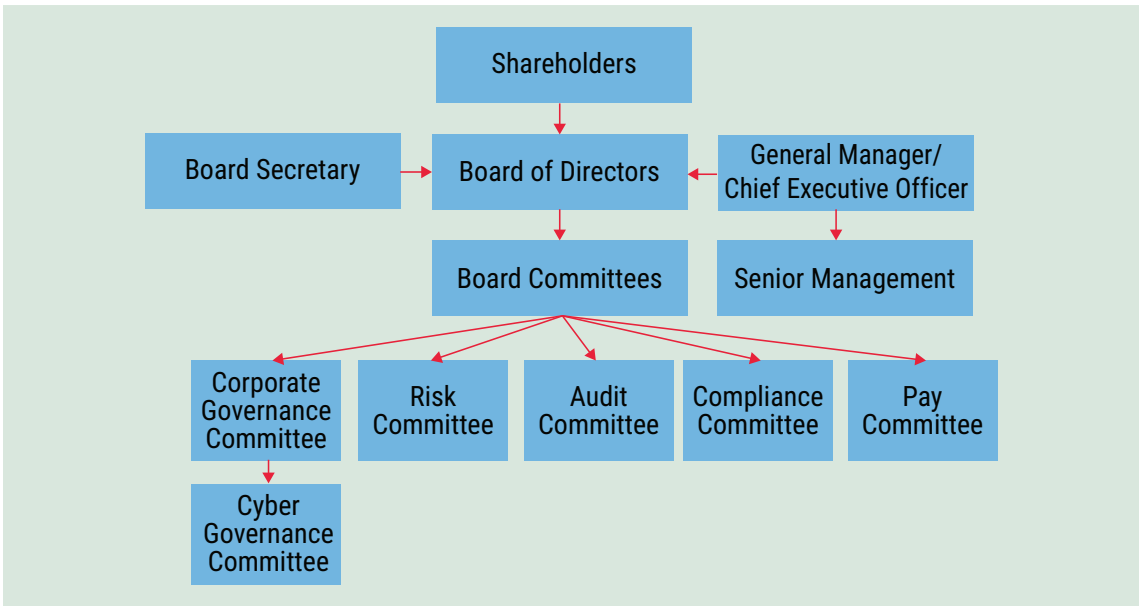
Redefining Corporate Governance for Better Cyberrisk Management

Corporate governance refers to the set of responsibilities to be fulfilled by the higher-level management structures of an organization, such as the management team, board of directors (BoD), and board and management committees. The demands and expectations set by investors and regulators have been a wake-up call, and it has become imperative for these higher-level management bodies to have their radars capture the governance aspects of cybersecurity in addition to their regular corporate governance activities.

Warnings issued by EU regulators on cyberthreats and risk scenarios posed by Brexit are classic examples of this imperative. A hacker group used a Brexit-themed document to deliver Zekapab malware to high-profile organizations such as the Organization for the Prohibition of Chemical Weapons (OPCW), the United Kingdom Defense and Science Technology Laboratory (DSTL), and the United Kingdom Foreign and Commonwealth Office (FCO). So chances are very high that by observing political developments, hackers may try to take advantage of the latest developments, such as Brexit, to innovate and advance cyberattacks such as Zekapab Malware attacks.[1] The Electronic Security Association (ESA) has advised that financial institutions should strive to improve their fragile IT systems and explore the inherent risk to information security, connectivity and outsourcing business transactions that will help organizations effectively address potential cyberrisk.[2] ESA has also provided advice to the financial sector on streamlining the incident management practice in a way that will help manage cyberattacks. The advice also has strategies on establishing a legislative approach (through effective corporate governance) to manage third-party service providers.[3]

Figure 1 depicts the typical corporate governance structure in an organization.

Figure 1—Structure of Corporate Governance in an Organization



Vimal Mani, CISA, CISM, Six Sigma Black Belt
Is the head of the cybersecurity program at Bank of Sharjah. He is responsible for the bank's end-to-end cybersecurity program. Mani coordinates cybersecurity efforts within banking operations across the Middle East. Mani is also responsible for coordinating bankwide cybersecurity strategy and standards, leading periodic security risk assessment efforts, leading incidents investigation and resolution, and coordinating the bank's security awareness and training programs. He is an active member of the ISACA® Chennai (India) Chapter. He can be reached at vimal.consultant@gmail.com.

Core Principles of Corporate Governance

The following are the critical set of corporate governance principles that enable organizations to proactively address various risk factors, including cyberrisk, and can enable reduced risk in business operations.

