CYBERRISKS&LIABILITIES_

9 Cyber Risk Questions Every Board Should Ask

When a data breach or other cyber event occurs, the damages can be significant, often resulting in lawsuits, fines and serious financial losses. What's more, cyber exposures impact businesses of all kinds, regardless of their size, area of focus, or status as a private or public entity.

In order for organizations to truly protect themselves from cyber risks, corporate boards must play an active role. Not only does involvement from leadership improve cyber security, it can also reduce liability for board members.

To help oversee their organization's cyber risk management, boards should ask the following questions:

1. **Does the organization utilize technology to prevent data breaches?**

   Every company must have robust cyber security tools and anti-virus systems in place. These systems act as a first line of defense for detecting and preventing potentially debilitating breaches.

   While it may sound obvious, many organizations fail to take cyber threats seriously and implement even the simplest protections. Boards can help highlight the importance of cyber security, ensuring that basic, preventive measures are in place.

   These preventive measures must be reviewed on a regular basis, as cyber threats can evolve quickly. Boards should ensure that the management team reviews company technology at least annually, ensuring that cyber security tools are up to date and effective.

2. **Has the board or the company's management team identified a senior member to be responsible for organizational cyber security preparedness?**

   Organizations that fail to create cyber-specific leadership roles could end up paying more for a data breach than organizations that do. This is because, in the event of a cyber incident, a fast response and clear guidance is needed to contain a breach and limit damages.

   When establishing a chief information security officer or similar cyber leadership role, boards need to be involved in the process. Cyber leaders should have a good mix of technical and business experience. This individual should also be able to explain cyber risks and mitigation tactics at a high level so they are easy to understand for those who are not well-versed in technical terminology.

   It should be noted that hiring a chief information security officer or creating a new cyber leadership role is not practical for every organization. In these instances, organizations should identify a qualified, in-house team member and roll cyber security responsibilities into their current job requirements. At a minimum, boards need to ensure that their company has a go-to resource for managing cyber security.

3. **Does the organization have a comprehensive cyber security program? Does it include specific policies and procedures?**

   It is essential for companies to create comprehensive data privacy and cyber security

programs. These programs help organizations build a framework for detecting threats, remain informed on emerging risks and establish a cyber response plan.

Corporate boards should ensure that cyber security programs align with industry standards. These programs should be audited on a regular basis to ensure effectiveness and internal compliance.

4. **Does the organization have a breach response plan in place?**

   Even the most secure organizations can be impacted by a data breach. What's more, it can often take days or even months for a company to notice its data has been compromised.

   While cyber security programs help secure an organization's digital assets, breach response plans provide clear steps for companies to follow when a cyber event occurs. Breach response plans allow organizations to notify impacted customers and partners quickly and efficiently, limiting financial and reputational damage.

   Board members should ensure that crisis management and breach response plans are documented. Specific actions noted in breach response plans should also be rehearsed through simulations and team interactions to evaluate effectiveness.

   In addition, response plans should clearly identify key individuals and their responsibilities. This ensures that there is no confusion in the event of a breach and your organization's response plan runs as smoothly as possible.

5. **Has the organization discussed and formalized a cyber risk budget? How engaged is the board in terms of providing guidance related to cyber exposures?**

   Both overpaying and underpaying for cyber security services can negatively affect an organization. Creating a budget based on informed decisions and research helps companies invest in the right tools.

   Boards can help oversee investments and ensure that they are directed toward baseline security controls that address common threats. Boards, with guidance from the chief security officer or a similar cyber leader, should also prioritize funding. That way, an organization's most vulnerable and important assets are protected.

6. **Has the management team provided adequate employee training to ensure sensitive data is handled correctly?**

   While employees can be a company's greatest asset, they also represent one of their biggest cyber liabilities. This is because hackers commonly exploit employees through spear phishing and similar scams. When this happens, employees can unknowingly give criminals access to their employer's entire system.

   In order to ensure data security, organizations must provide thorough employee training. Boards can help oversee this process and instruct management to make training programs meaningful and based on more than just written policies.

   In addition, boards should see to it that education programs are properly designed and foster a culture of cyber security awareness.

7. **Has management taken the appropriate steps to reduce cyber risks when working with third parties?**

   Working alongside third-party vendors is common for many businesses. However, whenever an organization entrusts its data to an outside source, there's a chance that it could be compromised.

   Boards can help ensure that vendors and other partners are aware of their organization's cyber security expectations. Boards should work with the company's management team to draw up a standard third-party agreement that identifies how the vendor will protect sensitive data, whether or not the vendor will subcontract any

services and how it intends to inform the organization if data is compromised.

8. **Does the organization have a system in place for staying current on cyber trends, news, and federal, state, industry and international data security regulations?**

   Cyber-related legislation can change with little warning, often having a sprawling impact on the way organizations do business. If organizations do not keep up with federal, state, industry and international data security regulations, they could face serious fines or other penalties.

   Boards should ensure that the chief information security officer or similar leader is aware of his or her role in upholding cyber compliance. In addition, boards should ensure that there is a system in place for identifying, evaluating and implementing compliance-related legislation.

   Additionally, boards should constantly seek opportunities to bring expert perspectives into boardroom discussions. Often, authorities from government, law enforcement and cyber security agencies can provide invaluable advice. Building a relationship with these types of entities can help organizations evaluate their cyber strengths, weaknesses and critical needs.

9. **Has the organization conducted a thorough risk assessment? Has the organization purchased or considered purchasing cyber liability insurance?**

   Cyber liability insurance is specifically designed to address the risks that come with using modern technology—risks that other types of business liability coverage simply won't cover.

   The level of coverage your business needs is based on your individual operations and can vary depending on your range of exposure. As such, boards, alongside the company's management team, need to conduct a cyber risk assessment and identify potential gaps. From there, organizations can work with their insurance broker to customize a policy that meets their specific needs.

Asking thoughtful questions can help boards better understand the strategies management uses to prevent, detect and respond to data breaches. When it comes to cyber threats, organizations need to be diligent and thorough in their risk prevention tactics, and boards can help move the cyber conversation in the right direction.

Cyber exposures impact organizations from top to bottom, and all team members play a role in maintaining a secure environment. However, managing personnel and technology can be a challenge, particularly for organizations that don't know where to start.

That's where The Insurance Exchange can help. Contact us today to learn more about cyber risk mitigation strategies you can implement today to secure your business.