Cybersecurity

Cybersecurity: Be sure to practice incident response

One of the common errors that often gets discovered during such an exercise is the manager who states that the responsibility for a certain task would fall to an employee who's not in the room—and that person has no idea of his expected duty

Carl Ayers - March 28 2025

It makes little sense to have a plan if you never practice it.

Given the prevalence of cyber bad guys, it's wise to conduct at least a tabletop exercise periodically to test how your incident response plan would work in the event of a breach.

Not my job

One of the common errors that often gets discovered during such an exercise is the manager who states that the responsibility for a certain task would fall to an employee who's not in the room—and that person has no idea of his expected duty.

"That's what practicing does. It lets everyone know" what their roles are, says **Joshua Cook**, a cybersecurity attorney with the **Wagner Law group** in Boston.

Words to live by

Cook wrote the book, ***Cyber Resilience by Design: The Executive's Guide to Managing a Cyberattack***, and spoke with ***RCW*** after conducting a recent cybersecurity webinar.

"When everyone knows what their responsibilities are, that friction" that can challenge a successful incident response plan disappears, he adds.

"[redacted]ttacks are incredibly cheap to pull off and they can be incredibly e[redacted]ve" to firms, he said during the webinar. "If you're ready for an attack, you could probably make it through it."

Practicing your incident response plan is "the simplest thing any business can do to get ready and handle an attack," he continued. The costs of an attack can cripple a firm. In 2023 alone, cyber bad guys cost U.S. businesses $2.9B in losses, he noted.

The continuing trend of working from home comes into play as well. A firm's incident response plan may work well for the main office but fail for a remote location or a staffer's home. "They need an incident response plan themselves," he contends. It would basically spell out actions to take for a suspected breach.

Ubiquitous phishing

Emails through phishing provide the most prevalent means of attack. "It is shocking how easy it is for bad guys to get into enterprise email systems," he said. "Phishing is ubiquitous." It's cheap "and it works" because humans often make mistakes in opening emails designed electronically to detonate, he continued.

Another way bad guys burrow into a business's system is when smart precautions aren't taken. He told a real-life story of a firm that unveiled a new enterprise system, which required new access credentials. The firm initially assigned everyone the same password "Welcome1."

"The bad guys figured that out," he said. While staffers logging in for the first time were prompted to change that password, some never did because Welcome1 continued to work—leaving the electronic doors open to the cyber bad guys. The lesson: Require new computer systems to force an employee to input new, strong passwords.

The role of the CCO

Years ago, a CCO could get away with delegating cybersecurity to an IT expert. Cook doesn't believe this satisfies regulators anymore. Now, "the CCO needs to really be conversive" in cybersecurity and the terminology, he tells *RCW*.

Examiners "don't want to see the CCO defer to a so-called expert," he asserts.

To bolster your cyber knowledge, begin by quizzing your internal resources, perhaps your chief information security officer, if your firm has one. "Talk to that person," he advises. "The two should be working together very frequently."

Be cautious about remote hires

An emerging cybersecurity risk detailed by Cook originates in North Korea. IT personnel there will apply for remote jobs overseas and pose as ideal candidates without divulging their true location.

"They will work that job remotely. They'll be in North Korea but the laptop that the company ships out to them will be in a server farm in the Philippines, India or somewhere else," he says. "They'll do the job for a while," collect a paycheck while all the time plotting to "exploit the environment" for a future cyberattack.

During an SEC exam, be prepared to show your written incident response plan. "Examiners are looking for thoughtfulness," meaning a plan tailored to your firm's actual risks and not some off-the-shelf solution, he contends.

Here are other cyber tips he suggests:

- Ensure your plan includes backup communications should your email system go down. Phone and text may be the best method to stay in touch with staff and clients. He recommends using Signal, which offers encryption "end-to-end."
- Know ahead of a breach how your notification process would work and "who is actually signing that letter" that alerts clients to the incident.
- Be aware that cyber bad guys prefer to strike on nights, weekends and holidays, believing firms are especially vulnerable at these times.
- Don't be surprised if your cyber insurance doesn't cover all you expect it to. But you could turn to your insurer ahead of time for recommendations to great resources and experts who may be able to help you strengthen your program.
- Turn to the federal government's Cybersecurity & Infrastructure Security Agency (CISA) for more resources.
- Instruct staff not to use free Wi-Fi sites on their laptops when traveling. "That is a red flag" when invited to use a Wi-Fi that lacks password protection.

"If you just make yourself a harder target," you'll reduce your threats, he believes. Then the bad guys are more likely to "move on to somebody else."

What do you think about this story? Please, share your thoughts with Publisher ***Carl Ayers****.*