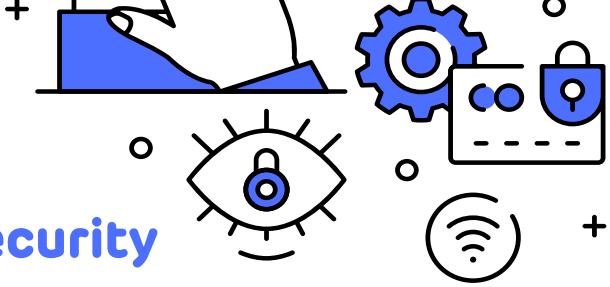


DON'T PANIC

5 Doable Ways to Improve Cybersecurity

Just when you think you understand cybersecurity, everything changes. In the case of cyber solutions, that change is always for the better, but it can still feel overwhelming.

One simple piece of advice: "Don't look at it and let that paralyze you," said Russell Marsh, Director of Cyber Operations in the Office of the Chief Information Officer at the National Nuclear Security Administration (NNSA).

Marsh and David Skyberg, Director for Product Management for Federal at Okta, spoke at a recent GovLoop virtual event, "Don't Fall Victim to Cyber Threats: Improving Upon Your Vulnerabilities."

Here are some takeaways from their discussion about how to make better security seem more manageable.

Focus on Identity

Good security begins with having the ability to authenticate the identity of any users (or systems) attempting to access your network resources.

Among other things, that's the basic premise for **zero-trust architecture**, said Skyberg, with Okta, which develops identity-based solutions. To determine whether someone is trustworthy or not, you need to know who they are, he said.

Another critical piece of zero trust is the concept of **least privilege**. The idea is that you should give people access only to those resources they absolutely need to do their jobs. But again, to enforce least privilege, you need to authenticate their identity.

"It all starts with a strong identity foundation," Skyberg said.

Make Security User-Friendly

Here's one of the inescapable truths of human nature when it comes to technology: If people find a tool or process too difficult or cumbersome, they'll find a work-around. In cybersecurity, such work-arounds open your agency's network or systems to malicious actors.

"You want an environment that's as user-friendly as possible," said Marsh with NNSA.

For example, one of the most common security vulnerabilities is a sticky note filled with passwords that hangs on the monitor. But this is a common sight in agencies where users are required to create and manage passwords for multiple applications.

Agencies can reduce that risk through a combination of two core solutions:

- **Multifactor authentication**, which requires a user to supply something beyond a password, such a code sent to a phone or a token of some sort
- **Single-sign-on technology**, which enables a user to sign in once and have their identity authenticated across multiple applications or systems

Build on Industry Advances

The good news is that security vendors and industry groups are developing strategies and standards for improving security without making life difficult for end users.

For example, the Fast Identity Online (FIDO) Alliance has been working on ways to make it easier for end-users to authenticate their identity beyond the use of passwords. The latest standard, FIDO2 (WebAuthn), makes it easier to incorporate the use of **biometrics**, such as fingerprints, including on mobile devices.

Another advance: **continuous access evaluation**. Once a user signs into a system, how long should that session last before they need to sign on again? The longer the session, the greater the chance that security could be compromised. One emerging solution is to continually monitor session activity for anomalous behavior and to end a session if any is detected.

These are examples of technology that "takes the burden off our users and puts it on our infrastructure," Skyberg said.

Get Ready for AI

Over the next couple of years, some of the biggest advances are likely to come from the use of **artificial intelligence** (AI) and **machine learning**.

For example, most devices and systems on a network generate a steady stream of data on everything that happens. IT and security teams can use those logs to troubleshoot problems or investigate security incidents. The Biden administration's May 2021 executive order on cybersecurity and related memorandum directed agencies to maintain system logs. But how do you actually get insight out of all that data?

"Artificial intelligence hopefully will help pick out patterns and things to investigate much quicker than a human could," said Marsh.

AI and machine learning also could help agencies detect the presence of malicious actors on a network before they can do any damage.

But to take advantage of AI, agencies need employees with enough knowledge both to select the right tools and to use them effectively, which could be a challenge for agencies with small training budgets, he said.

Don't Panic, Just Plan

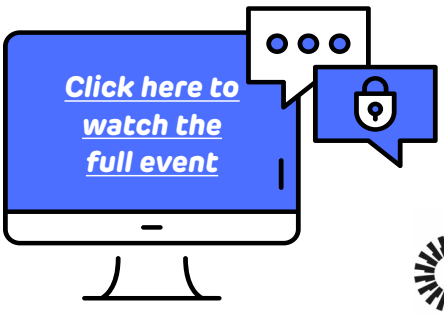
Recent advances in cybersecurity technology and strategies are promising but also come with a steep learning curve. But don't be daunted.

Zero trust, for example, is a complex undertaking, but you don't have to tackle it all at once, Skyberg advised. In fact, the Cybersecurity and Infrastructure Security Agency has published a zero trust maturity model that can serve as a roadmap.

"Recognize that step one is ensuring that you've got strong identity infrastructure, and build on top of that, one step at a time, throughout the maturity model, and you will get there," he said.

Marsh agreed that there's no point in thinking too far ahead or worrying about what you can't do. **"Whether you think you don't have the money, you don't have the resources, whatever, just lay everything out, start with a plan,"** Skyberg said.

"A lot of times I'll tell people, even if we can't get everything done, we're going document what we did and why we did it, and what we didn't do, and why we didn't do it," he said. "And before you know it, you'll actually make some significant progress and work your through that maturity model."



govloop

okta