Cybersecurity has an Imperative Role in Corporate Board Governance

D. Kirk Beatty, Ph.D.

Though previously existing to various degrees depending on company and industry, 2020 pushed the hybrid arrangement of people working from their place of employment, home, or anywhere in between to a never before seen scale increasing demands for cybersecurity.[1] Coupled this with the high profile cybersecurity breaches of Colonial Pipeline[2] and JBS,[3] 2021 further emphasized the need for effective cybersecurity and the imperative for corporate board level governance.

June 30, 2021

Kevin R. Brock, a 24-year career former FBI assistant director of intelligence and former principal deputy director of the National Counterterrorism Center discussed that the spring of 2021 found Americans "getting a taste of a specific threat the intelligence community and cybersecurity experts have warned about for years."[4] The threat - the simple reality that "cyberattacks, engineered overseas, can evolve to a point where they interfere with basic services we all depend on."

A Duke University/CFO Magazine Global Business Outlook Survey found data in 2015 to suggest that CFOs, worldwide, felt their organizations had been hacked, and the smaller the organization the greater the issue due to resource constraints.[5] Eighty percent of U.S. companies surveyed, and more than 85% of firms in Asia, Europe, Africa, and Latin America said their systems had been successfully hacked. These numbers, of course, may understate the issue because firms may be unaware of a breach.

Board Level Cybersecurity Governance

In a 2021 article, Robert R. Ackerman, Jr. discusses where Gartner found the highest levels of corporate management to view cybersecurity risk as the gravest of all threats.[6] This fueled Gartner's prediction that though currently below 10%, by 2025, "40% of American boards of directors will have a dedicated cybersecurity committee overseen by a qualified board member." Ackerman goes on to note that cybersecurity, however, has been seen mostly as a technology concern to be managed by the chief security officer, chief information officer, or an audit function for compliance. PwC, additionally, found that less than a third of corporate board directors surveyed had a grasp on their organizations' cyber vulnerabilities. Boards' unawareness of the matter is likely a significant reason why cybersecurity may be funded only at minimum levels.

Cisco notes how effective cybersecurity and risk communication and mitigation continues to be a struggle for senior leadership and their teams as well as effective articulation of cybersecurity strategy.[7] As a result, cybersecurity too often retains the initial grassroots initiatives for a particular need that have morphed into organizational strategy without the proper consideration for organizational needs. This further tends to realize threats that outmatch capabilities. Thus, cybersecurity is no longer a simple technical solution, but a business function and imperative board-level strategy requiring a greater level of transparency, reporting, and integration with other business units.

Governance Framework for Successful Cybersecurity

Successful cybersecurity programs arise from the same approach as other effective organizational programs. Key stakeholders, however, often claim that the programs are too technical and complex, too internal facing, and are poorly developed and implemented. Much of the challenge is the cybersecurity world does not agree on a standard cybersecurity framework that fits countries, localities, and industries. Nevertheless, a framework for an effective cybersecurity management program (CMP) is a must. Organizations, furthermore, must not underestimate the difficulty to establish a successful CMP. Virtually every individual or group in an organization is impacted, thus the CMP must best address all needs.

Further exploring cybersecurity threats and the question of whether the board of directors can identify and mitigate cybersecurity risks, critical is the financial and reputation risks increasing threats to revenues, customer gain, and customer retention as well as the imperative for board governance and investment.[8] Cyber incidents, additionally, can realize long-term intangible costs that directly impact all lines of business and decrease market value. Boards, however, are found to lack the necessary committee and board-level visibility. Moreover, board members as well as C-level executives often lack the necessary expertise thus preventing the holistic governance of cybersecurity risks. Findings illuminate the importance of designing and implementing a sophisticated governance to cope with the challenges and uncertainties in the ever changing

environment arising from globalization, rapid technological changes, deregulation, and market competition. A governance framework is needed to effectively monitor cyber-risk management and offer sufficient protection from cybercrimes and incidents. This includes the ability to determine the prevention strategies that best help employees and organizations avoid cybercrime and catastrophic cyber events. Various frameworks exist that seek to facilitate a structure to baseline current capabilities in cybersecurity workforce planning and establish a foundation for consistent evaluation. An effective framework further facilitates a mechanism to help those responsible for the implementation of cybersecurity to communicate effectively with the board of directors.

