7 Ways to Sharpen Your Cyber Focus

Cyber experts like to point out that ransomware and related malicious activity have become a booming business, literally. A growing number of attacks are coming from cybercriminal groups and nation-state actors, both of which are well-organized and well-funded.

To make matters worse, experts say AI will make threat actors of all stripes more effective at devising attacks and adapting quickly to new defenses.

This is a tough environment for government agencies, said Michael Gregg, Chief Information Security Officer (CISO) for North Dakota. "We're always dealing with limited budgets, and that makes it very difficult for you to understand where to start and how best to use that money."

Gregg spoke at a recent GovLoop Virtual Summit, "Staying Ahead of the Cyber Curve: 7 Trends You Need to Know." Here are highlights from that event, in which the participants discussed strategies and tactics for responding to the changing threat landscape. (To view the two sessions on demand, click here and here.)

#1

Assess Your Cyber Maturity

Michael Gregg, CISO, North Dakota

In the same way that people are supposed to get an annual physical exam, North Dakota conducts a cyber maturity assessment every year, said Gregg. "We look across the state at the level of security we have, so we understand areas where we are weak and areas where we're strong," he said.

And just as a doctor reminds patients to focus on the basics — having a healthier diet and getting more exercise — Gregg said the security assessment results in a renewed effort to follow good cyber hygiene:

- **Endpoint detection and response**
- **Vulnerability remediation**
- **Patch management**

Another basic practice is security awareness training, he said. As simple as it sounds, the math is compelling. "You may have 30 or 40 people in your security department, but you've got 2,000 or 10,000 employees. You need all those employees to [know] if they see something, they say something, so they're engaged and involved," he explained.

Focus on Processes

Gregg recommends breaking your cyber strategy into three pieces: People, technology and processes. Although you generally don't get much leeway to increase spending on people and technology, there are no such constraints on processes.

"If you go through and look at your processes, many times what you can find [are] ways to optimize those processes to gain additional value and free up overhead," Gregg said.

#2

Rethink Cyber Recovery

Michael Carroll, Area Vice President of Sales, U.S. State, Local and Education, Commvault

When agencies turn their attention to cyber response and recovery, they might be unsure how to proceed, said Commvault's Michael Carroll. Many try to adapt their disaster recovery plans, but that generally doesn't work, he said.

For example, if a data center goes down during a storm, you shift your data and applications to a backup center. But that's not necessarily a good strategy in the event of a cyberattack. "That [would] assume the data's not corrupt, or that the bad actors aren't in the environment with their hands on the steering wheel," Carroll said.

To build an effective cyber response and recovery plan, you need to assemble a team representing all the stakeholders who would be involved following an incident: executives, departmental leaders, legislators, IT service providers, and IT and security teams, he said. Together, they can work out the appropriate response step by step.

Test Your Plan

The next stage of the process is more challenging, Carroll said: Test the plan. Because this is something organizations often struggle with, Commvault, whose data management and protection software supports disaster recovery operations, has a program called Minutes to Meltdown that helps customers stage simulated cyber events.

"Being able to test a cyber plan is an absolutely critical piece of the puzzle, and there are very few ways to do that and very few partners that you can work with [that] are both technically viable and cost-effective," Carroll said.

#3

Take a Methodical Approach to Zero Trust

John Kindervag, Chief Evangelist, Illumio

If you wanted a giant building to be fully secure, you'd have to protect each room. The same idea applies to zero-trust architecture.

"Zero trust starts with the data or assets you're trying to protect and designs the system outward," explained Illumio's John Kindervag, who is credited with defining the zero-trust approach in 2010 when he was a principal analyst at Forrester Research.

He has a five-step process for implementing zero trust:

- Determine the protect surface, which includes data, applications, assets and services (DAAS).
- Map the transaction flows, looking at how the different elements interact and how data flows through the network.
- Once you understand how the network works, you can create the zero-trust architecture, implementing the controls to safeguard your protect surface.
- Define the policies for enforcing zero trust.
- Monitor and maintain it.

Kindervag says the foundation of zero trust is network segmentation. The idea is to implement security controls within the network, breaking up the protect surface into "bite-sized chunks" that make it easier to control access to those DAAS elements. Seen from that perspective, "I think zero trust is not as difficult and as expensive as people have been led to believe," he said.

High-profile data breaches in the defense and intelligence communities have emphasized the importance of network segmentation, Kindervag said. Strong multifactor authentication protected those systems, but once they were compromised, "you got access to everything on the network."

