zukowski**
  Principal Technical Consultant, Akamai

director of security strategies at Akamai. The goal is to put validation and control around each of those pillars.

Following the guidance and requirements of OMB's zero trust memo has been helpful for the Government Accountability Office according to Jennifer Franks, director of the IT and cybersecurity team for the GAO. "What zero trust offers all of us is the opportunity to really lessen some of the damage and the impact that occurs once the cyber incidents do happen," Franks said. This makes it more difficult for bad actors to move laterally across IT environments. To get there, Franks recommends continuously implementing sprints to reach each pillar.

For the Department of Education, implementing zero trust started with a gap analysis based on the system's original maturity model. "What was determined was that there was a need for secure access service end solutions and security automation and response solutions," said Wayne Rodgers, zero trust lead for the Department of Education. "And that was because there were technologies in place at various degrees of maturity."

Rodgers recommends every agency have a gap analysis performed to see where they are security-wise before starting with zero trust. Then, they can consider the identity aspect with advanced tools like secure access service edge network and security orchestration, automation and response technologies.

Making Cybersecurity Work With Good User and Customer Experiences

According to Randy Wood, senior vice president of North American sales at Akamai, three factors are driving how people interact with IT and government: Using technology to compete with peers and adversaries globally, driving warfighter technology and using technology solutions to meet users' expectations while driving better outcomes. According to Wood, good customer experience is defined by speed, availability and security.

And when it comes to security, it must be there – but it should also be out of the way. "We want a very strong, robust security posture environment, and at the same time, we want a very simple but powerful user and customer experience using technology," Wood said.

For the Department of Health and Human Services, achieving good user experience and robust cybersecurity in government means focusing on the user, the protection of data and the delivery of services. "That is also one of the areas that you see with the zero trust mandates," said Conrad Bovell, branch chief of cybersecurity advisory and strategy, OIS/OCIO/OS, for HHS. "That has had a very positive impact on organizations in terms of their efforts to deliver capabilities to their constituents."

Bovell has even incorporated human-centered design into the identity pillar of zero trust when rolling out a new identity management solution like single sign-on, multi-factor authentication and self-service portals – putting less dependence on admins. "We made it more effective, and the experience of conducting business in a more secure way was made easier," he said.

The Role of Threat Intelligence Sharing

Having a constant flow of threat information allows agencies to threat hunt and be proactive. The U.S. Census Bureau, for instance, created a dedicated team of five intel analysts to track adversaries and share data with threat hunting teams. "The threat actors primary focus is capability, opportunity and intent," said Beau Houser, CISO for the U.S. Census Bureau. "You need an understanding about what actors are out there and what threats may involve your organization."

For a smaller agency like the Nuclear Regulatory Commission (NRC), intel capabilities are rented or borrowed, and automation is used to make up for a lack of numbers or general expertise. "We do what we can to get things implemented as quickly as possible," said Jonathan Feibus, CISO for the NRC. Though not always real-time, this enables NRC to better predict the types of attacks it could one day encounter. And according to Feibus, the NRC is working to further improve its capabilities in that area.

Threat intelligence sharing could also be critical to addressing vulnerabilities and bringing down siloed resources. "The more you can break down the functional stovepipes and not so much focus on the tools, but instead the outcome of the entire mission and how those tools assist that mission, I think we will get better cross-collaboration among the teams," said Dave Zukowski, director of defense solutions at Akamai.

Cybersecurity requires a whole-of-government approach, after all. As Feibus said, sharing threat intelligence is an important part of the community. "If you are only taking, and not giving anything back, that is a lost opportunity to protect the entire federal enterprise," he added.

FEDInsider

Hosky Communications Inc.
3811 Massachusetts Avenue, NW
Washington, DC 20016

(202) 237-0300
Info@FedInsider.com
FedInsider.com
Facebook.com/FedInsiderNews
Linkedin.com/company/FedInsider
@FedInsider

carahsoft

Carahsoft
11493 Sunset Hills Road, Suite 100
Reston, VA 20190

(703) 871-8548
Info@Carahsoft.com
Carahsoft.com/Akamai
Facebook.com/Carahsoft
Linkedin.com/company/Carahsoft
@Carahsoft

Akamai

Akamai Technologies
11111 Sunset Hills Road, Suite 250
Reston, VA 20190

(617) 444-3000
Info@Akamai.com
Akamai.com
@AkamaiTechnologies
Linkedin.com/company/Akamai-Technologies
@Akamai