PRIVATE DIRECTORS ASSOCIATION®
Creating Value Through Board Excellence

Cyber Security Governance Overview for Boards

Executive Summary

- Cyber attacks are increasing at an exponential rate, posing significant risks to virtually all private companies regardless of size
- The C-Suite must prioritize cyber security and develop clear policies
- Cyber threats must be evaluated as an enterprise risk, not just an IT problem
- Boards should have the competency to govern cyber risk and increase business resiliency
- The PDA Cyber Security Initiative offers four guideposts for enhancing Board competency in Cyber Security at private firms

Background

Security industry trend data in the 2020 CISCO Cyber Security Report for Small and Medium-Sized Businesses (SMBs) indicate that smaller, mostly private firms face an equal amount of cyber risk compared to larger firms.[1] Further, SMBs face nearly identical public scrutiny from customers and vendors around their cyber security safeguards.

For leadership teams of most private organizations, this should signal a) that cyber security capabilities and tools need to be strengthened and b) that cyber risk must be overseen at the Board level.

The cyber security landscape is evolving rapidly, creating opportunities and challenges for all organizations, whether public, private, or governmental. Digital transformation is driving significant investment in business processes and operations, along with new tools and technologies used to reduce complexities and create competitive advantages; however, these technologies present unknown security risks. Further adding to the risk landscape, most companies' dependence on legacy technology exposes organizations to cyber intrusion from hackers and malicious software.

Strategic governance of significant business risk has always been important. Still the continual rise in the sophistication, velocity and impact of persistent cyber threats has created a business imperative to effectively manage this category of risk or face potentially crippling financial and reputational losses. The 2019 Ponemon Institute study[2] revealed that 66% of SMBs had experienced a cyberattack in the past 12 months with an average economic loss of $1.2 million.

The opportunity for management to leverage the Board in creating a meaningful improvement on strategic cyber risk management is compelling.

Companies have relied on the legal construct of "commercially reasonable actions" as a defense to lawsuits after a cyber-attack from a legal liability standpoint. The recent California attorney general ad hoc comments suggest that companies must adopt the Center for Internet Security (CIS) Top 20 controls standard to claim that the company took commercially reasonable steps to protect the organization. It is the first rulemaking of its type in the USA and subjects all firms doing business in California to arbitrary standards that will compound regulatory and litigation risks.

Recent studies indicate that organizations with effective and robust risk management programs are more likely to experience favorable growth and profitability. PWC's Risk in Review annual survey and report shows firms with strong risk management programs experience, on average, 8% more profit growth and 6% increased revenue growth. However, 49% of the companies surveyed do not require their risk, internal audit, compliance, and cyber security teams to develop a common view of the threats and risks across the ecosystem.[3]

Another common impediment is that only 30% of the companies surveyed by Cisco and Ponemon responded that they had a sufficient budget and personnel to achieve minimal security standards. Even more astounding is that only 9% of the companies responded that the Board is involved in setting cyber security priorities.

Like managing any significant strategic risk, the journey from the initial capability to advanced maturity requires organizations to optimize skill and risk management performance.

Maturing cyber risk management governance at the Board level is often a factor of a shared understanding of fundamental learnings in cyber security, including:

Not all risk is equal

While growing, historical cyber security spend has been spread across the enterprise, trying to protect against a basket of general threats identified in audits and security assessments. This expenditure of resources has not always been prioritized to the business's value-creating assets.

The result of this investment strategy is that all technology assets get some protection, but critical assets are generally under-protected. The reality is that the risks associated with customer information, company secrets, and manufacturing lines are always higher and more disruptive than less critical tools; therefore, those assets warrant increased protection. An alternative approach is to protect critical assets based on the risk level they face while providing the best protection possible to less critical assets.

Defining Enterprise Risk Tolerance

Management teams often resist defining risk tolerance levels because it is difficult and the dynamic and chaotic nature of cyber risk makes it impossible to manage through traditional risk management models. Board members should ensure that clear risk tolerance levels are defined, for critical assets at a minimum, and that security programs invest and prioritize activities to meet those tolerance levels.

