Harvard
Business
Review

IT Security Management

7 Pressing Cybersecurity Questions Boards Need to Ask

by Dr. Keri Pearlson and Nelson Novaes Neto

March 04, 2022

Javier Zayas Photography/Getty Images

Summary. Boards have a unique role in helping their organizations manage cybersecurity threats. They do not have day to day management responsibility, but they do have oversight and fiduciary responsibility. Don't leave any questions about critical vulnerabilities for... **more**

For every new technology that cybersecurity professionals invent, it's only a matter of time until malicious actors find a way around it. We need new leadership approaches as we move into the next phase of securing our organizations. For Boards of Directors

(BODs), this requires developing new ways to carry out their fiduciary responsibility to shareholders, and oversight responsibility for managing business risk. Directors can no longer abdicate oversight of cybersecurity or simply delegate it to operating managers. They must be knowledgeable leaders who prioritize cybersecurity and personally demonstrate their commitment. Many directors know this, but still seek answers on how to proceed.

We conducted a survey to better understand how boards deal with cybersecurity. We asked directors how often cybersecurity was discussed by the board and found that only 68% of respondents said regularly or constantly. Unfortunately, 9% said it wasn't something their board discussed.

When it comes to understanding the board's role, there were several options. While 50% of respondents said there had been discussion of the board's role, there was no consensus about what that role should be. Providing guidance to operating managers or C-level leaders was seen as the board's role by 41% of respondents, participating in a tabletop exercise (TTX) was mentioned by 14% of the respondents, and general awareness or "standing by to respond should the board be needed" was mentioned by 23% of Directors. But 23% of respondents also said there was no board plan or strategy in place.

Building on our findings, we developed the following recommendations for what Boards of Directors need to know, actionable steps directors can take, and smart questions you should ask at your next meeting.

Five things directors need to know about cybersecurity.

1. Cybersecurity is about more than protecting data.

Back in the "old days," protecting organizations from cyber incidents was primarily seen as protecting data. Company execs worried about personal information being leaked, customer lists

being stolen, and credit cards being used fraudulently. These are still issues, but cybersecurity is about more than just protecting data. As we have digitized our processes and our operations, connected our industrial complexes to control systems that enable remote management of large equipment, and linked our supply chains with automatic ordering and fulfillment processes, cybersecurity has taken on a much larger position in our threat landscape. Poor oversight can mean more than paying fines because data was not protected appropriately. Directors need a real picture of the cyber-physical and cyber-digital threats their organizations face.

2. The BODs must be knowledgeable participants in cybersecurity oversight.

It's the BOD's role to make sure the organization has a plan and is as prepared as it can be. It's not the board's responsibility to write the plan. There are many frameworks available to help an organization with their cybersecurity strategy. We like the NIST Cybersecurity Framework, which is a framework developed by the U.S. National Institute of Standards and Technology (NIST). It is simple and gives executives and directors a good structure for thinking through the important aspects of cybersecurity. But it also has many levels of detail that cyber professionals can use to install controls, processes, and procedures. Effective implementation of NIST can prepare an organization for a cyberattack, and mitigate the negative after-effects when an attack occurs.

The NIST framework has 5 areas: identify, protect, detect, respond, and recover. Organizations who are well-prepared for a cyber incident have documented plans for each of these areas of the NIST framework, have shared those plans with leaders, and practiced the actions to be taken to build muscle memory for use in a breach situation.

3. Boards must focus on risk, reputation, and business continuity.

When cyber professionals develop policies and practices, the fundamental triad of goals is to ensure confidentiality, integrity, and availability of both systems and data (the "CIA" of cybersecurity). That's necessary, but the discussion would be very different than one about the goals of risk, reputation, and business continuity, which are the key concerns of the BOD.

While the board tends to strategize about ways to manage business risks, cybersecurity professionals concentrate their efforts at the technical, organizational, and operational levels. The languages used to manage the business and manage cybersecurity are different, and this might obscure both the understanding of the real risk and the best approach to address the risk. Perhaps because cybersecurity is a rather complex, technical field, the board might not be fully aware of cyber-risks and the necessary protective measures that need to be taken. But there are actionable approaches to address this.

Directors do not need to become cyber experts (although having one on the board is a good idea). By focusing on common goals: keeping the organization safe and operational continuity, the gap between the BOD role and the cybersecurity professionals' role can be narrowed. Establishing clear, consistent communication to share useful and objective metrics for information, systems controls, and human behaviors is the first step. Comparisons to existing best practices and methodologies for cybersecurity risk management is another activity to identify areas of need and areas of strength in the organization. Directors asking smart questions of their cybersecurity executives is yet a third action to close the gap.

4. The prevailing approach to defense is depth.

A series of layered protective measures can safeguard valuable information and sensitive data because a failure in one of the defensive mechanisms can be backed up by another, potentially impeding the attack and addressing different attack vectors. This multi-layered approach is commonly referred to as the "castle

approach" because it mirrors the layered defenses of a medieval castle to avoid external attacks.

Layers of defense often include technology, controls, policy, and organization mechanisms. For example, firewalls (and many companies have multiple firewalls), identity and access management tools, encryption, penetration testing, and many others are all technological defenses that provide barriers to, or detection of, breaches. Artificial intelligence technologies promise to strengthen these barriers as new and persistent threats arise. But technology alone cannot keep us safe enough. Security Operations Centers (SOCs) provide oversight and human involvement to notice things the technologies miss, as was the case in the SolarWinds breach, where an astute associate noticed something unusual and investigated. But even SOCs can't keep the organization 100% safe.

