CEO-Level Guide: Cybersecurity Leadership

Governance

Your organization's cybersecurity starts and ends at the highest level of management. The CEO, together with the board, must maintain understanding of the risks and assume ultimate accountability and responsibility for the organization's cybersecurity activities and personnel. You should:

⇒ Hire a chief information security officer (CISO) if none exists or, if resources are too limited, appoint somebody within your organization to fulfill the function of a CISO.

⇒ Work with the CISO or other technical personnel to establish and maintain a cybersecurity strategy and framework tailored to the organization's specific cyber risks using international, national, and industry standards and guidelines.

⇒ Articulate clear roles and responsibilities for personnel implementing and managing the organization's cybersecurity.

- Work with the CISO to identify proper cybersecurity roles and access rights for all levels of staff.
- Oversee communication and collaboration to ensure that cybersecurity management is holistic especially if cybersecurity responsibilities are shared by multiple personnel or divisions within the organization (such as having separate information security, risk, and technology verticals).

⇒ Ensure that the CISO has a clear, direct line of communication to relate threats in a timely manner to you and to the board.

⇒ Invite the CISO or other technical personnel to routinely brief senior management.

⇒ Ensure that the organization's security policies, standards, enforcement mechanisms, and procedures are uniform across all teams and lines of business.

Risk Assessment and Management

Ensuring strong cybersecurity awareness and preparedness depends on continuous, risk-based analysis. To improve your organization's cybersecurity:

⇒ Establish cybersecurity risk assessment and management as a priority within your organization's broader risk management and governance processes. Work with your CISO or other technical personnel on a plan to conduct a risk assessment that involves:

- Describing your organization's assets and their various levels of technology dependency,
- Assessing your organization's maturity and the inherent risks associated with its assets' technology dependencies,
- Determining your organization's desired state of maturity,
- Understanding where cybersecurity threats sit in your organization's risk priority list,
- Identifying gaps between your current state of cybersecurity and the desired target state,

- Implementing plans to attain and sustain maturity,
- Continuously reevaluating your organization's cybersecurity maturity, risks, and goals, and
- Considering using third party penetration-testing or red-teaming,
- Considering protective measures such as buying cyber insurance.

⇒ Lead employee efforts during the risk assessment process to facilitate timely responses from across the institution.

⇒ Analyze and present the results of the risk assessment for executive oversight, including key stakeholders and the board.

⇒ Oversee any changes to maintain or increase your organization's desired cybersecurity preparedness, ensuring that any steps taken to improve cybersecurity are proportionate to risks and affordable for your organization.

⇒ Oversee the performance of ongoing monitoring to remain nimble and agile in addressing evolving cyber risk.

Organizational Culture

Your organization's cybersecurity is not a one-time process or the job of a few employees; it is a factor to consider in all business decisions and operations and a practice that must be maintained by all employees. To encourage continuous, holistic cybersecurity within your organization:

⇒ Begin cybersecurity discussions with the leadership team and communicate regularly with the personnel accountable for managing cyber risks.

⇒ Make cybersecurity training a part of all employee onboarding, ensuring that all staff are up to date on – and have signed documents agreeing to adhere to – your organization's cybersecurity policies and that your IT department or other technical personnel have briefed them on best practices.

⇒ Institute recurring cybersecurity training for all staff with regard to their short- and long-term security responsibilities.

⇒ Ensure that cybersecurity is always considered when your organization evaluates potential vendors and shares data with third parties.

⇒ Annually review your organization's cybersecurity policies.

⇒ Encourage voluntary information sharing about cybersecurity threats and incidents within your organization and with trusted counterparts.