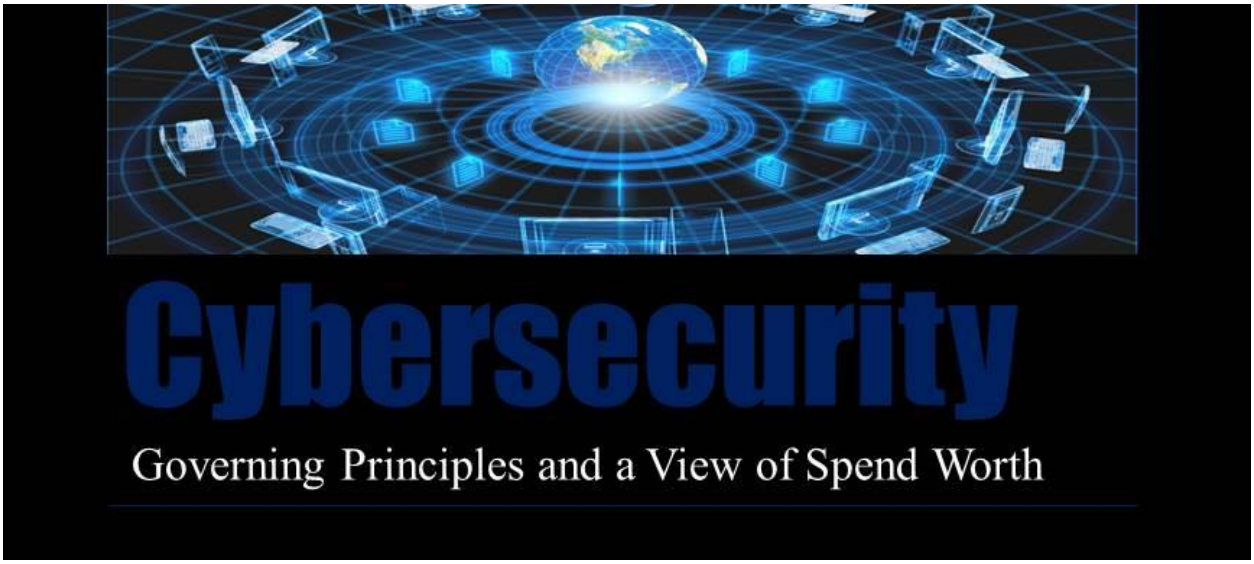
Cybersecurity Governing Principles and a View of Spend Worth

D. Kirk Beatty, Ph.D.

The article Cybersecurity has an Imperative Role in Corporate Board Governance[1] *discussed the importance of a cybersecurity management program (CMP). The article further discussed how imperative a successful CMP is for a comprehensive, effective, corporate board strategy to reduce successful cyberattacks and the negative, potentially devastating impacts to the organization's bottom line. This article continues the dialogue further discussing principles for cyber risk and resiliency governance and a perspective to view cybersecurity spend.*



July 26, 2021

Boards must periodically review management's cybersecurity risk assessment. The assessment must be based on a cybersecurity management program (CMP) framework that best matches the enterprise's needs.[2] Both the framework and needs can be expected to evolve to various degrees over time. The CMP must, also, provide boards the necessary visibility to supply chain and third-party vulnerabilities. Additionally, the board must have visibility into the organization's data hygiene to ensure the proper strategy and governance to minimize privacy risks. Finally, as cybersecurity grows in importance to the organization, the board must be cognizant to the growth in need for board governance. As demands increase, the board can expect to realize the need for a committee devoted more uniquely to cybersecurity and to support the necessary cyber spend to best protect the organization.

If Good People Can Get In, Bad People Can Too[3]

The corporate world could once operate on the concept of firewalls that encompassed the enterprise with protection and kept the bad actors at bay. This was mostly achieved because the

bad actors were without access to the organization's facilities, thus outside of the corporate network. Of course, the more the need for external access grew and the increasing reliance on the connectivity of the internet, the more bad actors had opportunity. Nevertheless, still something manageable, or at least many organizations thought they had it managed. Then the unique year of 2020 where the necessity of remote access transitioned from being a nice to have for some, normal business for others, to a business imperative for survival for most. As a result, the 2021 reality and a future that can expect access beyond the firewall to not only be accepted, but expected, demanded, and thus necessary for businesses to have the best opportunity to flourish and provide preeminent ROI. This, moreover, promotes the concept of *zero trust* networks that is now the necessary mindset.

Resiliency is the common factor that allows companies to adapt. To be capable of adapting a company must be agile to quickly change to meet the ever evolving challenges. To paraphrase Darwin, it is not the most intelligent, not the strongest that survives, but those best able to adapt. To adapt, an organization's cyber risk management must have board-level visibility and discussion, particularly regarding the potential impacts of a debilitating cyber event. Boards must, also, realize and communicate the reality that a effective CMP is fundamental to the successful execution of corporate strategy. In today's world a pair spending more time together. Also, the board must have overall governance, though that does not equate to a hierarchical imperative. In other words, decentralizing the decision-making facilitates the flexibility for cybersecurity selection as close as possible to the data systems' owners. This promotes the necessary agility based on conditions in the present as well as expected in the future to enable the business rather than hinder. Finally, promote a culture of continuous learning and improvement, including those in the boardroom, to best stay abreast of, and more importantly in front of, cyber risk and needs.

