How to Avoid Negotiating with a Hacker

By Naveen Bhateja

Listen to article

100

Advanced preparation and optimal board personnel are key if you want to avoid a cyber crisis.

We exist in an age of heightened data sensitivity, but that is the price of doing business in an increasingly globalized and digitized world. Connectedness is the reward; hyper vigilance is the price. For companies large and small, this means cybersecurity can no longer be outsourced. Instead, it must be internalized within an organization’s DNA.

No corporate board wants to find itself negotiating with a hacker who holds the integrity of the company’s data in their fingertips. The only way to keep pace with increasingly sophisticated cyberattackers is to dedicate resources to cybersecurity. To accomplish this, boards must prioritize hiring of highly skilled IT employees, upskilling current employees on cybersecurity tactics and creating an internal cyber wall of defense.

Understanding Different Kinds of Cyberattacks

 Ransomware is the most common type of cyberattack affecting corporations. Ransomware attacks are all about money. The perpetrators hold a corporation’s data or systems hostage, denying access to all legitimate users or encrypting files until a payment is made.

Phishing scams, which bait victims into sharing passwords or other sensitive information with hackers posing as credible contacts, target millions of people daily.

Disrupted denial-of-service (DDoS) attacks are another well-known variant of cybersecurity threats. These involve overwhelming a corporation’s network with automated false requests that disrupt business operations and keep legitimate customers from gaining access to web-based services.

DDoS attacks have been on the rise, since the pandemic necessitated the expansion of corporate network usage for remote work. The Anti-Phishing Working Group reported more than 300,000 phishing attacks in December 2021. Now hackers are using artificial intelligence to increase the effectiveness of their attacks, largely by identifying vulnerabilities faster and then exploiting them more broadly.

Unfortunately, the government response thus far has not addressed these attacks. On March 9, 2022, the SEC announced proposed amendments to its rules on how quickly and thoroughly companies must disclose cyberattacks, which could impact companies of all sizes. Notably, the comment period was only 30 days, far shorter than usual, which underlined the urgency of these threats.

Experts say that the proposed SEC requirements should be a wake-up call for boards to put cybersecurity at the top of their corporate governance agendas, yet, in 2021, Gartner reported that only 10% of corporate boards had a dedicated

cybersecurity committee overseen by a qualified board member.

Prepare (Not) to Fail

In 2017, Cybersecurity Ventures estimated global ransomware losses at $5 billion — a 15-fold increase in just two years. By comparison, in 2021 alone, the estimated loss resulting from such attacks totaled $20 billion. Many of these attacks were aimed at large corporations, particularly in the financial and healthcare sectors, though these numbers understate the severity of the problem because the FBI estimates that few cybercrimes are reported. Considering that a single victim — JBS, the world's largest meat processor — paid $11 million in ransomware, it can be safely assumed that total losses from these attacks have run into the billions.

Sadly, companies that don't integrate cybersecurity into their corporate DNA should be prepared to lose millions of dollars, and perhaps even fail altogether. Although, according to an analysis published in *Fast Company*, simply throwing more money at better technology won't solve the underlying threat because hackers are learning to be stealthier. The analysis cited data from Boston Consulting Group, illustrating that only 23% of breaches were a result of inadequate cybersecurity technology, whereas 77% were the result of human error.

Clearly, the solution needed for corporate boards is better cybersecurity and cyber literacy training. Every organization must create a culture of security, which starts with the creation of an internal cyber force. But it also means shifting responsibilities from the chief security officer to executive leadership, including the board. At the same time, cyber literacy training should be integrated into the employee onboarding process, with annual training for all employees that incorporates updates and continued education to build security "muscle memory" and best practices into the overall company culture. Digitization means every employee is a potential target — vulnerable to attack — and could also be the one to spot a red flag before it's too late.

Shoring Up the Board

Changing a company's DNA may seem like a daunting task, particularly to smaller companies that are short-staffed because of the pandemic or increased turnover

as a result of The Great Resignation. A good place to start is at the board level with a top-down approach to cyber resilience. The goal should be systematic preparedness, as opposed to systematic improvisation. In March 2022, the *Harvard Business Review* published a helpful article titled, “7 Pressing Cybersecurity Questions Boards Need to Ask.” These questions included five points that directors should know about cybersecurity right now:

- Cybersecurity is about more than protecting data.
- The board must be knowledgeable participants in cybersecurity oversight.
- Boards must focus on risk, reputation and business continuity.
- The prevailing approach to cybersecurity is defense in depth.
- Cybersecurity is an organizational problem, not just a technical problem.

Before addressing these issues, however, it’s going to be important to ask three fundamental questions:

- How cyber-literate is your current board?
- Where are the cyber awareness gaps in the current board, and what is your plan to address them?
- Do you have a team built around your CSO?

Keep in mind: Changes may be in order if your board composition is such that internalizing cybersecurity concepts would be overly difficult or too time-consuming to be effective. Be prepared to weigh those concerns against the cost to the business of not addressing gaps.

Proactively Prepare Against Cyber Threats

If your board pushes back against enhancing cybersecurity protocols or training, here’s a simple truth that should scare them into action: If you don’t test your networks, hackers will.

Security companies have developed state-of-the-art tabletop exercises and penetration testing drills that are constantly updated and should be integrated into every board meeting. The purpose of these exercises is threefold:

- Identify critical assets and processes
- Identify employee groups at risk
- Practice communication and negotiations strategy

Responsibilities should be delegated before an attack occurs.

Once a ransomware attack is implemented, your company will find itself under siege and in a hostage situation. By then, you will have lost critical leverage. If you're well prepared, you will be in a much stronger position to maneuver through the attack and possibly recover. Create a crisis playbook that involves your communications team and complies with the SEC's latest recommendations for dealing with attacks. In the meantime, conduct companywide phishing tests to find your weakest links and maintain organizational awareness to prevent bad actors from striking at any time.

While it is not the board's responsibility to develop technical strategies or be experts in the vernacular of cybersecurity, its goal must always be the survival and continued growth of the company under its purview. Recent ransomware attacks have proved that cybersecurity unpreparedness poses an existential threat to every organization. At minimum, every board should appoint a member dedicated to overseeing cybersecurity strategy and aligning with internal cyber experts to ensure that worst-case scenario preparations are deployed when needed across the organization. Only when these strategies are successfully implemented can cybersecurity become part of the company's DNA.

Naveen Bhateja is executive vice president and chief people officer at Medidata Solutions.