Hey! What's New? 2025-5

Ransomware Threat: Finance's 4-Part Defense Role

Andrew Kenney notes, in a recent issue of *FM Financial Management*, that "ransomware attacks are some of the most concerning for experts in the finance and cybersecurity spheres," noting that Allison Ward, CPA, a US-based partner with CapinTech, a CapinCrouse company that specializes in cyber consulting says that "ransomware is probably one of the things that keeps me up most at night."

Kenney explains that ransomware attackers breach corporate networks and use encryption software to digitally lock files and data, making it impossible for victims to use their own information, and then hold the company's data hostage. As the victim scrambles for a solution, the attackers make an offer: If the company pays a ransom, its files will be unlocked.

It can be an especially lucrative method of attack, he adds, "since the hackers are extorting money directly from their victims instead of needing to find a third-party customer for stolen data. And they are targeting companies of all sizes."

According to Kenney, here's how companies can strengthen their defenses, create a culture of security and prepare for the worst.

Assess and maintain technological defenses: Finance is a common target for cyberattacks, as it manages valuable data and important software systems. In addition, the CFO may hold or share responsibility for maintaining security technology and protocols, said Tin Lau, FCMA, CGMA, chief risk officer for Mirae Asset Securities in London."

It's key that finance leaders take responsibility, determining who owns key systems and responding appropriately, says Darron Sun, FCMA, CGMA, CPA (Australia). "That means keeping software up to date to fix known vulnerabilities; ensuring that firewalls and detection systems are in place; and employing experts to probe for vulnerabilities. Finance leaders should also ensure that backups of sensitive data are kept in multiple places, preferably including a backup option that is not connected to the company network or the internet."

Train staff to prevent attacks: Digital defenses stop only some attacks. In other cases, attackers use tactics to trick employees into taking actions that compromise security. Kasun Premechandra, who is based in Sri Lanka and leads portfolio management for the Finance Change division of the London Stock Exchange Group, says that "attacks commonly start with phishing attempts — fake messages that contain files or links that will allow the attackers onto the network if they are activated by the user."

These days the attackers may use generative AI to create fake video or audio messages from executives, or convincingly customized emails, that urge employees to download a file or click a link. “All it takes is one person to get busy, fall for a voice attack and disclose their MFA [multi-factor authentication] code, and the bad actor has access.”

According to Premechandra, “the strongest defense is to train individual employees to identify and reject phishing attempts. Training exercises can help them learn the telltale signs of an attempted attack. The goal of these tests and training is to create a culture where each employee understands that security is their responsibility — a process that begins at onboarding and continues throughout a worker’s tenure. It’s all about training, bringing awareness, and then empowering the staff so that they can be a human firewall, so that they will think for themselves, and then they will prevent threats from reaching the organization.”

Plan for the worst: Every company has to consider the possibility that, despite preventive efforts, their data will eventually be held hostage, Kenney points out. “One way to prepare is to improve the company’s data backup strategy. In the event of an attack, a well-prepared company might be able to simply restore backup data instead of paying the ransom to unlock the compromised data. But it’s key to keep these backups separate from operational systems, since the attackers will aim to lock or destroy any backups they find. Leaders also should think carefully about what data to back up — attackers may target unexpected but important information, such as contact information databases of employees.” He adds that “it may be appropriate to keep response plan documentation totally isolated from the company network so that it’s not revealed to attackers.”

Paying the attackers is a last resort, Kenney’s experts stressed. “Giving money to attackers gives them more resources and motivation to continue their attacks. They may even return to the same victim later. The real question — and the way that finance leaders may ultimately be judged — is how well teams have trained for and responded to the crisis.”

For a whole lot more advice, check out Ransomware threat: Finance’s 4-part defence role.