FEATURE

What the Board Needs to Know About the Organization's Cybersecurity Status

Cybersecurity breaches have come to the attention of boards of directors (BoDs) because of their impact. Disruption of business, loss of data, loss of reputation and financial loss, among others, are all consequences of breaches. The breaches may be the result of external attacks, lapses in organizational security or employee violation of procedures. Cybersecurity has become one of the top-five drivers of strategic change for enterprises.[1] Therefore, it is important for boards to know about cybersecurity risk, how it can harm the organization and ways to overcome it.

Figure 1 provides information on some of the major risk factors and ways to overcome them. This information can help boards decide which controls need to be implemented to strengthen the security posture of the organization. Some of these controls address multiple types of risk; these cues could help boards prioritize the approval of implementing security controls.

It is important for boards to know which controls management has in place to identify, mitigate and manage risk to the organization's business operations and the response to cybersecurity incidents. On a regular basis, the board should receive reports on cybersecurity activities and the risk associated with them, metrics on IT performance, and efforts taken by management to monitor and mitigate risk. The board should assess the adequacy of the resources devoted to policies addressing cybersecurity, support required, and sufficiency of controls in place regarding protection of data, compliance and education efforts. It should also review the measures taken by management to prevent cyberrisk.[2]

Figure 1—Major Cyberrisk Factors and Security Controls

Serial. No	Cybersecurity Risk	Security Controls
1	Unauthorized access of data	Data leakage prevention software, operating system (OS) and virus updates, firewall configuration, user awareness training, access controls, digital rights management, tokenization, policies, encryption
2	Inappropriate use of computers by current or former employees	Integrated risk management software, security information and event management software, password management, account and folder access restrictions, prompt deregistration, user awareness training, log monitoring, multifactor authentication
3	Installation of viruses and malware on computers	OS and virus updates, backup solutions, transport layer security for access through website, user awareness training, endpoint security
4	Social engineering	User awareness training, simulation, antiphishing solutions
5	Disruption or denial of service (DoS)	Configuration of firewall and server, network monitoring, deploying distributed denial of service (DDoS) protection applications

Harisaiprasad Kumaragunta, CISA, APP, ISO 22301 LI, ISO 27001 LA, ISO 9001 LA, Six Sigma Green Belt
Is an associate consultant with Mahindra Special Service Group and has 12 years of experience in the industry. He is currently ISACA® New Delhi (India) Chapter leader and social media chair. He is also a topic leader for the ISACA Certified Information Systems Auditor® (CISA®) online forum. Kumaragunta has written many articles for the ISACA Now blog that are related to the information security domain. He conducts user awareness training, internal auditor training, International Organization for Standardization (ISO) 27001 audits, regulatory audits, third-party audits, internal audits, IT audits and risk assessments, and implements ISO 27001, among other endeavors. He can be reached at harisaiprasad@gmail.com.

Boards should understand that handling cyberrisk is not just the responsibility of the IT department. Cyberrisk can be conveyed to the board during board meetings, through audit briefings, etc. It can be collaboratively handled by the board, management, business unit heads, and IT and security departments.[3] An effective cybersecurity framework cannot be established overnight; it is a long process that slowly matures over time. Because the threat profile is dynamic, the cybersecurity landscape must also continuously evolve.

> "AN EFFECTIVE CYBERSECURITY FRAMEWORK CANNOT BE ESTABLISHED OVERNIGHT; IT IS A LONG PROCESS THAT SLOWLY MATURES OVER TIME."

The board may be aware of the security controls that are required, but management should propose solutions and metrics to tackle the risk so the board can choose the solutions that are most appropriate for the organization. The following is a list of recommendations on what can be included in presentations to the board on the organization's cybersecurity status:

- **Employee awareness**—Employees are the biggest source of cyberrisk because their actions can cause great damage. Awareness is the first step toward cyberprotection. The metrics should contain details on the percentage of new employees trained and the percentage of current employees who have undergone refresher training. The chief information security officer (CISO) can explain the importance of training and ask for additional assistance in terms of resources or funds for employee training.

  Various multimedia and web tools can be used for the preparation of training materials; in a classroom setting, it would be difficult to accommodate all those who need training in a stipulated time frame.
- **Risk assessment**—A risk assessment is an important part of establishing a cybersecurity framework. It includes the various types of risk that arise and the controls provided to avoid, accept and mitigate the risk. The means of handling high risk should be highlighted. Solutions to emerging threats can be discussed to provide board support in acquiring solutions for handling such threats.
- **Patch, firmware and software update metrics**—OS patches, antivirus patches, router firmware, switches and software should be updated. The status of these updates should be presented in the form of metrics, and the way to deal with the systems that are not updated should be discussed. Solutions and recommendations for deploying relevant software for such updates should be presented.
- **Compliance**—Metrics regarding compliance of various regulations and disclosures related to privacy, security and data protection should be drafted and presented. It is important for boards to know the liability issues and steps that need to be taken to mitigate them.
- **Audits**—Cybersecurity audits are an important element in the cybersecurity framework. Audits of IT infrastructure such as firewalls, routers, switches, endpoints, servers and mobile/web applications form a major area for discussion. The gaps raised during audit, their mitigation plan and the status of closing these gaps should

be presented. Assistance from the board in terms of time frame for closure of the gaps or any new purchase of solutions to handle the gaps should be discussed.

- **Incident reporting**—It is imperative for the board to know what attacks have taken place, how they were addressed and how they were resolved. Quarterly metrics of incidents, their repeatability, corrective actions and mitigation strategies can be discussed.

Board meetings mainly focus on the current organizational status of cybersecurity through the presentation of metrics. The granting of budgets for the implementation of a cybersecurity framework and cyberinsurance, among others, should also be discussed with the board for their approval and allocation of funds.

Conclusion

Cybersecurity is not just an IT-related activity; it is an enterprise-level activity that affects all parts of an organization. The board should assess the status of organizational cybersecurity on a regular basis and determine means to tackle future threats and vulnerabilities that could impact the organization. It should provide proper guidance to management such that the organization is cyberresilient. Allotting funds for cybersecurity is not an expense, but a competitive strategy.

“THE BOARD SHOULD ASSESS THE STATUS OF ORGANIZATIONAL CYBERSECURITY ON A REGULAR BASIS AND DETERMINE MEANS TO TACKLE FUTURE THREATS AND VULNERABILITIES THAT COULD IMPACT THE ORGANIZATION.”

Author’s Note

Opinions expressed in this article are those of the author and do not necessarily represent the views of his employer.

Endnotes

1 Clinton, L.; *Cyber Risk Oversight*, National Association of Corporate Directors, 2017
2 Gregory, H.; “Board Oversight of Cybersecurity Risks,” Sidley, 2018, *https://www.sidley.com/en/insights/publications/2018/07/board-oversight-of-cybersecurity-risks*
3 PricewaterhouseCoopers, “How Your Board Can Better Oversee Cyber Risk,” 2018, *https://www.pwc.com/us/en/services/governance-insights-center/library/risk-oversight-series/overseeing-cyber-risk.html*