CORPORATE COUNSEL
An ALM Website
corpcounsel.com | May 31, 2018

Prepared for the Hack: Demystifying Cybersecurity for Corporate Executives

Many executives are less comfortable confronting cybersecurity risks than they might be with other corporate issues.

By Lynn Haaland and Paul Rosen

Executives at even the most sophisticated companies are understandably worried they haven't done enough to prevent or prepare for a cyberattack. And the stakes are high: loss of proprietary data and consumer information, potential government enforcement and plaintiff actions, as well as reputational harm. But many executives are less comfortable confronting cybersecurity risks than they might be with other corporate issues.

Photo: Shutterstock

Their concerns coalesce around three realities: cybersecurity is a constantly evolving landscape, and the threat actors and vectors are constantly changing; cybersecurity can seem like a technically complex and overwhelming topic to master, even for business leaders; and companies and government agencies with all the resources in the world are getting hacked.

These realities have led some executives to delegate important tasks and key oversight out of a concern that the issues and answers are so technical that only experts in the field would truly understand them. In doing so, some companies have not yet achieved meaningful integration of cybersecurity into their corporate governance, business continuity, and security plans.

However, executives can and must play an integrated role in their company's cybersecurity. Gone are the days that cybersecurity can be relegated to the IT department; it is now a C-suite and board issue that requires corporatewide attention. By asking the right questions and following a risk-based roadmap for prevention and response, executives can better protect their compa-

nies, customers and shareholders. These steps can help:

First, learn the basics. You don't have to be a coder to play a meaningful role in your company's cybersecurity efforts. But you should take reasonable steps to learn the foundational elements of cybersecurity, including the threat actors (e.g., nation-states, criminals, vandals); the common types of attacks (e.g., phishing, unpatched software vulnerabilities); and various ways companies and organizations can protect themselves (e.g., regular backups, encryption, network segmentation, limiting administrative access, multifactor authentication).

Second, identify your crown jewels and understand your network. It is important to have a basic understanding of what kind of sensitive information your network possesses and how your systems store or transmit that information. For example, a financial institution may be holding sensitive data, like Social Security numbers or account numbers for millions of customers. Similarly, a health care company may have protected health information, detailing the most personal health information of its customers. Or, a bourgeoning tech company may store its valuable algorithm on its network, perhaps leaving it exposed. Whatever the corporate crown jewels may be, knowing what they are and how your network operates to protect them is key.

Sometimes protecting your own data and systems isn't enough. Businesses often rely on third-party vendors to transfer or store sensitive data. Cybersecurity and legal teams need to be involved in vetting and selecting contractors and vendors, as well as conducting cyber due diligence in acquisitions. Companies must develop a business structure that gets necessary information to the cybersecurity team in near real time, while at the same time ensuring that executives are sufficiently educated on the threats.

Third, formulate and ask the hard questions to assess legal and practical risk. Once you understand what hackers might want to steal and how your network protects (or doesn't protect) that information, evaluate the risk to the business. This starts with legal risk. How do federal and state laws require you to protect your sensitive information? What might enforcement agencies do if you don't take reasonable steps to protect that information? If you have shareholders, will they have a cause of action, or will other individuals whose sensitive personal information was taken have a case? At the same time, it is also important to understand the practical risks of a cybersecurity vulnerability. Reputational damage may be just as or even more harmful than financial loss. As executives analyze the risk of a cyberattack, keeping the legal and practical concerns front of mind is paramount.

Fourth, make decisions to mitigate cyber risk. If an intruder's access to a certain database would present unmanageable risk, direct the development of alternate options that enhance your defenses: partition the data into different databases, encrypt and back up the data, and limit access, for example. There are, of course, business realities that may limit how quickly businesses can make changes, such as software compatibility issues or the need for quick and regular access to data. While these realities may present challenges, executives are uniquely positioned to push for creative solutions.

Fifth, plan for a breach, including managing board or senior

management expectations that there should never be one, because a breach likely will occur. In any large organization with sensitive or valuable information, breaches on some scale are inevitable. The question is: how quickly can the company detect the problem and limit the potential damage? Ensuring a corporatewide response plan is in place and well-practiced is something that executives should embrace. This starts with having the right team in place: what is the breach reporting chain, who makes the decisions, and is everyone appropriately represented in response planning? Practicing the plan allows the senior executive team to exercise their best skills, to include problem solving, drilling down on issues, identifying areas of improvement, and taking a leadership role on an issue of widespread concern.

Companies and government agencies with the strongest cybersecurity practices often spend months or more preparing and practicing scenarios that put leaders and systems to the test, and managers make it a priority to participate. Know what actions to take (or not take) with limited information when it comes to the real thing. Exercises often reveal gaps that can unravel even the strongest plans.

For example, you may discover that hackers who are demanding a cyber ransom are operating out of a sanctioned regime like North Korea and you haven't considered the legal implications of paying. Or you may learn that the executive responsible for calling law enforcement is on vacation and cannot be reached, and you have no backup. A crisis team in one country may begin to respond, even publicly, before realizing the attack has impacted multiple countries or the whole region. Conducting these kinds of drills will help flesh out these and other challenging questions, like: what do you tell your customers and when? What, if anything, do you tell government—and which agency? Which official? Practice doesn't necessarily make perfect, but it does make challenging situations a whole lot better.

In addition to the substantive benefits of lessening the impact of a successful attack, a good plan also provides the added benefit of demonstrating to regulators and would-be plaintiffs that you have taken cybersecurity seriously in the aftermath of a potential breach.

In the end, corporate executives should treat cybersecurity like so many of the other risks they manage, and they are well-equipped to do so.

***Lynn Haaland**, a former federal prosecutor, is senior vice president, deputy general counsel, global chief compliance officer, and chief counsel for cybersecurity at PepsiCo. **Paul Rosen**, the former chief of staff at the Department of Homeland Security and a former federal prosecutor, is a white-collar, government investigations, and cybersecurity partner at the law firm of Crowell & Moring, and is a fellow at the Harvard Kennedy School Belfer Center's Homeland Security Project.*