Fairness
In dealing with the issues of the organization, the board must be fair and free of prejudice. If an independent opinion is required, boards should seek a knowledgeable independent entity to review the issue and provide its opinion. Considering the inputs from all the stakeholders without partiality and inviting a third party to assess specific business transactions such as mergers and acquisitions are some of the ways in which fairness can be integrated into the structure of corporate governance. Not being fair with stakeholders will not help an organization in taking concrete action to address the various cyberrisk factors faced by the organization. Being fair with stakeholders here indicates honesty and disclosure made by an organization to the stakeholders on its efforts and about the effectiveness of existing controls to protect the organization from cyberattacks. A lack of adequate disclosure may result in not getting the right direction or approvals from stakeholders for new initiatives planned for cyberrisk management.

> “A LACK OF ADEQUATE DISCLOSURE MAY RESULT IN NOT GETTING THE RIGHT DIRECTION OR APPROVALS FROM STAKEHOLDERS FOR NEW INITIATIVES PLANNED FOR CYBERRISK MANAGEMENT.”

Accountability
Accountability refers to the right to hold people to a set of standards and to judge whether they have fulfilled their responsibilities in light of these standards or not. For example, the audit committee needs to demonstrate its accountability in review of financial statements, internal control systems and use of external auditors. Lack of accountability results in the risk of people not performing their assigned roles and responsibilities, and policies and procedures may not be followed, leaving the organization vulnerable to risk. Holding people accountable to actions and policies that support effective cyberrisk management can help ensure that the enterprise is holistically supporting strong cyberrisk practices.

Responsibility
Responsibility refers to the actions to be performed by various stakeholders as part of the corporate governance structure. Failing to fulfill the assigned responsibilities could result in risk. For example, it could lead to ineffective security strategy, security plans, lack of security awareness among staff, etc. When people do not fulfill their accountabilities of implementing security policies and procedures, the risk is directly proportional to the degree of accountability.

For example, consider the areas of patching and network security. By not implementing patches in line with policy objectives, systems tend to become vulnerable, which makes them a ripe target for hackers. Not deploying foolproof network security solutions in line with the network security policy to protect the network perimeter can lead to an organization easily becoming compromised by hackers. In the Bangladesh central bank hacking

incident, a lack of firewalls and the deployment of a poor router were identified as some of the root causes of the incident.[4]

The following are some corporate governance responsibilities:

- Providing strategic direction to the organization
- Monitoring the health of the organization, performed by the organization
- Monitoring the operational and financial health of the organization
- Ensuring that business is driven by an ethical base supported by good business conduct and activities
- Overseeing the potential risk factors faced by the organization and ensuring the timely execution of appropriate risk mitigation actions
- Monitoring the health of internal controls of the organization and ensuring the timely execution of required corrective actions
- Ensuring the soundness of reporting mechanisms supporting effective disclosure of the financial health of the organization
- Overseeing the chief executive officer's (CEO's) performance and ensuring the timely execution of corrective actions required to fulfill the expectations of the organization's stakeholders

Transparency

Transparency is about providing timely reporting of potential issues faced by the enterprise. Shareholders should have a transparent view of the organization on a regular basis to understand the risk posed to their investments. Transparency refers to the respect that should be given to stakeholders and their right to factual, quality information in a timely manner. For example, the financial disclosure to investors and shareholders is a critical activity that needs complete transparency. Lack of adequate transparency could result in risk such as loss of stakeholder, consumer and staff trust; regulators imposing fines; and more.

Responsibilities of Board Committees

The following are the responsibilities of various board committees, which play a critical role in improving corporate governance practices for enabling lower-risk business operations:

"SHAREHOLDERS SHOULD HAVE A TRANSPARENT VIEW OF THE ORGANIZATION ON A REGULAR BASIS TO UNDERSTAND THE RISK POSED TO THEIR INVESTMENTS."

- The audit committee oversees financial statements and strength of the internal controls of an organization, and makes timely disclosures to investors on the financial strength of the organization and on the variety of risk factors faced by the organization. In doing this, the audit committee should engage an external auditor who will review the enterprise's annual financial statement and the design and implementation efficiency of internal controls over financial reporting.
- The risk committee, in coordination with the audit committee, delivers reports summarizing the committee's review of the risk posture of the organization, with a focus on various business risk factors such as strategic risk, credit risk, operation risk, cyberrisk, legal risk, internal fraud, regulator-enforced actions, litigations, whistleblower-identified issues, technology issues and the status of an enterprisewide risk management framework implementation.
- The compensation committee (pay committee) oversees the implementation of the compensation policy of the organization, guides development of performance-based compensation packages and approves compensation packages developed.
- The corporate governance committee oversees and determines the membership of the BoD and measures the quality of performance of the BoD as a whole and of individual board members.

