Cybersecurity Capacity-building Tool Box for Financial Organizations

Board-Level Guide: Cybersecurity Leadership

Fundamentals of Cyber Risk Governance

Confirm that you can affirmatively answer the following questions:

1. Has your organization **met relevant statutory and regulatory requirements**?

2. Has your organization **quantified its cyber exposures and tested its financial resilience**?

3. Does your organization have an **improvement plan** in place to ensure exposures are within your agreed-upon risk appetite?

4. Does the board regularly **discuss concise, clear, and actionable information regarding the organization's cyber resilience supplied by management**?

5. Does your organization have **incident response plans in place that have been recently dry-run exercised**, including at board-level?

6. Are the **roles of key people responsible for managing cyber risk** clear and aligned with the three lines of defense?

7. Have you obtained **independent validation and assurance** of your organization's cyber risk posture?

Oversight

As the highest level of your organization's leadership, the board assumes ultimate accountability for governing cyber risk and therefore must oversee the organization's strategy, policies, and activities in this area. Specifically, the board should:

⇒ Take ultimate responsibility for oversight of cyber risk and resilience, whether as the full board or through delegation of oversight to a specific board committee.
⇒ Assign one corporate officer, usually the CISO, to be accountable for reporting on your organization's capability to manage cyber resilience and progress in implementing cyber resilience goals. Ensure that this officer has regular board access, sufficient authority, command of the subject matter, experience, and resources to fulfill these duties.
⇒ Annually define your organization's risk tolerance; ensure consistency with your corporate strategy and risk appetite.
⇒ Ensure that a formal, independent cyber resilience review of your organization is carried out annually.
⇒ Oversee the creation, implementation, testing, and ongoing improvement of cyber resilience plans, ensuring aligned across your organization and that your CISO or other accountable officer regularly reports on them to the board.
⇒ Integrate cyber resilience and risk assessment into your organization's overall business strategy, risk management, budgeting, and resource allocation, with the goal of fully integrating cyber risk into overall operational risk.
⇒ Periodically review your performance of the above and consider independent advice for continuous improvement.

Staying Informed

The board's effective cyber risk oversight depends on members' command of the subject and up to date information.

⇒ Ensure that all individuals joining the board have appropriate and up-to-date skills and knowledge to understand and manage the risks posed by cyber threats.
⇒ Solicit regular advice from management on your organization's current and future risk exposure, relevant regulatory requirements, and industry and societal benchmarks for risk appetite. Further, engage in regular briefings on latest developments with respect to the threat landscape and regulatory environment, joint planning and visits to best practice peers and leaders in cybersecurity, and board-level exchanges on governance and reporting.
⇒ Hold management accountable for reporting a quantified and understandable assessment of cyber risks, threats, and events as a standing agenda item during board meetings.
⇒ Maintain awareness of ongoing systemic challenges such as supply chain vulnerabilities, common dependencies, and the gap in information sharing between boards on cyber risk governance.

Setting the Tone

Alongside senior management, the board must set and exemplify your organization's core values, risk culture, and expectations with regard to cyber resilience.

⇒ Promote a culture in which staff at all levels recognize their important responsibilities in ensuring your organization's cyber resilience. Lead by example.
⇒ Oversee management's role in fostering and maintaining your organization's risk culture. Promote, monitor, and assess the risk culture, considering the impact of culture on safety and soundness and making changes where necessary.
⇒ Make clear that you expect all staff to act with integrity and to promptly escalate observed non-compliance within or outside your organization.

CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE · SWIFT INSTITUTE · FS-ISAC · Standard Chartered · CYBER READINESS INSTITUTE · GLOBAL CYBER ALLIANCE