Digital Transformation, Cybersecurity Governance, and the Corporate Boardroom

D. Kirk Beatty, Ph.D.

Digital transformation addresses how organizations use technology to compete. The unique events of 2020 drove organizations, across industry and throughout the world, to embrace innovative and transformative digital solutions. This included 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 and board-level governance,[1] a necessity emphasized by the high profile cybersecurity breaches of Colonial Pipeline[2] and JBS.[3] Much of the conversation has been about how organizations have been impacted and have had to adapt to get the right information into the right hands to inform effective strategy and drive execution, from the line worker to executives in the C-suite. Another key team has had to adapt as well - members of the corporate boardroom. Thus 2020 drove not only organizations to embrace innovative digital solutions, but also the corporate boardroom for effective strategy and governance for the reality of 2020 and beyond to protect and grow the bottom line.

August 30, 2021

Business growth is rooted in innovation. In a digital world innovation is rooted in the digital. Digital transformation, therefore, addresses how organizations leverage technology to compete, a process that continuously redefines the business landscape. Additionally, digital transformation drives the need for effective cybersecurity as in the digital world an organization's cybersecurity protects both the organization and its transformation.

Board's Role in Digital Transformation

Digital transformation is more than just delivering products and services more efficiently with improved margins. Digital transformation is all about driving innovation to develop new products and services to remain relevant. Digital transformation, thus, has move beyond simply doing things faster and more efficiently to innovative ideas and tools potentially further facilitating a change in company culture. Due to the challenge to understand digital technologies, their risks and advantages, and the connectivity to stakeholders as well as threats, e.g. hackers, organizations and their boards of directors cannot afford to be lacking expertise in any of these areas. Additionally, to be transformative, the stimuli must create competitive, sustainable advantages otherwise budgets are consumed and the organization may stray from the ultimate goal to succeed with exceptional customer experiences.

The board's role in digital transformation is to have oversight of the strategic plan that understands the risk and opportunity to drive long-term value for the company. Because boards are focused on whether the CEO has the correct strategy, understanding how digital transformation is imperative to that strategy is crucial to the digital transformation's strategic role driving the right strategy and culture. The right strategy will further recruit and lead the organization's talent through the execution of the digital transformation embraced by the strategic plan. Because boards will be deeply involved with questions and insights facilitating the CEO's formation and execution of the right strategy, directors must know what questions to ask to successfully leverage the continued digital transformation. Boards will want oversight, possibly a board-level committee, to have the deep-dive discussions with management. This may, additionally, leverage outside experts to ensure the transformation has the right scale. Moreover, digital transformation often touches every aspect of the business and is engrained in the corporate culture directly tying to the strategic plan. Keys to a digital transformation, therefore, include a strategic plan that understands digital transformation ends with goals linked to the organization's business strategy, a culture that has the right talent that embraces the necessary transformation, metrics that accurately gauge the success of the transformation, and a plan to address risk and opportunity.

What Boards Want

With over 80% of directors across the globe finding digital transformation should be part of board strategy, successful companies tend to be outwardly focused to keep an eye on how well the business strategy is working seeking the agility to adapt and grow. Directors expect management to stay abreast of all key aspects that affect the company and look for proactive opportunities including technology, globalization, and market developments. Management must, additionally, have a plan to address risks and opportunities as the way things are done will change. New technologies will be required which bring risk and opportunity of their own, including new and larger amounts of data which have to be secured maintaining the desired quality of services and products. Digital transformation requirements change necessitating

change management including a culture of entrepreneurialism, innovation, collaboration, and new ways of thinking where failing is essentially new learning. Digital transformation also requires talent and upskilling in the digital space as well as communication with stakeholders, both internally and externally, to tell the company's story and its strategic vision. This should be a part of management's multiyear strategy discussed with the board else the board may take the lead.

What Boards Must Do

For successful digital transformation boards must understand the strategy and market, have access to management and data, and be able to ask the questions to flush out any needed change. Digital investments must be included in the strategic plan with the right risk appetite understanding the risk of doing nothing. This may require directors with related experience, which is often in a younger talent pool. This talent, also, does not have to be from the traditionally known places such as Silicon Valley. Despite the growing importance of digital since the early 2000s, boards nevertheless are found to lack a digital skillset at sufficient levels. Thus, board directors must leverage network as digital savviness means different things for different businesses and sectors. Digital savviness, moreover, equates to understanding an ecosystem's complexity and how to leverage technology for that ecosystem to drive business value. Additionally, along with the right leadership comes the necessity to have the right culture, a culture that embraces change and the entrepreneurial mindset inviting transparency, communication, and *outside of the box* thinking. Though digital is fast, digital transformation is a continuous series of marathons, i.e. an ongoing journey. Digital transformation must have milestones and KPIs to gauge the ROI pivoting as necessary. Furthermore, boards must understand and sufficiently fund realizing the ROI may take time.

