New Cyberattacks: The Threat Is Real

The headlines alone can be nerve-racking. In March, a hack forced one of Australia's biggest broadcasters off the air. Two weeks ago, a hack crippled a major US oil pipeline. And this week, a hack shut down operations in several countries of one of the world's largest meatpackers.

At a time when organizations might deal with everything from mounting supply shortages to continued pandemic safety concerns, the last thing any C-suite needs is to fret about mounting cybersecurity attacks. And yet experts agree that other significant disruptions are on the way, that all organizations are vulnerable, and that there is no foolproof defense. "It's only going to get worse," says Craig Stephenson, Korn Ferry's managing director for the North America Chief Technology Officers practice.

By some estimates, a hack attempt occurs every 39 seconds, and the proliferation of internet-connected devices, organizations relying on old software, and even the increase of people working remotely will make it more challenging to squash all the attempts. Indeed, as the major hack of the US Department of Defense exposed last year, an organization can vigorously check its computer systems internally and still end up with externally purchased software that has been compromised. "Rather than companies securing their own perimeter, they need to secure an ecosystem," says Freddie Montagu, a principal in Korn Ferry's EMEA Technology Officers practice and a specialist in cybersecurity.

Normally, hackers will threaten to shut down an organization's digital systems unless paid a ransom. The amount given to hackers—or adversaries, as they are called in the cybersecurity industry—is also on the rise. While individual ransom attempts vary wildly, Coveware, a ransomware-negotiation firm, reported that the average payout was $220,298 in the first quarter of 2021, up 43% from the previous quarter and close to the record high hit in the third quarter of 2020. The firm says hackers almost always deliver a decryption tool to the hostage companies or organizations once the ransom is paid. The United States government does not encourage organizations to pay a ransom, but many organizations do.

These days, most chief information security officers are realistic, says Tarun Inuganti, head of Korn Ferry's global Technology Officers practice. "They say a hack is going to happen," he says, adding that it's up to the firm's top technology executives to alert the board of the risks and the potential impact of a successful hack. It's why these days, one of the most prized skills in chief information security officers isn't their ability to code or find the right software package but working with the C-suite and even the board to understand the issue.

Experts say it is primarily boards—not just management—that will have to step up, since directors must oversee the overall corporate risk and weigh the firm's tolerance for it. To do that, they will need to understand that cybersecurity isn't a problem that can be solved by throwing money or people at it. Some forward-thinking boards have added chief technology officers or chief information security officers as directors, a move that can help highlight not only the risks of cybercrime but help the entire board and management determine how much risk they are willing to take, Stephenson says.

To be sure, realizing your organization will get hacked doesn't mean that a firm should just roll out the red carpet for the perpetrators. Security officers and other executives need to ensure all employees are trained to use basic security methods, such as logging in using two-factor identification and not opening strange-looking emails. ("If you don't know it, delete it," Inuganti says.)