CXO FOCUS

ACCELERATE A CULTURE OF TRUST

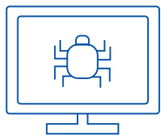
CISO SAYS EXERCISES, COMMUNICATIONS AND COLLABORATION ARE AS VITAL AS TECHNOLOGY IN THE FIGHT AGAINST CYBERCRIMINALS

—

JUNE 2023

POWERED BY

NUTANIX



“The internet is an accelerator for evil and the bad guys are using this against us”

Said Dan Lohrmann, field CISO with Presidio, the cloud services company. The acceleration of internet usage, cloud computing and data levels that have occurred since the COVID-19 pandemic have increased cybersecurity threats as well as awareness.

As organizations deal with the rising cybersecurity threat, it is important for business technology leaders to create the right culture, define responsibilities, and prepare for an attack and for recovery.

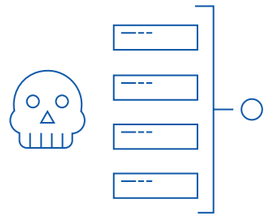
“It got personal when a six-year-old asks about the lines at the gas stations, and you have to explain ransomware to children,” Lohrmann said of how the Colonial Pipeline attack of 2021 followed the SolarWinds attack a year before.

These have made cybersecurity a broadly understood issue. “There is a doubling of incidents each year, and the number of incidents has skyrocketed,” he said of the post-COVID environment.

Despite the rising awareness, the senior leadership team of organizations needs a high level of education on the risks that cybersecurity attacks pose to the business.

“A lot of executives don’t want to do an exploration of their risks because once you know something exists, then you have to do something about it,” Lohrmann said. One organization that did was shocked by its discovery.

“We had a disruption last year that shut down our network for one of our datacenters for 18 hours”



A secure culture

The right technology is only part of the solution. As the airport example demonstrates, this organization did not have a culture that encouraged its staff to consider the security risks of where they saved forms, staff records and schedules, thus exposing the airport to potential cyberthreats.

“How you react, respond and learn from incidents is about the culture and values of the organization,” Lohrmann said.

Joshua Surre, assistant vice president of infrastructure and operations at HCA Healthcare, agreed. “We had a disruption last year that shut down our network for one of our datacenters for 18 hours,” he said. “So let’s figure out the lessons from that, as we are an essential service.”

Surre explained that HCA Healthcare analyzed the incident to ensure it protected itself more effectively in the future.

“Cybersecurity is a business risk issue, not just an IT issue, and supply chain attacks are opening people’s eyes”

Lohrmann explained that “An Asian airport looked at all its data and did a full risk assessment, and what they found is completed security forms that would grant access to the airport, staff records, schedules, all on servers across Asia, Europe, and the USA. It was a roadmap for a terrorist organization to attack the airport.”

“Cybersecurity is a business risk issue, not just an IT issue, and supply chain attacks are opening people’s eyes,” he added. There is a major push by the U.S. government to adopt zero-trust security technology, something Lohrmann ardently supports.

Lohrmann concurred, adding that “When you have after-incident reports, make sure that you act on them. Act and adjust as the situation evolves. Do people know their roles and responsibilities when an attack hits, and do they know how to communicate in this situation?”

It is essential for organizations to clearly set out who takes charge of what and the processes they follow when a cyberattack happens, Lohrmann advised. He noted that effective cybersecurity responses use the same methods as a physical emergency.

“Think of it the same way as would a fire and flood,” he pointed out. Lohrmann learned this from personal experience when he was CSO for the State of Michigan, which suffered a major power outage in 2003.

During that event, two-thirds of the critical people who needed to respond were not available due to holidays, family commitments or the power outage. He says this can be a typical situation and that organizations must prepare for a cyberattack with the knowledge that they can strike on days when critical staff members are not available.

Prepared for attack

“Many firms have carried out tabletop exercises and thought they were ready for an attack,” Lohrmann says. Typically, these attack exercises feature all team members, and the CISO says more organizations should take team members out of the exercise to better reflect reality.

Preventing an attack and its severity is one aspect of cybersecurity. Organizations must also have a strategy and practices in place to recover from an attack.

“If attackers encrypt your devices and your backup data, then you cannot recover,” Surre said. “So how do you make your backup data immutable? What can I do to air-gap the backup data so that it’s in an isolated data vault? And how can I provide services from an isolated recovery environment?”

Surre emphasized that it is imperative for the business technology leadership to ask these questions. “There is so much to unpack that it goes beyond an immutable copy of your data,” he added.

“The other side of the conversation is differentiating between business continuity and cyber-recovery,” Surre said of translating the two differing demands to the non-technical members of the senior leadership team.

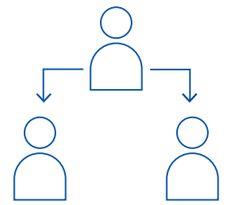
He advised CXO peers to discuss recovery times and plans and to gauge how they feel about the time it takes to recover. That discussion must also break down the technology estate and explore what are essential services in the face of a cyberattack.

“What is it about my business that I care about?” he asked. “It cannot be everything, so you have to know what your essential services are.”

There is another cultural change that CISOs must initiate and lead if they are to protect organizations. Lohrmann cautioned that if a CISO’s department garners a reputation of saying “no” too often, it won’t gain the trust that is required when a cyberattack takes place.

> The other side of the conversation is differentiating between business continuity and cyber-recovery”

> In an emergency, if you are viewed as the no guy, then they will question how you can lead.”



“We have to be enablers, and it will be the same for ChatGPT, cloud computing and the internet-of-things,”Lohrmann said. “In an emergency, if you are viewed as the no guy, then they will question how you can lead.”

Business and security leaders that create a culture of trust and collaboration will be able to deal more effectively with the rising tide of cybersecurity threats to the enterprise.

KEEP UP TO SPEED
WITH THE LATEST CONTENT

NUTANIX.COM/CXO