Leaders Agree that Cybersecurity is About People

Endpoint users will always be the weak link in cybersecurity. How do we mitigate the risk?

James Mersol

Mon, 09/09/2019 - 09:36

Photo credit: metamorworks/iStock

No matter how robust your cybersecurity controls are, one user incident could compromise your entire network. This dire warning — and more importantly, the solutions to it — was a running theme among cybersecurity leaders this week.

“When it comes down to protecting our systems and information,” said Federal Chief Information Security Officer Grant Schneider at the Billington Cybersecurity Summit Wednesday, “it really is about the people.”

Schneider explained that his three main priorities for his office are risk management, workforce and training, and compliance and federal regulation. Two of those, he said, require federal agencies to focus on its people from strategic planning to implementation.

The call was not for security professionals to rethink their vulnerabilities, but instead for everyone in every organization, from C-suite to contractor, to recognize their risk and train personnel on how to recognize and avoid threats.

“If you are using a phone, if you are using a computer, you are a cyber operator,” said Gregory Touhill, former federal chief information security officer who served in the role in 2016, “you are a target.”

In one breakout session, international cybersecurity experts and leads from top cybersecurity firms simulated a ransomware attack on an app developer and cosmetics company. Rather than discuss the decision-making process for the company’s incident response team, the participants played the role of the C-suite, asking the questions executive leadership ought to if found in the same situation, ranging from, “How long would it take to recover our system from backups?” to “Do we have a company bitcoin account if we decide to pay the ransom?”

As the participants chose not to pay even as the number of compromised systems and ransom demands grew, the scenario — modeled after a real attack, down to the amount of bitcoin the attacker demanded — eventually affected distributors and customers, and both law enforcement and regulatory authorities became involved.

Moreover, the incident required input from stakeholders not typically associated with cybersecurity, including the chief financial officer and marketing and public relations teams. In the end, though, even those stakeholders could not effectively mitigate the damage from a ransomware attack.

“The key takeaway is ‘protection up front,’” said Juliana Vida, chief technical advisor for Splunk who served as one of the participants. She advised that every agency needs to have a plan in place and act upon it to protect their systems ahead of ransomware, including a risk calculation put in terms that everyone in the company understands.

“If I tell you there’s a 100% chance your phone is going to be compromised,” Vida said in a subsequent interview, “that doesn’t mean something in the same way it would if I told you there was a 100% chance a tree was going to fall on your house.”

Educating everyone about security is especially important as paradigms surrounding cybersecurity shift. Traditionally, experts thought of a strong perimeter as the most important way to defend critical networks and systems.

“I think everyone has had this false sense of security about the perimeter,” said Sylvia Burns, deputy CIO for enterprise strategy at FDIC. “If you have one phishing attack, your entire network is compromised.”

Instead, cybersecurity experts have realigned their emphasis toward a zero-trust philosophy and continuous detection and monitoring to ensure that cybersecurity teams know who and what is on the network at all times. In the end, though, it comes back to the people.

“We’re trying to build systems that are more cognizant about how people operate,” said John Zangardi, chief information officer at the Department of Homeland Security . This effort has included “training days” for all staff at DHS, the first of which focused on teaching employees about cloud migration and related concepts and terms. The next training session will focus on “Cybersecurity 101,” and the final one will be just for IT and cybersecurity employees to ensure they’re up to date on the newest threats and ways to mitigate their impact as well as check to see that all staff’s credentials and certifications are up to date.

View printer friendly version
workforce
ransomware
cybersecurity
DHS
federal CISO
Standard