PRIVATE DIRECTORS ASSOCIATION®
CYBERSECURITY

Cybersecurity Governance for Private Companies with a Governing Board

"Everybody has a plan until they get punched in the mouth."
- Mike Tyson

A $2 million punch. The average cybersecurity incident at a small- or medium-sized company leads to $2 million of business interruption losses, according to the most recent Ponemon Institute.[1] Yet only 30% of the companies surveyed believe they are adequately prepared for the evolving nature of cyber threats.

The C-suite must formulate a strategy to defend its most valuable assets, allocate sufficient resources, and vigorously improve its cybersecurity posture. **Here are ten guidelines to consider:**

1. **The board must identify and institutionalize its role and responsibility for cybersecurity governance, separate from management and the audit committee.**
   Management must first assess the critical assets and functions of the company. The board, then, must define what issues and severity rise to the level of requiring board governance oversight. Typically, this includes significant cybersecurity risks where the impacts could cross an unacceptable threshold when the board's tolerance for business risk is considered. Engaging an outside advisor is often helpful to validate the broad range of threats and potential losses in specific business contexts.

2. **The nominating and governance committee should ensure the board's chosen approach is clearly defined in committee charters to avoid confusion or duplication of effort.**
   The full board should be briefed on cybersecurity matters at least quarterly and as specific incidents or situations warrant. Committees with designated responsibility for risk oversight and oversight of cyber-related risks should receive briefings on at least a monthly basis. To encourage knowledge sharing and dialogue, a board may consider inviting its directors to attend committee-level discussions on cyber risk issues or make use of cross-committee membership.

3. **You need cybersecurity expertise, ideally a skilled and business-focused CISO.**
   Organizations that are serious about cybersecurity require an internal expert that understands their business and can evaluate the security of their critical resources. Previous experience in law enforcement, IT, finance, or engineering is insufficient; this person must have business experience and communicate well with the C-suite. The role and its accompanying mandate must report to a level senior enough to be free of interference and conflict from other departments and their goals.

4. **The CISO should routinely report directly to the board, unfiltered by other leaders.**
   The board must ensure that the CISO reports in a business-focused manner, prioritizing the board that prioritizes the board issues, not the company's overall cyber matters. Ideally, the CISO should report to the CEO or one of their direct reports rather than a senior leader of IT. Boards should ensure a succession plan for senior CISO positions, evaluate the training and retention plans for the CISO team, and evaluate outsourcing or partnerships as a backstop.

5. Not all risk is equal. Identify and protect your organization's most valuable assets.
Companies cannot completely insulate themselves from cyber risk. Management should evaluate their organization's most vital assets and functions and concentrate on their protection. These assets include critical intellectual property, reputation or family name preservation, the ability to operate, and unrecoverable financial losses.

6. Good cybersecurity requires ruthless protection of an organization's most valuable assets.
The tone from the top must is non-negotiable when considering cyber risk in everyday business decisions. After the message to protect corporate assets has been issued, operational business decisions should adhere to the decisions of the board and C-suite.

7. Compliance and best practices have very little to do with security.
No matter how well-meaning, regulations are reactive and will not succeed when faced with a hacker's innovation. Government and industry compliance regimes are minimum protections, and while an organization may be complying, hackers are busy exploiting new techniques that are not covered by current regulations and compliance requirements.

8. Cybersecurity is a business issue.
Cybersecurity is directly tied to the action or inaction of a company's employees, vendors, and partners. What may appear to be a routine business decision may have detrimental consequences to a company's cyberattack surface.(2)

9. Companies must have a clear Cyber Incident Response plan.
The impact of a cyber incident can range from a minor glitch to an enterprise blackout. Response plans must be proportionate to the severity of the potential consequences. The critical factors to consider include: Who should be notified of an incident? How frequently are the cyber incident response plans revisited? Are the plans tabletop-tested? Is leadership prepared for ransom, loss of sensitive information, and extortion?

10. Most small-to-mid-size companies are blind to their actual cyber risk position.
There is little correlation between the size of an organization and the cyber threat risk that it may face. The value of a company's intellectual property, trade secrets, and other crucial information will determine its desirability as a target and the sophistication of the attack. In today's world, sophisticated strategies, tactics, and tools are needed to detect an enterprise's vulnerabilities. Outside assistance to identify internal risks is highly recommended.

One of the benefits of PDA is conferring with peers including directors, owners, and executive members. For additional guidance and support, please contact PDA's Cybersecurity Initiative.

Originally published May 2021.
Presented by the Cybersecurity Initiative Team of the Private Directors Association®. Authored by David Tyson, Douglas Neal, and Robert Barr.

(1) Ponemon Institute, 2019 Global State of Cybersecurity in Small and Medium-Sized Businesses
(2) See RiskIQ's Analysis of an Attack Surface at the Private Directors Association® Cybersecurity Initiative Whitepapers