

Federal Agencies Face Sophisticated Cyber Threats Head-On

Increased data security, threat information sharing & automation tools are a few ways IT leaders are protecting against today's cyber warfare.

Featured Experts:

■ **Nicole Willis**
Chief Technology Officer,
Office of Inspector
General, Health &
Human Services



■ **Patrick Gould**
Director, Cyber &
Telecom Portfolio,
Defense Innovation Unit



Today's connected world creates unique challenges for government agencies. Cyber defenders are faced with an overwhelming number of cyberattacks that are getting more sophisticated and complex. Attackers, from both criminal organizations and nation-state actors, are causing cyber conflicts in the virtual world almost every week – and some are even attacking federal agencies.

To manage these cyber threats, agencies are taking the necessary steps to understand the cyber landscape and how to defend against it. Members of the government recently spoke at [a FedInsider panel](#) to discuss the nature of cyber warfare and share useful mitigation information.

Securing Federal Networks and Data

Cyberattacks like ransomware, zero-day attacks and phishing campaigns are on the rise to try and exploit data, target an organization's widely-used software, extort monetary ransom, gain access to a network or application, expose sensitive information and more. These threats are putting organizations' missions at risk.

So, when the pandemic hit and people began working from home, data integrity became a must. "We realized quickly that there was not a lot of at-home and remote data

integrity capabilities or trust capabilities for much of the workforce," said Patrick Gould, director of the Cyber and Telecom Portfolio for the Defense Innovation Unit.

Luckily, the DIU was already familiar with commercial tools and environments. The agency was able to set up remote work environments over the course of a week-end. One of those solutions was secure cloud management via cloud-based access points that the commercial sector has been using for years to move to the cloud and remote environments. "These increased security posture for remote work needed to be at a high level, but could not kill productivity for the DOD," Gould said. Securing data was a must so that at-home users weren't routing applications and data back and forth from the DOD's secure gateway network.

Securing agency data is also about culture, like adopting a zero trust mindset, said Nicole Willis, chief technology officer for the Department of Health and Human Services' Office of Inspector General. "Really trying to make sure that trust is not implied, and the devices should be continuously monitored to make sure that they are accessing the right data and applications at the right time," Willis said.

There are several things that can be done if an intrusion does happen, like understanding and mapping out dataflow to know what normal behavior is and what is an anomaly. There is also optimizing devices and using automated discovery to assess what is unused and unneeded.

"Why secure those devices if no one is using them when they're not providing any value and can expose additional vulnerabilities?" Willis said. Having insight into all network endpoints, understanding normal behavior versus abnormal behavior, and knowing agency data and how users interact with it are key to securing federal networks and limiting the movements of a hacker inside the network.

Taking Preventative Measures

There are ways agencies are getting ahead of enemy attacks to be proactive. Gould said there's an entire wing of cybersecurity training and awareness focused on defending data and protecting systems. It's about understanding "the threats to your environment, not just the protections and the controls and the physical limitations of the device that you have, but understanding why someone would want access to your data...and how can they gain access to the data and systems," he said.

Once that is determined, IT teams can develop the best defense strategy and capabilities to defend against that. Sophisticated actors are getting past generic security controls, so it's time to think creatively.

Sharing threat intelligence, best defense practices and tools is also helping organizations defend against cyberattacks. "The more, as an industry, across both private and public sector that we can share the data, the more beneficial that will be to people that need that data to protect their systems. But really, that collective understanding of the actual threat above and beyond system control is the most important part of that ability," Gould said.

It's also important (and mandated by the OIG) to have accountability over everything attached to the network, so that assets are inventoried and tracked. "Really leveraging some automated discovery solutions and being able to continuously learn about the assets that are on your network...truly will let you understand what is normal operation for those devices," said Willis.

Having a full picture of the asset landscape and building a comprehensive asset management program can help keep track of devices and avoid bad actor access. This is where automation comes in. "We all are struggling with a finite amount of resources, so really leveraging automation to where we can automate

tasks to detect and respond to minor incidents and some of the more repetitive ones allows our resources to focus on morbid things," Willis added.

Expanding on Cybersecurity's Primary Areas

Typically, cybersecurity involves preparing, detaching, responding and recovering. Willis, however, would add identifying to that list. "Add identifying your endpoint, your cloud access and data access," she said. "Really understand what access is needed at the right time, understand that business and understand the risks and the risk tolerance."

Protection involves ensuring the right safeguards are in place to keep critical infrastructure services and continuous monitoring running – like data loss prevention solutions, cloud security solutions and automation for incident detection.

Response plans should include a strong communication plan to relay information after an event has happened. It should also include educating stakeholders. "Recovering is making sure that you have a good recovery plan and external communications that go along with that to communicate with your stakeholders the recovery and impact of the cyber incident," Willis said.

For Gould, that response includes a playbook. "There's a lot of good resources out

there if you are just starting out or want to employ a more threat-centric approach. If you are not seeing threats every day, it is hard to understand when you see them, especially given the intense level of sophistication that we are seeing out there," he said. That is where those external threat resources can come in handy. They can give your teams an idea of what to look for without having to actually encounter a dangerous threat.

And automate as much as possible. Clear up lower-level tier tasks of detection, preparation and response actions. With thousands of events happening at any given time, let automation relieve the burden of what human brains can't physically track and free up security professionals' time. "The more we can do that as a society for private and public entities, I think the better off that we will be on the defensive side moving forward," Gould added.



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](https://Twitter.com/FedInsider)



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](https://Twitter.com/Carahsoft)



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

☎ (617) 444-3000
✉ Info@Akamai.com
🌐 Akamai.com
📘 [@AkamaiTechnologies](https://Facebook.com/AkamaiTechnologies)
🌐 LinkedIn.com/company/Akamai-Technologies
📱 [@Akamai](https://Twitter.com/Akamai)

© 2022 Hosky Communications, Inc. All rights reserved. FedInsider and the FedInsider logo, are trademarks or registered trademarks of Hosky Communications or its subsidiaries or affiliated companies in the United States and other countries. All other marks are the property of their respective owners.