Deloitte's Deborah DeHass and Andy Main in their article *The Board's Role in Shaping Digital Transformation* discuss digital transformation as getting the right information to board members and organizational leaders to inform effective strategy. They, additionally, note how boards must engage management with in-depth deliberation to ensure the strategy impacts stakeholders in transformative ways for new as well as the existing organizational capabilities, particularly for customers and business-units. This includes the connectivity to transform engagement among all stakeholders "by connecting people, spaces, products, data, and technology." This connectivity must facilitate innovative, winning digital customer experiences. This further facilitates the use of AI tools and data analytics for the intelligence to provide innovative insights for customer tailored offerings. The organization must, also, deliver leading-edge innovation by leveraging "emerging technologies such as augmented and virtual reality, machine learning, and AI to create innovative products and services that help build competitive advantage." This will, moreover, drive success by use of automation and digital tools to improve operations, engage customers with more rewarding experiences, and better utilize talent for greater valued activities.

Given the increased hacking and risks of intrusions, and the increase in distributed work and the use of the internet that goes beyond the firewall and allows access inside the firewall, cybersecurity is another paramount component of a board and organization's successful digital transformation and overall strategy. While investing in digital tools, boards must also invest in the cybersecurity tools to protect the facilitated activity. Cutting-edge cybersecurity must be implemented for data security over connected devices. Boards must ensure a security culture throughout the organization is well engrained in the organization's day-to-day operations. To reach this threshold, there are increased calls for a board-level committee dedicated to cybersecurity for the organization.

Questions Boards Must Ask About Digital Transformation

With the complexity that joins digital technology and the speed of innovation and change offering necessary opportunity, corporate board directors realize digital is vital to their organizational strategy, but many are uncertain how they add value to the conversation. As digital transformation requires new board mandates further facilitating not only opportunity, but also new risk and competition, McKinsey's senior partners Celia Huber, Alex Sukharevsky, and Rodney Zemmel suggest boards must understand the implications of technology in digital transformation is not about going digital, but about creating value. In a Harvard Business Review article Huber et al. propose five questions boards should ask to ensure they are focused on the most impactful digital challenges to ensure their organization has the best, effective, competitive advantage:

1) Does the board understand the implications of digital and technology well enough to provide valuable guidance?

2) Is the digital transformation fundamentally changing how the business creates value thru scale, source, and scope?

3) How does the board know if the digital transformation is working?

4) Does the board have a sufficiently expansive view of talent?

5) Does the board have a clear view of emerging threats?

While the core function of the board remains the same, the scope is expanding regarding intervention on risk and competition. With the continuous and rapid change in technology, boards aren't necessarily to understand the technology but more the implications. Thus boards should include members with expertise that aligns with the strategic priorities.

To ensure the organization is leveraging digital to create value, boards must focus on scale, source, and scope. *Scale* should realize digital initiatives driving operating profits by at least 20

percent changing technology, operating, and business models as necessary for the company and possibly the industry. *Source* addresses where technology facilitates more than just cost savings and leads to innovation and new sources of value. *Scope* discusses how digital transformations require a long-term horizon to reap the benefits. Most in the industry will have committed to the investments to reap short-term gains, but the long-term investments are the differentiators. Thus boards must ensure their CEOs have the right mix of long-term spending and must "understand the implications of technology and digital on the business and sources of revenue." Moreover, boards must challenge management's assumptions regarding how digital will transform the industry and new ecosystems evolve to disrupt traditional value chains. Boards, additionally, can be expected to scrutinize new director candidate's digital transformation experience regarding its fit with the company's digital strategy. Finally, as necessary boards must seek training that focuses on key technologies and methodologies.

Boards can ensure management is focused on the domains that create the most value and follow progress to ensure the digital transformation is working by tracking the right ROI metrics on digital and technical investments. Metrics include the speed to which new ideas become revenue producing tools as well as the split in talent working on agile teams spurring innovative change. Boards will want insight into outcomes and leading indicators tied to value, e.g. "customer fulfillment in e-commerce, or reduced time to first quote." Boards will also require visibility for behavior and process changes deep in the organization such as the number of ideas translated into frontline tools and what key processes are driven by AI versus traditional non-digital methods. In other words, focus to succeed on the transformation and digital will occur because digital is the only way the transformation will happen. Finally, though boards will not get into the details of hiring the digital talent, boards must engage management on the progress made and help management keep ahead of talent needs. Boards will want to ensure management understands the talent needed to drive the digital transformation is being secured with up to a 12-month view.

