pwc

Governance Insights Center

January 2017

As the cyber threat landscape evolves, boards continue to look for ways to get a better handle on how to oversee cybersecurity risk. Boards understand the potential damage a breach can do, but there is often a knowledge deficit to overcome. Boards aren't expected to have all of the answers related to cyber risk, but they do need to talk with management and ask the right questions so they can stay on top of this complex and dynamic risk. Here are seven key questions your board should be asking about cybersecurity:

1. *Do we have the information we need to oversee cyber risks?*
2. *How effective is our cybersecurity strategy at addressing the risks the business faces?*
3. *How do we protect sensitive information handled, stored and transmitted by third-party vendors?*
4. *Do we have cyberinsurance?*
5. *Do we have the right data governance strategy to minimize our exposure?*
6. *How do we stay current on the threat landscape around the industry and market?*
7. *Do we have a tested cyber incident response plan?*

---

1. *Do we have the information we need to oversee cyber risks?*

Boards can keep up to speed with the company's security program by meeting regularly with the company's top security owner, such as the chief information officer (CIO) or the chief information security officer (CISO). Today, more directors are meeting with the company's CIO at every formal meeting.

Boards may also want to consider meeting with outside experts to get additional insights on the latest trends and risks. During these discussions, boards should get information about the company's threat environment and its resistance to cyberattacks, as well as related security metrics.

▶ *Only 36% of directors are very comfortable that management provides the board with adequate reporting on security metrics.*[1]

2. *How effective is our cybersecurity strategy at addressing the risks the business faces?*

Many companies invest in core safeguards to better defend against evolving threats. Some are increasing their cybersecurity budgets, and others are incorporating strategic security initiatives, such as cloud-based or third-party cybersecurity services, data analytics to identify threats and more sophisticated firewalls.

Boards should ask management about the company's comprehensive strategy for addressing data security, whether it is effective, and whether the program includes new technologies to monitor, identify and respond to cyber threats or incidents.

---

[1] PwC, *Annual Corporate Directors Survey*, 2016.

3. *How do we protect sensitive information handled, stored and transmitted by third-party vendors?*

The company's third parties (suppliers, contractors, service providers and others) may have access to sensitive information—which can create a potential cybersecurity breach. Boards should understand how the company selects, vets and monitors third parties, along with how these parties protect the company's sensitive information. They'll also want to understand the company's legal rights related to the third party, particularly if there is a cyber breach.

- *While employees remain the most cited source of compromise, incidents attributed to business partners climbed 22%.*[2]

4. *Do we have cyberinsurance?*

The frequency and severity of cyberattacks has many companies considering cyber insurance. It's a new and evolving industry, making it important that companies thoroughly understand the policies—what's covered, and more importantly, what isn't.

Boards will want to understand the company's policy (if one is purchased) and how the cyber insurance market is changing, particularly as underwriters become more sophisticated.

- *Cyberinsurance market is expected to triple in size to $7.5 billion in 2020 from $2.5 billion in 2015.*[3]

5. *Do we have the right data governance strategy to minimize our exposure?*

Companies today create a vast amount of data and information about their business. With this information comes risk. Companies will want to have effective policies, processes, and controls to manage and get rid of information and data proactively, that is, pre-breach. Boards will want to discuss with management whether the company's data strategy is updated and effective to help minimize costs, legal claims and impact to brand should a breach occur.

- *Only 51% of organizations report having an accurate inventory of data.*[4]

6. *How do we stay current on the threat landscape around the industry and market?*

Information sharing is one way to learn more about how other companies are addressing cybersecurity. Some companies today are moving toward a more collaborative approach, where intelligence on threats and response techniques are shared with external partners in the public and private sectors.

It's important that boards ask what their company is doing to learn from others to improve its own resilience and cybersecurity.

7. *Do we have a tested cyber incident response plan?*

A security breach can cause serious damage to a company's reputation and financial position. Boards should discuss with management the company's incident response plan, what it involves around cybersecurity, how management tests the plan and if it could be improved and more effective.

- *Only 29% of directors say they're very comfortable that their company has adequately tested its cyber incident response plan.*[5]

Cybersecurity needs to stay on the board's agenda. The board needs to actively talk with management about what they have done to protect their company's information assets in our ever-increasing digital world.

Learn more about governance trends and topics at:
www.pwc.com/us/governanceinsightscenter

[2] PwC, *Global State of Information Security Survey*, 2016.
[3] Ibid.
[4] PwC, *Insurance 2020 & beyond: Reaping the dividends of cyber resilience*, 2016.
[5] PwC, *Annual Corporate Directors Survey*, 2016.