Effective Governance and Board Oversight in a Globalized Information Environment

Disponible également en françaiss
www.isaca.org/currentissue

Governance of technology and cybersecurity is increasingly becoming a top strategic priority because of enterprise, client and vendor dependence on Internet-facing technologies that introduce third- and fourth-party risk. Most modern enterprises have Internet-facing systems and interact with consumers, vendors and partners using some Web interface. Many enterprises use cloud services in one form or another, which means some of their data are transported and stored in the cloud on servers scattered around the world, constituting part of a globalized information environment. The use of cloud vendors only exacerbates cybersecurity risk exposure.

ALLEN ARI DZIWA | CISA, CRISC, CCSP, CEH, CISSP

Serves as a risk specialist and subject matter expert (SME) for the US Federal Reserve Bank of Cleveland. He has worked in technology and cybersecurity consulting for 15 years. He previously served on the Information Systems Security Association (ISSA) North Texas (USA) Chapter E-Council's Ethical Hacking Advisory Board and as an SME for the International Information System Security Certification Consortium (ISC)². He is a certified ethical hacker and threat intelligence analyst. This article does not represent the views of his current or previous employers.

Successful enterprises are run by executives who effectively balance taking advantage of opportunities with managing the risk that follows execution of their chosen strategies. The board of directors (BoD) oversees management to ensure that managers implement approved strategies within the established risk appetite. The board has the role of holding senior management accountable and ensuring that management is providing the needed information to help the BoD make optimal, risk-informed decisions. When it comes to technology and cybersecurity, the board is involved in approving budgets, supporting independent risk management and internal audit. The board must also ensure that its members are capable of providing adequate oversight by reviewing strategy, determining risk appetite and overseeing other important enterprise responsibilities.

The globalized information environment is characterized by evolving technologies and fast-paced innovation. Therefore, to preserve confidentiality, integrity and availability of data used in revenue-generating operations, board members must understand how technology advancements affect enterprise data and information security and how the risk taken by management affects information assets:

> *As the board of directors is the key element of corporate governance, it is clear that its composition must be responsive to the basic functions that are assigned to it: supervising and monitoring, avoiding opportunistic behavior on the part of executives, and providing advice to decision makers to improve the management of the business.*[1]

The board must be comprised of people whose fundamental skills include strategic planning, corporate finance, risk management and a clear understanding of legal and regulatory compliance. Most enterprises have BoDs with specifically assigned teams to oversee technology and cybersecurity risk. The most common are the audit, risk and technology committees.

One group of researchers highlighted the perceptions of directors and senior managers regarding the role of a board in overseeing risk and compliance, strategy, governance, development of senior management and relationships with stakeholders. They found that directors and managers believed that different combinations of these roles determined effectiveness.[2] Because of the complexity of technology and cybersecurity, a superficial understanding of technical concepts is no longer sufficient. A deeper understanding of these issues is necessary so that the board can provide adequate oversight and ensure that proper steps are being taken to manage risk.

Board committees focused on technology and cybersecurity, when properly constituted, can provide effective governance and critical scrutiny, which guides management in identifying and mitigating cyberrisk.

Audit Committee

Although the audit committee is widely known for overseeing the internal audit function, external audit and financial reporting, it also oversees technology and cybersecurity audits. Ideally, some members of the audit committee should have a financial background, and at least one member should be a certified public accountant (CPA). With the ever-increasing complexity of cybersecurity issues, it is imperative to have technically savvy board members with strong backgrounds in computer science or IT. Having at least one member who holds the Certified Information Systems Auditor® (CISA®) credential is ideal. Members who are technically savvy in their areas, such as financial or technical audit, are empowered to challenge assumptions and methodologies used by management.

A technically savvy audit team can easily identify problems such as those that led to the Enron scandal in which:

> *The Enron Board of Directors failed to safeguard Enron shareholders and contributed to the collapse of the seventh largest public company in the United States, by allowing Enron to engage in high risk accounting, inappropriate conflict of interest transactions, extensive undisclosed off-the-books activities, and excessive executive compensation.*[3]

If the board audit committee members are able to read and understand audit reports, they can hold senior management—especially the third line of defense—accountable. While a technical auditor may lead the audit committee in reviewing technical audits, that board member could also be someone who understands business, legal and compliance issues. Technical issues do not occur in isolation—rather, they occur in a business context, which includes business benefits and regulatory compliance.

A deeper understanding of these issues is necessary so that the board can provide adequate oversight and ensure that proper steps are being taken to manage risk.

It has traditionally been the practice to appoint board members who are former or current executives without considering their expertise in technical areas. This must change.

