CYBERSECURITY FOR SMALLER ORGANIZATIONS

CEO CHECKLIST: CYBERSECURITY LEADERSHIP

GOVERNANCE

- ☐ **Appoint a Chief Information Security Officer (CISO) if none exists.**
- ☐ **Establish and maintain an organization-wide cybersecurity policy that is risk-based and informed by international, national, and industry standards and guidelines.**
- ☐ **Define roles and responsibilities for all personnel involved in cybersecurity. Work with your CISO to identify proper cybersecurity roles and access rights for all levels of staff.**
- ☐ **Establish or identify clear communication channels between any separate units or personnel that deal with different aspects of cybersecurity.**
- ☐ **Ensure your CISO has a clear, direct line of communication to relate threats in a timely manner to you and to the board.**
- ☐ **Maintain a regular invitation for your CISO or other technical personnel to brief senior management.**
- ☐ **Check that cybersecurity policies, standards, and mechanisms are uniform across the entire organization.**

RISK ASSESSMENT AND MANAGEMENT

- ☐ **Conduct a cybersecurity risk assessment in collaboration with your CISO or other technical personnel, which should include:**
  - 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,
  - Evaluating and earmarking funds to invest in security and address existing gaps,
  - Continuously reevaluating your organization's cybersecurity maturity, risks, and goals, and
  - Considering protective measures such as buying cyber insurance.
- ☐ **Analyze and present results to key stakeholders and the board.**
- ☐ **Plan to oversee any steps to increase cyber preparedness and monitor progress.**

ORGANIZATIONAL CULTURE

- ☐ Regularly discuss cyber risk and security at the leadership level.
- ☐ Ensure that cybersecurity training is part of all employee onboarding and have all employees sign documents agreeing to adhere to the organization's cybersecurity policies.
- ☐ Establish recurring cybersecurity training for all staff.
- ☐ Ensure that cybersecurity is always considered when the organization evaluates potential vendors and shares data with third parties.
- ☐ Integrate an assessment of an organization's cybersecurity when considering mergers and acquisitions.
- ☐ Institute an annual review of the organization's cybersecurity policies.
- ☐ Encourage technical personnel to engage in voluntary information sharing about cybersecurity threats and incidents.