- The compliance committee's responsibilities include reviewing corporate governance practices of the organization and recommending improvements to the board, monitoring the independence of directors and reviewing the criteria for assessing independence, and handling and resolving potential conflicts of interests.
- The ethics committee supports the BoD in establishing, embedding and overseeing organizational values in the culture and business of the organization; ensuring and monitoring the overall ethical health of the enterprise; and complying with ethical standards and the business code of conduct established by the organization.

The board's oversight of cyberrisk management-related policies and procedures needs to be enhanced further to effectively manage cyberrisk. Boards should plan to delegate to the committees' tasks related to this on an ongoing basis, which will help the organization in managing cyberrisk in a proactive and timely manner. The committees should plan to be actively involved in the following to help them get a better understanding of the cyberrisk posture of the organization and the effective measures to be taken to manage cyberrisk faced by the organization:

- Understanding the cyberrisk appetite and cyberrisk tolerance level
- Actively engaging in dialogue with chief information officer (CIO), chief information security officer (CISO) and chief risk officer (CRO) on cyberrisk management strategy planning and implementation-related activities and their progress and challenges faced
- Reviewing the cyberrisk register on a regular basis to understand the likelihood and impact of unaddressed cyberrisk
- Being part of cyberrisk assessments and cybersecurity assessments carried out as key stakeholders
- Reviewing the adequacy of budgets allocated for cyberrisk management initiatives, training and awareness programs, cybersecurity policies and procedures, and other controls implemented in the organization
- Making appropriate recommendations to the board for improving the existing cyberrisk management practice in line with global standards by comparing it with the cyberrisk management practices of other organizations in the industry

Why Cybersecurity Is Considered a Corporate Governance Issue

The BoD of an organization oversees the risk management activities of the organization, which should also include cyberrisk management as an integral element.[5]

On an ongoing basis, the management team should oversee the strength of its internal controls, the weakness and failure of which could result in potential cyberthreats. The BoD also is responsible for ensuring that the right resources are allocated in a timely manner to address emerging cyberthreats.

The US Securities and Exchange Commission's (SEC's) recently issued guidance for public companies on cybersecurity-related disclosures has garnered a great deal of attention for what it says about the threat and risk that cybersecurity presents for public companies—large and small.[6, 7] This guideline narrates the SEC's expectations regarding the expected behavior of board members with respect to cybersecurity risk. Corporate governance models will quickly become obsolete if they do not have strong cyberrisk management.[8]

Recent cyberattacks have caught the attention of boards around the world due to the impact on organizations' top-line and bottom-line figures. For example, FedEx reported a US$300 million hit to earnings due to the Petya malware attacks in June 2017. International shipping company Maersk reported that the Petya malware attacks will result in approximate losses up to US$300 million.[9]

A 2015 survey conducted by the New York Stock Exchange (NYSE) Governance Services shows the extent to which boardrooms are unprepared to deal with cyberattacks. Sixty-six percent of survey respondents still lack confidence in their organization's ability to protect itself against cyberattacks.[10]

It has become very clear that cybersecurity is no longer only the responsibility of those in the C-suite such as CIOs or CISOs, but it should become one of the responsibilities of the BoD. Strong alignment between corporate governance and cybersecurity governance has become imperative. Vulnerable business sectors such as banking and financial services should consider having an exclusive cyberrisk committee, or cyber-related aspects need to be bundled with digital/technology steering committees.

The board and senior management need to take appropriate measures to ensure the optimum alignment of corporate and cyberrisk governance. To do this, changes need to be initiated from the board level down throughout the enterprise. Best practice guidelines on corporate governance[11, 12, 13] need to be considered for improving the alignment of corporate and cybersecurity governance practices. Specifically, the Evaluate, Direct and Monitor (EDM) domain of the COBIT® 5 Framework helps in defining and implementing a responsible, accountable, consulted, informed (RACI) matrix, which will help organizations in making the board members responsible, accountable, consulted and informed on various happenings centered around cybersecurity at the board level.

How Boards Can Become Cyberrisk Focused

The board should set the tone to ensure adequate cyberrisk mechanisms exist. Board-level cybersecurity awareness is critical for contemporary organizations. Additionally, boards should have good insights into the risk appetite, cybersecurity strategy, operational and tactical cybersecurity controls implemented, investments made in lieu of cybersecurity threat prevention and protection arrangements, and threat intelligence management practices of their organizations.