Risk Committee

Board members need to demonstrate a clear understanding of how technology and cybersecurity risk affects operations. The risk committee is responsible for risk management policies and oversight. It must be able to understand and challenge risk updates that are provided by the second line of defense (i.e., managers). The chief risk officer (CRO) must be able to directly access the board risk committee to report activities that pose serious risk to the enterprise without interference from the chief executive officer (CEO). The independence of the CRO is important for the enterprise to effectively identify, monitor and mitigate risk. The risk committee assures this independence.

Members of the risk committee must be equipped with project management skills, change management experience, a reasonable understanding of legal and compliance risk, and knowledge of contingency planning and cybersecurity. They must avoid conflicts of interest and maintain and update written charters, and report to the full board as frequently as quarterly to discuss issues related to their areas of focus. In addition to having technical skills, risk committee members must be able to understand financial statements and processes. The risk committee must be committed to upholding the independence of the enterprise's risk management function.

LOOKING FOR MORE?

- Read *How to Drive Growth, Strategy and Governance Through Design*. *www.isaca.org/growth-through-design*
- Learn more about, discuss and collaborate on governance in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

The board of the future must balance value-creation activities and manage risk within the established risk appetite.

In terms of legal and regulatory compliance, risk committee board members may monitor and track compliance by reviewing management reports with appropriate metrics. Board members who have only peripheral knowledge of regulatory requirements may approve and rubber-stamp reports without holding management accountable if metrics indicate the organization is falling out of compliance.

Technology Committee

A technology committee reviews, approves and oversees major technology acquisitions and deployments. Members of such a committee are expected to understand financial statements and be able to review and approve technology budgets. Whenever new acquisitions are planned, the technology committee must be able to discuss the risk associated with the new technology with the risk committee. The committee members must have a clear understanding of project management, change management and the pros and cons of acquiring new technologies. They must hold the senior management who are responsible for the first line of defense accountable.

Conclusion

Rapid changes in technology and anticipated advancements in artificial intelligence (AI), machine learning (ML) and quantum computing are creating disruption in the cybersecurity space. Therefore, enterprises need to have forward-looking board members who are ready to make adjustments and flow with the changes in the global information environment. Board members must have skills in disciplines such as finance, technology and people management to help them see issues beyond their immediate committee responsibilities so they can effectively challenge assumptions made by senior management before they make decisions that affect technology and cybersecurity risk for the enterprise.

The board of the future must balance value-creation activities and manage risk within the established risk appetite. Gone are the days when board members did not know how to use a computer, but made major decisions on technology and cybersecurity risk. The future board should consist of technical experts who can connect technology and cybersecurity issues to business functions including regulatory compliance. Board members serving on the audit, risk and technology committees must be comfortable interpreting key performance indicators (KPIs) and key risk indicators (KRIs) and must demonstrate confidence that the enterprises they govern are in a position to implement necessary and appropriate controls, develop metrics, and report on technology and cybersecurity risk.

The future board must have shrewd members who can easily discuss thorny issues and clarify expectations for their organization's enterprise and cybersecurity culture. They must be capable of self-evaluation and accept responsibility if the strategy and culture they establish from the top fails. If their contribution fails to prevent major cybersecurity attacks that result in enterprise reputational and legal issues, they must be willing to relinquish the privilege of being on the board. Board members must not simply rubber-stamp what management proposes, but rather use critical skills and expertise to scrutinize and challenge assumptions made by management and hold decision makers accountable for all risk-taking activities. The future board is highly analytical, technical, savvy and diverse.

Endnotes

1. Martin, C. J. G.; B. Herrero; "Boards of Directors: Composition and Effects on the Performance of the Firm," *Economic Research-Ekonomska Istraživanja*, vol. 31, iss. 1, 1 May 2018, *https://www.tandfonline.com/doi/full/10.1080/1331677X.2018.1436454*
2. Nicholson, G.; C. Newton; "The Role of the Board of Directors: Perceptions of Managerial Elites," *Journal of Management and Organization*, vol. 16, iss. 2, May 2010, *https://www.cambridge.org/core/journals/journal-of-management-and-organization/article/abs/role-of-the-board-of-directors-perceptions-of-managerial-elites/96D707EB8F784ABC95EB39F5A08C0B2C#*
3. US Senate Committee on Governmental Affairs, *The Role of the Board of Directors in Enron's Collapse*, USA, July 2002, *https://www.govinfo.gov/content/pkg/CPRT-107SPRT80393/html/CPRT-107SPRT80393.htm*