By Dave Zielinski

October 14, 2023

CEOs rise to their positions because of the breadth and depth of their expertise in areas such as strategic planning, finance, marketing, negotiations and communications.

But recent research suggests there's a troubling gap in CEOs' extensive skill sets that's placing their organizations at risk: how to prepare and respond to the increasingly menacing problem of cybercrime.

Cybercrime has emerged as a major threat to the continued health and profitability of businesses across industries. It even made the World Economic Forum's list of the top 10 most severe global risks to organizations over the next decade.

In one of the latest examples of the havoc cybercrime can cause, Las Vegas-based casino company MGM Resorts shut down its computers for 10 days in September to shield its data from a cyberattack, according to an Associated Press report. Earlier that month, Reno, Nev.-based casino operator Caesars Entertainment paid a $15 million ransom to a cybergroup that disrupted its systems, multiple news outlets reported.

The research group Cybersecurity Ventures reports that the financial impact from global cybercrime will hit $10.5 trillion annually by 2025, more than triple the $3 trillion impact in 2015. There has also been a 67 percent increase in ransomware cases in the first six months of this year compared to the same period in 2022, according to NCC Group's latest Cyber Threat Intelligence Report.

Organizations of all stripes face increasingly sophisticated and relentless cyberattacks in the form of ransomware, phishing, business email compromise, crypto crime and other tactics that not only can cost millions and take out operations for extended periods, but even put some companies out of business. Countermeasures put in place by top-notch IT security teams are now regularly rendered obsolete by cybercriminals who perpetually operate one step ahead.

CEOs forced to contend with this mushrooming problem often have significant gaps in their education and flawed perceptions about how best to address cybercrime, according to the *CEO Report on Cyber Resilience* from the University of Oxford's Said Business School and Istari, a Singapore-based cybersecurity company.

The study found that CEOs too often focus on trying to prevent cyberattacks at the expense of building resilience, or funneling time and resources into planning how to

quickly respond and recover from attacks once they happen. Successful cyberattacks in today's technology-dependent business environments are inevitable, the study found, and CEOs and their security teams should focus more on how to limit the damage once they occur.

"It's an overly narrow framing of today's cyber risk landscape because it implies that always protecting the availability, integrity and confidentiality of computer systems and data is achievable," the *CEO Report*'s authors wrote. "That simply is not the case. It also implies that a possible solution to the problem of cyber insecurity is purely technical in nature."

The study found that CEOs feel more discomfort in making decisions about cybersecurity than in most other areas of their business. Some 72 percent of survey respondents said "no" when asked if they feel comfortable making decisions in the area of cybersecurity, in large part because of the perceived technical complexity.

But many CEOs also said they had issues trusting those around them—including chief information security officers (CISOs) and their IT security teams—to make good decisions about preventing cybercrime or responding effectively once attacks happen.

Cybersecurity experts say that while using state-of-the-art methods and tools such as artificial intelligence to prevent external cyberattacks remains vital, allocating too much budget or executive attention to trying to thwart attacks at the expense of response planning is a dubious business strategy.

"It's inevitable that cybercriminals are going to break into systems," says Chris Scott, managing partner of Unit 42 at Palo Alto Networks, a global cybersecurity company based in Santa Clara, Calif. "There are millions of lines of code out there, and they all have some vulnerabilities. CEOs should understand that it's only a matter of time before bad actors will find holes in organizational systems."

Jay Preall, a senior consultant in the technology consulting practice at Segal, a New York City-based advisory firm, agrees that CEOs and CISOs who focus too much on prevention while giving short shrift to post-attack planning are courting trouble.

"No organization has enough expertise or money to prevent every cyberattack," Preall says. "I encourage CEOs to think about it like Newton's third law: 'For every action, there is an opposite and equal reaction.' Every time an IT security team figures out how to stop a certain type of cyberattack, there is an equal and opposite reaction from hackers in terms of, 'OK, let's invent a new form of attack.' "

Preall also believes many CEOs fail to grasp the true gravity of the problem, even with cyberattacks now regularly in the news.