The risk management committee should notify the board of potential insider-caused cyberthreats/risk. Board members should be aware of the incident management capabilities and incident response preparedness of the organization. Board members should be aware of the crown jewels (i.e., critical information systems) of the organization to be protected from potential cyberattacks.

> “THE BOARD AND SENIOR MANAGEMENT NEED TO TAKE APPROPRIATE MEASURES TO ENSURE THE OPTIMUM ALIGNMENT OF CORPORATE AND CYBERRISK GOVERNANCE.”

Cyberrisk-related discussions should become a regular item on the board’s meeting agenda, as should IT and privacy risk. Participation of cybersecurity executives (e.g., CIOs, CISOs) in board meetings can result in major improvements to the cybersecurity practices of the organization. CIOs and CISOs should make board members aware of how revenue, costs, profit margin, staff productivity, customer satisfaction and market reputation of the organization can be significantly impacted by cyberattacks. Board members should have discussions with the management team on how to improve the cyberrisk management capabilities of the organization and the competencies of staff to prevent and protect the organization from emerging cyberattacks. Board members should try to address their knowledge gaps in cyber-related areas by attending external training programs and having a cybersecurity expert as an advisor to the board.

Boards should review the results of cybersecurity audits and assessments. Based on the insights gathered from their reviews, they should ask the right questions to the management team to ensure that timely measures are taken to reduce the cyberrisk of the organization. As a corrective and recovery measure from cyberattacks, the BoD should ensure that the management team subscribes to the relevant cyberinsurance plans available in the market. Board members should be aware of the disaster recovery and crisis management capabilities of the organization.

Boards should invite industry experts to be part of their meetings to discuss cyberrisk management best practices. Boards should also invite law enforcement (e.g., police, civil defense authorities of the region where the organization operates) and market intelligence agencies to present on the

> PARTICIPATION OF CYBERSECURITY EXECUTIVES (E.G., CIOS, CISOS) IN BOARD MEETINGS CAN RESULT IN MAJOR IMPROVEMENTS TO THE CYBERSECURITY PRACTICES OF THE ORGANIZATION.

potential cyberthreats and attack trends emerging in the region.

BoDs should guide the management team in establishing a strong operational risk management culture that should include a cyberrisk management element as an integral component. BoDs should ensure that cyberrisk management guidelines are integrated into the enterprise risk management framework in a seamless manner. Finally, the board should ensure that cybersecurity risk disclosures are made to investors as appropriate and as required.

How the Audit Committee Can Become Cyberrisk-Focused

Audit committees should ask the right questions in a timely manner about the adequacy of cyberrisk management measures in place, and they should benchmark the same with peers in the sector. This will help them in gauging the risk appetite of the organization and evaluating the gaps and decisions made by senior management. This committee should be aware of cybersecurity trends, cyberrisk-related regulatory developments and major cyberthreats faced by the organization, and the systemic, economic and business disruptions caused by these cyberthreats. Audits need to be designed as completely risk-driven. IT- and cyber-related risk control self-assessments (RCSAs) should be made mandatory to ensure that the organization and its technology infrastructure are adequately protected with well-designed and effectively implemented controls.

How the Risk Committee Can Become Cyberrisk-Focused

The risk committee should review the organization's strategy to mitigate cyberrisk and examine disaster recovery and continuity plans to ensure the adequacy of cyberrisk management measures in place. The risk committee should support the BoD in giving cybersecurity issues higher urgency and prioritizing them with strong oversight as part of good governance. In addition, the risk committee should communicate with the internal controls committee and the audit committee to help them understand specific risk and who is accountable for different types of cyberrisk. The risk committee should review the cyberrisk appetite on an ongoing basis. The risk committee should also review risk assessments covering the technology management, vendor management, human resources (HR), legal and compliance departments.

How the Senior Management Team Can Become Cyberrisk-Focused

The management team should ensure that all required policies, processes and systems are implemented and adequate. This helps ensure that cyberrisk factors are identified in a timely and proactive manner. The management team should ensure that appropriate communication channels are in place to report the cyberrisk/threat events. This team should continuously monitor the cyberrisk posture of the organization and ensure that cyberrisk/threat events are reported in a timely manner using the communication channels established.