Six Principles for Cyber Risk and Resiliency Governance

In a March 2021 report titled *Principles for Board Governance of Cyber Risks*,[4] the World Economic Forum in collaboration with the National Association of Corporate Directors (NACD), the Internet Security Alliance (ISA), PwC, and a working group of industry professionals identified the following six principles boards should consider for governance of cyber risk and cyber resiliency:

1. *Enablement: View cybersecurity as a strategic business enabler.*
   Cybersecurity is more than just an IT concern and presents "persistent, strategic enterprise risks." Thus, successful strategy and governance contributes "to both value preservation and new opportunities to create value." Successful risk navigation, moreover, "requires a culture of cybersecurity with leadership commitment to, and modelling of, good cybersecurity decision-making."
2. *Understanding: Appreciate the economic drivers and impact of cyber risk.*

Strategic initiatives that drive profitability can also increase cyber exposures and risks. Thus, effective strategy must include cost-benefit considerations for digital transformation and cyber risks.

3. *Alignment: Position cyber-risk management with business needs.*
   Boards must understand effective cyber-risk governance in the pursuit of the right strategy. This will realize a security profile that understands enterprise needs and aligns with the organization's risk appetite facilitating alignment of cyber-risk management to strategy across every facet of board decision-making.
4. *Design: Ensure an organizational design that supports cybersecurity.*
   Organizational governance must address enterprise-wide cybersecurity clearly defining ownership and KPIs for management and reporting. This, additionally, must facilitate the integration of cybersecurity practices into operations and decision-making.
5. *Governance: Incorporate cybersecurity expertise into board education and governance.*
   Boards must continuously demand diversity of cyber resources and increase their own knowledge to stay abreast of the ever and rapidly changing cyber landscape.
6. *Strategy: Promote systemic resilience and collaboration.*
   The right, effective strategy includes ensuring cyber resilience for the organization as well as supply chains and partners. This promotes the "overall resilience of the interconnected whole" that organizations increasingly find as their operating normal, their reality.

A Perspective to View Cybersecurity Spend

Cyber risks transcend industries with a variety of concerns, including the underinvestment in cybersecurity leaving industry exposed.[5] The energy sector is one that quickly comes to mind in the United States due to the often reported concerns in news media related to energy grids, plants, and pipelines. The year of 2021, of course, found the possibility become reality with the high profile cybersecurity breaches of the energy industry's Colonial Pipeline[6] and the food industry's JBS[7], both highlighting the devastating possibility and reality to company, community, and country. Moreover, these events emphasize the imperative for board-level strategy and governance of effective cybersecurity. Now, with the shift to remote connectivity being more of a business imperative, this posture increases breach exposures and events. Thus, when deciding what funds to allocate for cybersecurity, instead of viewing cybersecurity as a cost center with a budget, consider viewing cybersecurity as insurance where worth is ascertained based on the value of the assets needing protection, i.e. the corporate enterprise.[8]

Conclusion

As boards increasingly incorporate cybersecurity into board-level strategy and governance, boards will strive for the necessary visibility and agility to achieve these ends. Spurred by a culture of continuous learning and improvement, boards can be expected to increasingly realize motivations to move cybersecurity into its own committee for the necessary strategy formulation

and governance. Facilitating strategy and governance are the six principles identified for governance of cyber risk and cyber resiliency. Finally, as cyber risks transcend industries with remote connectivity being more of a business imperative increasing the possibility of breach exposures and events, boards and organizations will increasingly view cybersecurity less as a cost center with a budget and more as necessary insurance where worth is ascertained relative to the value of the corporate enterprise to protect.

Author:

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

Endnotes

[1] Beatty, D. K. (2021). Cybersecurity has an imperative role in corporate board governance. *Datatech*. Retrieved from https://www.datatechis.net/media

[2] Kappel, K. & Rodi, J. (2021). Oversight of cybersecurity and data governance. *KPMG*. Retrieved from https://boardleadership.kpmg.us/relevant-topics/articles/2021/oversight-of-cybersecurity-and-data-governance.html

[3] Malone, S. (2021). One Year In: Crises Continue to Call for Cyber Resilience. *NACD Board Talk*. Retrieved from https://blog.nacdonline.org/posts/crises-cyber-resilience

[4] World Economic Forum (2021). *Principles for board governance of cyber risks*. Retrieved from http://www3.weforum.org/docs/WEF_Cyber_Risk_Corporate_Governance_2021.pdf

[5] Bissell, K. (2021). America's path to cyber resilience. *Accenture*. Retrieved from https://www.accenture.com/us-en/blogs/security/americas-path-to-cyber-resilience

[6] 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/

[7] 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/

[8] Kress, R. (2020). The corporate director's guide to managed cybersecurity services. Accenture. Retrieved from https://www.accenture.com/us-en/blogs/security/corporate-directors-guide-to-managed-cybersecurity-services