PRIVATE DIRECTORS ASSOCIATION®
Creating Value Through Board Excellence

True Security expertise is rare

General familiarity and product knowledge of IT by management and the Board is not a substitute for sophisticated cyber security expertise:

- Outside expertise may be beneficial to Boards in understanding and managing strategic business-critical cyber risks
- The US has less than half of the qualified cyber security candidates it needs; for every 100 active postings, there are a mere 48 qualified candidates.[4]
- There is an even smaller subset of professionals who truly understand how to effectively protect the business at a strategic level.

The Private Directors Association® Position

Board engagement is imperative - Dynamic and asymmetric risk[5] management topics, like cyber security, are best managed by a Board of Directors to minimize conflicts, increase the depth of analysis, and increase healthy tension in risk tolerance discussions with management and IT, especially in private and family-owned firms:

- Organizations must develop resilient enterprises not only to capitalize on the digital age, but to survive.
- Traditional risk management models cannot be applied to cyber security risk because they are slow, based on periodic reviews, and centralized management decision making. Cyber risk is dynamic based on people, process, and technology behaviors. Clear guidance for accepted levels of risk must be decentralized and governed.
- Broad experience is required to manage nebulous risks like cyber security – Board members must become cyber aware and develop capabilities to understand and govern cyber risk.

Cultivate Board fluency and expertise – This should be guided by the organization's size and the relationship the firm holds with risk-creating activities. For example:

- Environments with large volumes of assets sought by threat actors (personal data, employee data, intellectual property, financial transactions, manufacturing, etc.);
- Organizations with large financial transactions (1000+) or several strategic M&A activities during a year (3+); or
- Organizations with a large quantity of outdated IT (end-of-life systems) or low levels of historical infrastructure upgrades and modernization. Often IT environments have hundreds or even thousands of computers, servers, and applications that are out of date and vulnerable to attack because patching and routine maintenance has been deprioritized for many quarters/years. Each one of the vulnerable systems is a potential entry point to a hacker.

Effective cyber security risk management requires transparency and accountability – Cyber Security must be engrained into the company's culture and supported by:

- A mandate to manage cyber security risk
  - Defined expectations and time frame to implement
  - Leaders across the organization that are accountable
- Precise measures of strategic cyber risk improvement evaluated over time
  - Cyber security expertise present with improving results
  - Critical asset protection levels rising
  - Maturing of essential resilience programs like Cyber Incident Response capability
- Board-level reporting and situational transparency
  - The CISO or security expert must report to the Board regularly
  - The CISO must be free of encumbrances in expressing risk levels
  - Business leaders must be owners of the risk and be accountable for improving it
  - Business leaders should not accept more risk than they have approved
- A skeptical view to generalist best practice security regimes and agreement that compliance does not equal security; the goal is securing the business to the risk tolerance level
- Continual development of cyber security literacy at the Board level

Be clear about who owns what – The Board and Management must delineate their roles as it relates to managing cyber security risk:

- Not all risk is strategic, nor are all risks worthy of Board discussion; define clear boundaries so the Board is focused on appropriate risk issues
- Having the right people asking the right questions at the right time is crucial to governance effectiveness.

In Summary

Cyber risks are rapidly increasing, particularly for private companies that have not prioritized their critical digital asset protection nor assessed their unique attack surface. Cyber security is an enterprise risk that must be addressed from a holistic viewpoint and engrained into the company's culture. As with all corporate risks, the Board should be actively involved in monitoring cyber security and Board members should strive to continually improve their own cyber literacy and proficiency.

Published January 2021

Presented by the Cyber Security Initiative Team of the Private Directors Association®. Authored by David Tyson and Robert Barr. Edited by Douglas Neal. Many thanks to the Contributing Editors including Ken Hoganson, Diane Meister, Mary Smith, and Bryan Stewart.

[1] Cisco, Small and Medium-Sized Business (SMB) - Cisco Cybersecurity Series May 2020

[2] Ponemon Institute, 2019 Global State of Cybersecurity in Small and Medium-Sized Businesses

[3] https://www.pwc.com/us/en/services/risk-assurance/library/2020-global-risk-study.html

[4] Emsi: https://www.economicmodeling.com/cybersecurity/

[5] Asymmetric risk occurs when an attacker expends very few resources in order to inflict large losses on the defender