Conclusion

If they currently don't, corporate boards of directors must recognize effective cybersecurity as a board governance matter. Ackerman, additionally, notes the recent growth of cyber-risk measurements may not go far enough and must include a holistic approach of "technical analysis, governance, and company culture." Ackerman, moreover, finds necessary an appreciation of the financial devastation that can stem from adverse cyber events. This is essential for senior leadership teams and corporate boards to understand their organization's exposures, technological vulnerabilities, and risks. Ackerman, also, notes how boards need to replace the focus on the technical with a broader, risk orientation view for the best corporate strategy. This will further assist boards to appreciate and make the investments needed to improve their enterprises' cybersecurity posture. When events do happen, communication is essential to promote a single version of events for both those inside and outside of the organization as well as mediation steps to establish trust. Finally, for the best visibility boards must have metrics that cut through the noise and reports that replace technical jargon with a presentation of the matter in plain terms.

Regardless of the precise structure, the successful framework will support a holistic approach to cybersecurity to meet organizational needs. Effective cybersecurity also starts with a clear strategy originating from the board of directors and senior leadership communicating not just an endpoint but an ongoing journey. In short, development, implementation, and maintenance of a cybersecurity management program is a significant undertaking, but will reduce instances of successful cyberattacks and negative impacts to the bottom line - an imperative for a comprehensive, effective, corporate board strategy.

Author:

- D. Kirk Beatty, Ph.D. - Founder & President/CEO, Adroite & Datatech Information Services, Inc., www.datatechis.com, https://www.linkedin.com/in/kirkbeatty/ -- Datatech is a provider of cybersecurity governance services.

LinkedIn Links:

- *https://www.linkedin.com/feed/update/urn:li:activity:6816069848938897408/*
- *https://www.linkedin.com/pulse/cybersecurity-has-imperative-role-corporate-board-d-kirk/?trackingId=hn2pHo84Q2KEE5eLer3tkQ%3D%3D*

Endnotes

[1] Rundle, J. (2021, June 8). Why the hybrid workplace is a cybersecurity nightmare . *Wall Street Journal*. Retrieved from https://www.wsj.com/articles/why-the-hybrid-workplace-is-a-cybersecurity-nightmare-11623164400

[2] Nakashima, E. & Aratani, L., (2021, May 5) DHS to issue first cybersecurity regulations for pipelines after Colonial hack. *Washington Post*. Retrieved from https://www.washingtonpost.com/business/2021/05/25/colonial-hack-pipeline-dhs-cybersecurity/

[3] Marks, J., (2021, June 2). The Cybersecurity 202: The meat industry is the latest to be thrown into chaos by ransomware. Washington Post. Retrieved from https://www.washingtonpost.com/politics/2021/06/02/cybersecurity-202-meat-industry-is-latest-be-thrown-into-chaos-by-ransomware/

[4] Brock, K. R. (2021, June 7). Ransomware attacks show we're getting clobbered on cybersecurity. *The Hill*. Retrieved from https://thehill.com/opinion/cybersecurity/557021-ransomware-attacks-show-were-getting-clobbered-on-cybersecurity

[5] Duke Today (2015, June 5). New CFO Survey: More than 80 percent of firms say they've been hacked. *Duke Today*. Retrieved from https://today.duke.edu/2015/06/cfohacking

[6] Ackerman, R. R. (2021, May). Corporate boards are better at cybersecurity but still need improvement. *Security Magazine*. Retrieved from https://www.securitymagazine.com/articles/95141-corporate-boards-are-better-at-cybersecurity-but-still-need-improvement

[7] Cisco. (2017). *Cybersecurity management program* [Whitepaper]. Retrieved from https://www.cisco.com/c/dam/en/us/products/collateral/security/cybersecurity-management-programs.pdf

[8] Rahman, B., Karim, T., & Chowdhury, I. U. (2021). Role of boards in cyber security risk profiling: The case of Bangladeshi commercial banks. *Global Journal of Management and Business Research: Administration and Management, 21(3)1.0*, 49-58. Retrieved from https://globaljournals.org/GJMBR_Volume21/5-Role-of-Boards-in-Cyber-Security.pdf