#4

Secure Your Identities

James Imanian, Federal Technology Officer, and Gram Slingbaum, Solutions Engineering Manager for Public Sector, Cyberark

Traditional cybersecurity focused on firewalls and other perimeter protections — often called the moat-and-castle approach — but zero trust emphasizes something else: identity management. It is "the concept that every identity, not just the privileged identity, but the workforce, the developer, the machines … have to have the right set of intelligent privilege controls to be secure," said Cyberark's James Imanian.

He believes that agencies must account for three factors, or forces, when handling user access. First, organizations must consider that new identities are being created, including machines that talk to other machines on behalf of people.

Second, new environments are being established, especially as more agencies transition to the cloud while maintaining some on-premises infrastructure and as hybrid work takes hold.

And third, new threats have appeared, requiring a response. "As we've moved across these things — the new identities and new environments — adversaries are taking notice," Imanian said. "And they've evolved, and they've innovated."

The Least of Your Privileges

Bad actors want to steal administrator credentials, added Gram Slingbaum, also with Cyberark. "They don't want my account if all they can do is browse the web, but they do want my account if I have admin access to things," he said.

Adopting a least-privilege defense will limit user capabilities, and Cyberark helps agencies implement their privilege-focused strategies, he said. Agencies "get to the point where people are doing their jobs with the right level of permission," Slingbaum said.

#5

Craft Your Cyber Policies With Intent

Michael Toland, CISO, Oklahoma Office of Management and Enterprise Services

"Cyber policy is something we all love to hate," said Michael Toland of Oklahoma's Office of Management and Enterprise Services. "But we need them."

The trick to drafting an effective cyber policy, Toland said, is finding the "Goldilocks" position — neither so strict that people circumvent it to get their work done, nor so lax that it's meaningless. He's found that it comes down to three aspects of intent.

1. **Be clear about you why you are creating the policy.** "Knowing your intent can help you to write a policy that's clear and to the point, and doesn't confuse the audience," Toland said. If your intent is just to say no, people won't respect the rule.
2. **Look at the policy from the end user's perspective.** What's their intent? For example, you want to ban USB drives. But users need them because they're the only way to transfer files between necessary systems. "If I just write that policy and implement it today, we effectively shut them down," Toland said.
3. **Don't let a focus on enforcement distract you from your original purpose.** When you're asked to make an exception to the rule, find out why before you crack down. You may discover a better solution.

By following these guidelines, Toland said, "we're starting to write kinder, gentler policies — policies that are more empathetic to the end user. And [in return], they are less inclined to just ignore the policy and go around it."

#6

Focus on Measurability

Steve Faehl, Federal Security Chief Technology Officer, Microsoft Federal

In recent years, government agencies have developed strong security policies, most recently around zero trust. But here's the difficult part: How do you know if they work or if employees are following them? Increasingly, organizations are realizing that "publish and hope is not a security policy strategy," said Microsoft's Steve Faehl.

In fact, agencies need to assume that policies will fail or be ignored, he said, and so they need a way to constantly monitor their environment and measure performance. To do that, they need to look to data.

One approach is to deploy sensors that collect data on every aspect of the IT environment, giving the security team deep insights into the state of operations. The team also can tap into the log data that devices and systems on the network are constantly generating.

With the advances in sensor technology and analytic capabilities, including AI, agencies "have more tools at their disposal than they ever had before," Faehl said.

Bring in AI

AI models are embedded in Microsoft's endpoint detection and response clients, improving those tools' ability to detect indicators of potential insider-threat behavior. "Having that ensemble of models that can reason over human behavior and come back with great detections, high-quality detections is important," Faehl said.

#7

Get up to Speed on AI

Robert Imhof, Consulting Systems Architect, Fortinet Federal

AI is on its way to becoming an "essential technology and tool that every security professional will eventually need to master," said Fortinet Federal's Robert Imhof. "[It's] likely to have a very profound impact in cybersecurity operations due to its ability to automate and enhance security practices."

Seeing and analyzing patterns is AI's strong suit, so its first important cybersecurity applications will be detecting anomalies and remediating the threats it finds, Imhof said. It can review much more data far faster than humans can.

Agencies need to increase their use of defensive AI, he warned, because of the risk that bad actors will use the technology for their own ends. "State-sponsored attackers and other organized groups are weaponizing AI," Imhof said.

When you deploy AI-powered defensive products within your own networks, it's best to start slow, testing one innovation at a time, he said. Trying several new things at once makes it harder to determine what's working and what's not.

Train Up Your Staff

All new technologies have a learning curve, Imhof said, and security professionals will need training for AI. But learning to work with it may be the best way to quell fears that AI will take jobs. "Security professionals that can master utilizing AI in addition to their other technical skills are going to be highly sought after by employers," he said.

Click **here** and **here** to watch the two sessions on demand.