"What many CEOs don't realize is these attacks are automated and relentless now," he says. "These are not just lone-wolf hackers out there banging away on keyboards. These are sophisticated criminals running automated scripts. They are constantly scanning the internet looking for vulnerabilities. The idea that most of these hackers will be brought to justice and that the cyberattacks will stop is not reality."

Build Resilience

To limit the financial and public relations damage from a successful cyberattack, experts say that CEOs must not only deepen their knowledge of how their organization's critical technology infrastructure is protected from such attacks. They also should become more active and engaged participants in creating and rehearsing a preparedness strategy.

That begins with learning to trust CISOs, IT departments and supply chain teams in new ways. It also means having the humility to ask questions about the workings of security practices, which can be difficult for CEOs who are unaccustomed to showing anything less than mastery-level knowledge of business operations. The technical nature of cybercrimes makes this kind of crisis more challenging to CEOs, who often have a higher level of comfort around problem-solving related to finance, operations or marketing, the *CEO Report* found.

"CEOs need to ask more questions of their IT and security leadership around how the changing threat landscape introduces risk to their organizations," says Paul Furtado, a vice president analyst with Stamford, Conn.-based research and advisory company Gartner. "CEOs need to be challenging their teams by asking, 'What are you hearing about how emerging technologies like generative AI or quantum computing can impact our security environment?' "

Preparedness or "incident response" plans should help CEOs think through the division of labor among company leadership when a cyberattack hits, experts say.

"CEOs should know what decisions they'll need to make on their own during a crisis and how much they'll be delegating to their teams," Scott says. "They need to know what information they'll need from the CISO to understand the situation, which will allow the CEO to focus more externally as needed and respond to things like requests from the media or analysts about the situation."

CEOs also need to fully understand their business risks from operational, financial, legal and reputational perspectives, should their organization experience a serious cyberattack, experts say.

"Cybersecurity is a business problem, not an IT problem," Furtado says. "But there are still many CEOs and organizations that treat it as an IT-only problem."

Understanding threats to the business requires that CEOs be much more than the public face of the organization during a cyberattack—they also need an active and ongoing role in rehearsing instant response plans through activities such as tabletop exercises, cybersecurity experts say.

"From an operational perspective, for example, what will happen if payroll, accounting or customer service is shut down?" Preall says. "One company we know of had a large cyberattack and watched its customer service call center go from handling a few hundred calls a day to 1,000 calls a day, coming from concerned and angry clients. Is your company prepared to respond to that? Has it created good manual backup systems for critical technologies? There are a lot of contingencies to plan for."

Good incident response planning also goes far beyond just creating a solid strategy.

"Documentation is not the same as preparation," Preall says. "You might have a very well-documented instant response plan in place, but if you never test it or practice it, your actual response won't be nearly as effective. People need to practice so they know instinctively what to do in these situations. Every second you delay in the case of events like ransomware attacks can get you deeper into a hole."

CEOs also need to understand they'll often be "managing blind" through the early stages of a cyberattack, experts say.

"When the crisis begins, there will be a period of time when the CEO is operating with a lot of unknowns," Scott says. "They'll have to make a lot of decisions with incomplete information and without perfect answers. It takes time to do things like forensics, to dig down through computer logs and more, to understand what really happened during a cyberattack, before you can make decisions."

While boards of directors have long been interested in the C-suite's cybersecurity strategy, given boards' core oversight and fiduciary duties, a new rule issued by the U.S. Securities and Exchange Commission (SEC) in July 2023 is likely to heighten that interest and engagement even further—and raise expectations for how CEOs report to boards on their companies' cybersecurity strategies and practices.

The SEC rule requires companies to disclose material cybersecurity incidents they experience within four business days of occurrence and also disclose on a yearly basis "material information" concerning their cybersecurity risk management, strategy and governance practices. The disclosures will be due beginning with annual reports for fiscal

years ending on or after Dec. 15, 2023.

