Cyber Risk

Safeguarding the Crown Jewels: The Board's Role

By Emily Mossburg and Clay Young

Many boards find oversight challenging in today's complex, technical world. As organizations of all types and sizes grow more connected, cyber risks continue to increase. However, a deep technical understanding is not necessary for board members to oversee how the company's cyber risks are managed. Instead, they should consider it another critical area of required oversight to address. A key to effective cyber-risk governance is knowing what questions to ask of management and understanding how to evaluate management's responses in the context of the cyber-risk landscape.

Elevating Confidence

As board members work to increase their individual comfort levels with cyber-risk oversight, these considerations may help move them toward greater confidence in their approach.

Understand management's view of the key risks to the organization's crown jewels. Board members should understand what the company's key strategic assets, or crown jewels, are. They need to understand where the greatest vulnerabilities exist, and how much and what type of oversight is needed to protect those assets. Focusing in this manner can enable boards to help develop a governance model that aligns with the organization's cyber-risk oversight needs.

Research cyber risk more broadly. Board members should educate themselves on the key cyber risks and potential business impacts that are common within their industry or business model. Conversations with peers or internal and external subject-matter specialists can also be valuable.

Keep asking questions. Directors should not stop asking questions of management until they are satisfied that they understand the greatest threats to the crown jewels and potential impacts. If management reports are too detailed or technical, boards should focus on the aspects that are understandable. They should also push management to answer the tough questions and identify potential weaknesses in the organization's cyber-risk strategy and capabilities. If reporting still leaves too many unanswered questions or does not reflect a consistent view of the organization's cyber threat landscape, boards may consider seeking the services of an outside advisor.

Require consistent reporting across the organization. From information technology to internal audit, boards should consider requiring greater consistency in how information is shared with the board. Consider asking management to:

- Select a single reporting framework for cyber risk. Ask the reporting units to agree on the method of measurement and reporting.
- Provide a common set of key performance and risk indicators that enable the board to quickly ascertain the state of cyber risk across the company.
- Use consistent visuals to report on cyber risk across the organization.

Questions for Management

Asking management these questions may help board members understand the organization's current cyber risks:

1. What are the organization's crown jewels and who owns them?
2. What can happen outside of the company's control that could create a vulnerability?
3. Who might try to steal the company's crown jewels?
4. Have data assets been classified according to their value to the organization?
5. Is the organization sufficiently resourced to protect the crown jewels?
6. Does the company's internal audit function have the experience and technical depth to assess the maturity and risk of the organization's cyber-risk program and its capabilities? How often does it do so?

The effectiveness of cyber-risk governance is dependent on the board's ability to determine whether management is effectively executing its duties and responsibilities for managing cyber risk. Boards that do this well direct questions to management about the crown jewels and require strategic reporting that enables objective measurement of key cyber risks over time.

Emily Mossburg is a principal and leader of the Secure practice in Cyber Risk Services at Deloitte & Touche LLP. Clay Young is a partner and U.S. leader of IT Internal Audit at Deloitte & Touche LLP.

This publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor. Deloitte shall not be responsible for any loss sustained by any person who relies on this publication.