As digital increases opportunities blurring traditional boundaries, digital will bring nontraditional threats and increase the speed of threats. Digital can be expected to increase complexity of threats beyond just cybersecurity such as governing laws regarding data server locations, competitive threats from new business and technologies that suddenly emerge, and new digitally facilitated sectors. Thus boards must ensure management thinks outside of the box enough with more sophisticated scenario planning by asking the *what if* and *have we thought about* questions.

Trading Places with Digital for the Boardroom Itself

Prior to 2020 board meetings were about 95% in-person to 5% virtual. 2020 found those numbers trading places. While there are definitely advantages to in-person meetings, the experience of 2020 can be expected to find boards utilizing virtual or hybrid meetings more often due to efficiency and attendance gains. Small, but important items such as document signatures forced boards to transition to digital functionality eliminating the need to circulate hardcopies of

board papers and ultimately reducing costs of meetings. Much of this has been accomplished with common tools such as Google Meet, Zoom, etc., rather than tools designed specifically for board governance and the security required in the digital world. However, boards are adapting to more secure tools for their board work. Nevertheless, there is plenty of room for improving secure, board governance in the digital world. Thus, digital transformation drives the need for robust cybersecurity for not only the organization in conducting its business, but also for the board in the governance of that business.

Board's Role in Cybersecurity Governance

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…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.

Addressing the non-profit space, the Community Foundations of Canada published a fact sheet on cybersecurity and privacy where they noted ""Nonprofits, like every other organization or corporation, are taking in more information than ever before, and more than we know how to handle."[6]

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.[7] 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.[8] 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.[9] 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.

Cybersecurity Governance and Spend

Boards must periodically review management's cybersecurity risk assessment. The assessment must be based on a cybersecurity management program framework that best matches the enterprise's needs.[10] 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[11]

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*,[12] 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.[13] 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[14] and the food industry's JBS[15], 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.[16]

Conclusion

For an organization's digital transformation, corporate board directors must surround themselves with the best experts, and this may go beyond the CTO or CIO in the company. Boards must be educated, which can involve relationships with younger talent as well as onboarding new directors with digital skillsets. Boards will want to consider digital at the committee level asking the right questions fostering inspirational leadership championing digital transformation. The board's role in digital transformation, additionally, includes operational digital tools and effective cybersecurity to go along with those tools. Moreover, a certain board-level digital savvy and training is required to stay abreast of emerging digital capabilities facilitated by new tools, technologies, and business models. Companies are more and more seeking digitally competent board talent who can grasp how new technologies are evolving the landscape, thus companies must recruit the right talent and invest in continuing education to stay digitally competent. With the digital transition experienced prior to 2020, and the sudden and rapid shifts required as a result of 2020, the adoption of new digital solutions requires investing in new digital technologies, embracing cybersecurity and its culture, and ensuring board-level digital competency for effective, organizational strategy and execution.

Additionally, if they currently don't, corporate boards of directors must recognize effective cybersecurity as a board governance matter. Moreover, 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" (as quoted from Ackerman). Also, necessary is 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. Boards, furthermore, 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. Moreover, 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. Thus, regardless of the precise structure, the successful framework will support a holistic approach to cybersecurity to meet organizational needs. Therefore, effective cybersecurity 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.

As boards increasingly pursue digital transformation and further 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 digital transformation and 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 as they pursue and execute their digital transformation.

Author:

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

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] Community Foundations of Canada (2021, June 14). Fact sheet: Community Foundations of Canada: cybersecurity and privacy. *The Learning Institute*. Retrieved from https://communityfoundations.ca/wp-content/uploads/2021/08/Fact-Sheet_-Community-Foundations-of-Canada-CYBERSECURITY-AND-PRIVACY.pdf
[7] 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
[8] Cisco. (2017). *Cybersecurity management program* [Whitepaper]. Retrieved from https://www.cisco.com/c/dam/en/us/products/collateral/security/cybersecurity-management-programs.pdf
[9] 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
[10] 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
[11] 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
[12] 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
[13] 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
[14] 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/
[15] 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/
[16] 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