Policies and procedures are necessary to meet control requirements and those are set up by management. And, frankly, in today's world, we need every single person in our organizations to provide some level of defense. At a minimum, everyone must be aware of scams and social engineering attempts to avoid falling victim. By the way, that includes directors, who are also targets and must know enough to not be caught by fallacious emails or notices.

5. Cybersecurity is an organizational problem, not just a technical problem.

Many cybersecurity problems occur because of human error. A study from Stanford University revealed that 88% of data breach incidents were caused by employee mistakes. Aligning all employees, not just the cybersecurity team, around practices and processes to keep the organization safe is not a technical problem — it's an organizational one. Cybersecurity requires awareness and action from all members of the organization to recognize anomalies, alert leaders, and ultimately to mitigate risks.

Our research at MIT suggests this is best done by creating a cybersecurity culture. We define a "cybersecurity culture" as an environment infused with the attitudes, beliefs and values which motivate cybersecurity behaviors. Employees not only follow their job descriptions but also consistently act to protect the organization's assets. This does not mean that every employee becomes a cybersecurity expert; it means that each employee is held accountable for overseeing and behaving as if he or she was a "security champion." This adds a human layer of protection to avoid, detect, and report any behavior that can be exploited by a malicious actor.

Leaders set the tone for prioritizing this kind of culture, but they also reinforce and personify the values and beliefs for action. The BOD has a role in this, too. Simply by asking questions about cybersecurity, directors imply that it is an important topic for them, and that sends the message that it needs to be a priority for corporate executives.

The questions your board needs to hear.

Here is a list of seven questions to ask to make sure your board understands how cybersecurity is being managed by your organization. Simply asking these questions will also raise awareness of the importance of cybersecurity, and the need to prioritize action.

1. What are our most important assets and how are we protecting them?

We know we cannot be 100% secure. Difficult decisions must be made. The BOD must make sure the organization's most important assets are secure at the highest reasonable level. Is that your customer data, your systems and operational processes, or your company IP? Asking what is being protected and what needs to be protected is an important first step. If there is no agreement on what to protect, the rest of the cybersecurity strategy is moot.

2. What are the layers of protection we have put in place?

Protection is done with multiple layers of defense, procedures and policies, and other risk management approaches. Boards don't need to make the decision on how to implement each of these layers, but the BOD does need to know what layers of protection are in place, and how well each layer is protecting the organization.

3. How do we know if we've been breached? How do we detect a breach?

The BOD would be ignoring an important part of their fiduciary responsibility if it does not ensure that the organization has both protection and detection capabilities. Since many breaches are not detected immediately after they occur, the BOD must make sure it knows how a breach is detected and agree with the risk level resulting from this approach.

4. What are our response plans in the event of an incident?

If a ransom is sought, what is our policy about paying it? Although the board is not likely to be part of the detailed response plan itself, the BOD does want to be sure that there is a plan. Which executives and leaders are part of the response plan? What is their role? What are the communications plans (after all, if systems are breached or unreliable, how will we communicate?). Who alerts authorities? Which authorities are alerted? Who talks to the press? Our customers? Our suppliers? Having a plan is critical to responding appropriately. It's highly unlikely the plan will be executed exactly as designed, but you don't want to wait until a breach happens to start planning how to respond.

5. What is the board's role in the event of an incident?

It would be helpful for the BOD to know what their role will be and to practice it. Is the board's role to decide on paying a ransom or not, to talk to the largest customers, to be available for

emergency meetings with organization execs to make just-in-time decisions? An earlier article of ours discussed the importance of practicing responses. Using fire drills and tabletop exercises to build muscle memory sounds like a luxury, but should your company have an incident, you want to be sure that response muscle is ready to work.

6. What are our business recovery plans in the event of a cyber incident?

Many execs we have interviewed have not tested their business recovery plans. There can be significant differences in the recovery from a business disruption due to a cyber incident. Data recovery might be different if all records are destroyed or corrupted by a malicious actor who encrypts files or manipulates them. BODs want to know who "owns" business recovery, whether there is a plan for how to make it happen, and if it has been tested with a cyber incident in mind?

7. Is our cybersecurity investment enough?

You can't invest enough to be 100% secure. But since a budget must be set, it is crucial that companies guarantee they have an excellent security team with the appropriate expertise to tackle technical problems and understand vulnerabilities inside the core critical functions of the business. By doing that, the company will be better prepared to allocate investment where it is most needed. Companies should evaluate their level of protection and their risk tolerance before they engage in new investments. Two ways to do this are through simulations of cyber-attacks and from penetration/vulnerability tests. These actions expose vulnerabilities, enable actions to minimize potential damage based on priority, risk exposure and budget, and ultimately ensure appropriate investment of time, money, and resources.

Boards have a unique role in helping their organizations manage cybersecurity threats. They do not have day to day management responsibility, but they do have oversight and fiduciary

responsibility. Don’t leave any questions about critical vulnerabilities for tomorrow. Asking the smart questions at your next board meeting might just prevent a breach from becoming a total disaster.

DP

Dr. Keri Pearlson is the Executive Director of the research consortium Cybersecurity at MIT Sloan (CAMS). Her research investigates organizational, strategic, management, and leadership issues in cybersecurity. Her current focus is on building a culture of cybersecurity.

NN

Nelson Novaes Neto is a Partner and CTO at C6 Bank. He is also a Research Affiliate at MIT Sloan School of Management.