Senior management should ensure that the cybersecurity unit is engaged in regular dialog with business units on an ongoing basis to ensure effective cyberrisk management controls in the business unit. The senior management team should ensure that adequate business continuity and IT disaster recovery arrangements are in place and the organization's disaster preparedness is tested on a periodic basis. The management team should ensure that the critical cyberrisk management competencies are identified and staff are trained to acquire those competencies. The management team should ensure that risk-informed decision-making is happening in the day-to-day operations and risk management is a seamless part of operational business processes.

Conclusion

The lack of adequate oversight on cyberrisk governance could result in loss of customer confidence, reputation damage (which could also result in inflated stock price), potential regulatory actions and litigation. To avoid such pitfalls, boards and the senior management team should have adequate oversight of the cybersecurity posture of the organization. Alignment of corporate and cyberrisk governance practices should be considered one of the top priorities that will help prioritize and mitigate the array of cyberrisk factors faced by organizations. Having a cybergovernance subcommittee under the corporate governance committee; providing good oversight on cyberrisk management activities carried out; and assimilating cyberrisk management aspects into the fiduciary, oversight and risk management responsibilities of the BoD can help organizations manage their cyberrisk posture in a very effective and timely manner.

> "ALIGNMENT OF CORPORATE AND CYBERRISK GOVERNANCE PRACTICES SHOULD BE CONSIDERED ONE OF THE TOP PRIORITIES THAT WILL HELP PRIORITIZE AND MITIGATE THE ARRAY OF CYBERRISK FACTORS FACED BY ORGANIZATIONS."

Endnotes

1 Yip, M.; "Snakemackerel Delivers Zekapab Malware," Accenture blog, 29 November 2018, *https://www.accenture.com/us-en/blogs/blogs-snakemackerel-delivers-zekapab-malware*

2 European Supervisory Agencies, "EU Regulators Warn of Cyber-Threats and Brexit Risks," Finextra, 12 April 2018, *https://www.finextra.com/pressarticle/73431/eu-regulators-warn-of-cyber-threats-and-brexit-risks*

3 Finextra, "European Regulators Advise Against One-Size-Fits-All Cybersecurity Policy," 10 April 2019, *https://www.finextra.com/newsarticle/33670/european-regulators-advise-against-one-size-fits-all-cybersecurity-policy/security*

4 BBC News, "$10 Router Blamed in Bangladesh Bank Hack," 22 April 2016, *https://www.bbc.com/news/technology-36110421*

5 Broadman, H.; "Corporate Boards' Oversight of Cyberrisks Is Too Passive," *Forbes*, 28 November 2018, *https://www.forbes.com/sites/harrybroadman/2018/11/28/corporate-boards-oversight-of-cyber-risks-is-too-passive/#45ad65ef1f81*

6 Fontaine, D.; J. R. Stark; "Cybersecurity: The SEC's Wake-Up Call to Corporate Directors," Harvard Law School Forum on Corporate Governance and Financial Regulation, 31 March 2018, *https://corpgov.law.harvard.edu/2018/03/31/cybersecurity-the-secs-wake-up-call-to-corporate-directors/*

7 Clayton, J.; "Statement on Cybersecurity Interpretive Guidance," US Securities and Exchange Commission, 21 February 2018, *https://www.sec.gov/news/public-statement/statement-clayton-2018-02-21*

8 Federation of European Risk Management Associations (FERMA), "At the Junction of Corporate Governance and Cybersecurity," *https://www.eciia.eu/wp-content/uploads/2019/02/FERMA-Perspectives-Cyber-risk-governance-09.10.2018_0.pdf*

9 Harrell, B.; "Improving Cybersecurity Governance in the Boardroom," *CSO*, 25 September 2017, *https://www.csoonline.com/article/3227887/improving-cybersecurity-governance-in-the-boardroom.html*

10 Knowledge@Wharton, "Corporate Governance in the Age of Cyber Risks," 1 December 2015, *https://knowledge.wharton.upenn.edu/article/corporate-governance-in-the-age-of-cyber-risks/*

11 IT Governance Institute, *Guidance for Boards of Directors and Executive Management*, 2006, *https://www.isaca.org/Knowledge-Center/Research/Documents/Information-Security-Governance-for-Board-of-Directors-and-Executive-Management_res_Eng_0510.pdf*
12 Estevam, R.; J. S. Neto; "Four Steps to Integrate IT and Corporate Governance," *COBIT Focus*, 1 December 2014, *www.isaca.org/COBIT/focus/Pages/FocusHome.aspx*
13 ISACA®, *COBIT® 5 for Information Security*, USA, 2012, *www.isaca.org/COBIT/Pages/Information-Security-Product-Page.aspx*