MGS650 Response 1 – Cybersecurity Risk Governance

Some of the key components of cybersecurity risk governance strategy are:

-Set and manage accountability and decision rights:

This includes obtaining senior leadership commitment to governance strategy, setting strong policies by formalized leadership and most importantly strategic integration of enterprise security charter (CIA Triad), Enterprise risk management (ERM), and mission driven assurance and security strategies within and beyond the enterprise by the leadership.

-Decide Acceptable Risk Management:

This includes a comprehensive governance, risk and compliance (GRC) solution to assist with risk assessment, arbitration and mitigation. This also includes managing the firm's risk exposure and utilizing risk profile to prioritize risk mitigation decisions.

-Enable Risk Control:

This includes executing the right mix of risk based technology solutions i.e security and Information assurance programs, compliance and frameworks. This is essential to streamline the adopted custom or regulatory frameworks or standards (NIST CSF, ISO 27001, PCI-DSS, HIPAA etc). This ensures enabling connection between security controls (risk management) and policy objectives (governance) to establish proper functioning (compliance). This can also use a security development framework with system development life-cycle (SDLC) implementation.

-Assure Control Effectiveness:

This enables clear guidelines for audit processes particularly in terms of direction, monitoring, reporting and follow up. This can include utilizing metrics related to threats, vulnerabilities, consequences to tailor organization’s threat modeling, incident handling, security and governance measures. This provides valuable insights to correct issues that pose significant risks and formulate a strategic security posture for the organization.

Some of the key challenges with ownership of security governance:

- Lack of a truly centralized security ecosystem i.e., group risk ownership that can coordinate efforts around people, processes and technologies to support organization’s security operations decisions and remain accountable.
- Although the CISO team is essential for the growth of an organization by providing good risk decisions and to remain in compliance, it is arguably considered as the least operationally important stakeholder in the current scenario.
- A common practice of security governance ownership given to highest authority(Board of directors) and not transferring risk ownership down to the organization chain can pose

a significant security challenge for corporate security teams since it leads to lapse in quick decision, limiting visibility and ultimately hindering a positive risk culture.

- Another challenge in ownership of security governance is the tendency to form organization silos between business units that would obstruct effective practice of an enterprise risk management.

Some of the core challenges with oversight of security risk governance:

- Lack of adequate cybersecurity expertise and limited importance given to cyber risk management in corporate boards agenda.
- Ineffective integration of cyber security with already crowded audit committees is leading the audit committee to put together a team lacking cyber expertise.
- Lack of clear segregation of duties(SoD) i.e., guidelines delegating responsibility, obligations among the existing range of committees that includes risk, governance and technology sub committees.
- Lack of specialized proprietary cybersecurity committees for organizations could pose a threat to operational effectiveness since the nature of cybersecurity risk is constantly changing while different sectors have different security concerns.

Some of the potential methods to address these challenges:

- Integrate enterprise risk management by clearly defining the expected role of the chief information security officer vis-a-vis others, such as the chief risk officer.
- Board of directors use various techniques to minimize their oversight by adopting cybersecurity awareness and training including individual training, deep dives, table top exercises and thus minimize managerial ineffectiveness by amplifying accountability for cyber oversight in subcommittees.
- Frameworks can help translate risk in simpler understandable literature with focus on risk appetite, information risk and operational resiliency.
- Reliance on third parties to provide business critical services while leveraging their expertise in assessing the risk, and actively investing in cyber risk information sharing capabilities across public and private sectors thus achieving objectives that are enabling for boards.
- Introduce cybersecurity risk governance in early phases of product and service design and development processes that ensures privacy and security-by-design in product development and deployment.

How might I implement a cyber security governance strategy if I were the CISO in an organization?

- Understand and clearly clarify business and security-related roles to reduce board level oversight and ineffective coordination between security roles and functions. This ensures better identification of stakeholders in the organization and could enable shared responsibility.
- Assessment of current state of controls in place must be conducted through assessments or audits to evaluate the business mission, principles, policies, procedures, standards and frameworks in place. This ensures strategic alignment of security governance with IT and the business.
- Develop and maintain a sound risk culture by regulating risk maps, risk accountability and standardising metrics to aid assessments and tracking progress. Conducting security assessments helps to update controls ultimately enabling people processes and technology.

Challenges observed in small, medium, and large businesses:

- In large global businesses, although there are stakeholders assigned for prioritized focus areas, there is an imminent disconnect with array of future technologies such as artificial intelligence, augmented reality, 5G communication that will pose cyber threats and introduce novel unprecedented risks.

- In small and medium businesses, some of the security roles may not exist or present with few people and lack of oversight is prevalent. SMEs operate on rigid business models that lack specialized focus at any point of time which may lead to malware attacks, burdening hidden costs. Lack of efficient BYOD policy in SMEs is a prevailing concern.

References:

Williams, Carol. “5 Critical Steps to Cultivating a Positive Risk Culture.” *Carol Williams*, 17 Jan. 2018, www.erminsightsbycarol.com/cultivating-positive-risk-culture

“Resilient Governance For Boards Of Directors” | The University of California, Berkeley https://cltc.berkeley.edu/wp-content/uploads/2020/01/Resilient-Governance-for-Boards-of-Directors-Report.pdf

“Secure Software Development Framework | CSRC.” *Secure Software Development Framework*, 25 Feb. 2021, csrc.nist.gov/projects/ssdf