Amy de La Lama, a partner with law firm Bryan Cave Leighton Paisner in Boulder, Colo., and chair of its global data privacy and security practice, says the new SEC rule will cause boards to give even greater scrutiny to how CEOs and chief information security officers create prevention and instant response plans related to cybercrime.

"I think boards will be increasingly more interested and concerned about how organizations are preparing for cyberattacks, and CEOs should be prepared to start reporting and engaging boards in much greater detail on that," de La Lama says.

Paul Furtado, a vice president analyst with Gartner, says the new regulatory requirements should give CEOs even more incentive to educate themselves on cybercrime issues and build cybersecurity preparedness programs that stand up to board and investor scrutiny.

"The SEC rule changes also create mandatory regulatory accountability at the board level," Furtado says. "That elevates the cybersecurity question into the highest level in a company: the boardroom." —D.Z.

Prepare and Protect

Creating an effective response strategy also depends on a CEO empowering an organization to respond in nimble and decisive ways. For example, requiring employees to get approval up the chain of command to take certain actions can lead to costly delays that worsen the impact of cyberattacks.

"A good example is if someone detects something suspicious going on with the endpoint on a manager's laptop, would the CEO empower the CISO or his or her security team to isolate that endpoint and quickly figure out what happened?" Scott says. "Or would policy not allow them to immediately isolate the laptop, leading to delays that could allow an attacker to move into the broader company environment and cause more problems? Some of the biggest damage during cyberattacks happens when companies don't respond quickly in that fashion."

Scott says organizations need to accept there may be "false positives" in such scenarios.

"That is a risk you often have to take," he says. "What's the level of impact employees are allowed to have to try to stop an attack early, knowing sometimes they'll make the wrong call? Finding the proper balance in such scenarios can come from a CEO's leadership."

Experts say that CEOs also need to ensure their organizations have the right level of cyber insurance to limit the impacts of cyberattacks—and be prepared to pay more for it, since the insurance has grown more costly in recent years in many industries as a result of the growing number and severity of cyberattacks.

The global average cost of a single data breach reached $4.45 million in 2023, a 15 percent increase over the last three years, according to research from the Ponemon Institute and IBM.

"These attacks can be immensely expensive," Preall says, referring to both the tangible and intangible costs of cybercrime. "CEOs will often read media reports about the huge costs companies incur from cyberattacks and not believe them. But the costs quickly add up. There are investigation and legal fees, employee overtime costs, regulatory fines, consultant fees, a need to replace technology or equipment, and much more. Cyber insurance can help offset some of those costs."

Don't Deflect

Furtado says few CEOs lose their jobs because their company was the target of a successful cyberattack—but how these executives go about preparing their organizations to withstand and respond to inevitable attacks can make them more vulnerable to action by a board of directors.

"We've seen a growing number of CEOs and top IT leaders lose their jobs because of how they responded to a cyber event, not because they were attacked," he says.

Furtado points to the case of former Equifax CEO Richard F. Smith, who in 2017 retired under pressure in the wake of a massive data breach at the credit reporting company that exposed the personally identifiable data of almost 150 million Americans.

Although Smith initially retired soon after the breach, *The New York Times* reported that the Equifax board "took an unusual step that reflected the damage from the breach, saying it could retroactively classify Mr. Smith as having been fired for cause." The *Times* reported that after the cyberattack, Smith "sought to play down the severity of the problems that led to the breach and deflected questions about how far Equifax would go to compensate consumers who were financially harmed" when he was forced to testify before Congress about the cyberattack.

"The court of public opinion is no longer tolerant of executives who aren't prioritizing a security mindset in any business operation," Furtado says. "That doesn't stop with the CISO. It goes straight up to the CEO."

Dave Zielinski is a freelance business journalist in Minneapolis.