Cyber-Risk Oversight:

Key Principles and Practical Guidance for Corporate Boards in Europe

Summary

Boards are increasingly focused on addressing cyber threats.

The ISA's cyber-risk handbooks (also available for US, UK, Japan and Latin America) are an attempt to provide Board members with a simple and coherent framework to understand cyber risk, as well as a series of straight-forward questions for Boards to ask management to assure that their organisation is properly addressing its unique cyber-risk posture.

The handbook—developed in partnership between ISA, Ecoda and AIG — will promote continued adoption of uniform cybersecurity principles for corporate Boards not only in Europe but across the globe. A summary of the 5 principles for managing cyber risk is below, along with key recommendations and links to practical toolkits.

The full handbook can be found here

Principle 1

Directors need to understand and approach cybersecurity as an enterprise-wide risk management issue, not just an IT issue.

Key recommendations:

- Information security should not be considered as purely a technical issue left to the IT department;
- Cybersecurity has to be perceived as an enterprise-wide risk management issue through the whole life cycle of the company;
- The risk-oversight should be a function of the full board;
- The board should not rely on a one-size-fits-all approach, they have to define their own tailor-made plans;
- The board should develop the right culture inside the company to ensure that all employees take cybersecurity as a serious matter;
- The management's duty is to make information related to the prevention, detection and response capabilities and knowledge of the maturity scale in which the company operates, available to the board. In doing so, the management should not consider only the organisation's own networks but its larger ecosystem.

Tool Kits

Toolkit A for suggested questions to include in the Board Review & Self Assessment to help assess the Board's level of understanding of cybersecurity issues or cyber literacy

Toolkit B for a list of cybersecurity questions that directors can ask management on issues such as strategy, risk assessment, prevention measures, incident, incident response, and post-breach response and communication

Toolkit C for related questions that directors can ask to promote optimal performance metrics and reporting

Toolkit D for cybersecurity considerations related to mergers and acquisitions.

Toolkit E for references to international standards

Principle 2

Directors should understand the reputational and legal implications of cyber risks as they relate to their company's specific circumstances.

Key recommendations:

- Cybersecurity is not just about reputational issues, it is also about liability of board members;
- Board members should have a good knowledge of the existing legislations be at European or national level, or even Industry-specific in order to exercise properly their duty of care.

Principle 3

Boards should ensure adequate access to cybersecurity expertise, and appropriate reporting, at both Board and Committee level.

Key recommendations:

- Board members should employ the same principles of inquiry and constructive challenge as for strategic decisions;
- The board has the duty to precisely specify its expectations to the management and be directive in the type of information they wish to receive;
- Even if Cybersecurity is entrusted to a specific committee, the full board should feel concerned and get at least quarterly debriefings from the management;
- Cybersecurity should not be treated as a stand-alone topic, it has to be embedded in all dimensions of the company's strategy.

Tool Kits

Toolkit B for aspects on the cyber risk management team and organisations

Toolkit C for possible questions on and examples of cyber-risk reporting metrics and dashboards

Principle 4

Board directors should ensure that management establishes an enterprise-wide cyber-risk management framework which encompasses culture, preventive, detective and response capabilities, monitoring and communication at all levels. Resources should be adequate and allocated appropriately by the strategies adopted.

Key recommendations:

- The management should establish both an enterprise-wide technical framework (mobile devices, AI, ...) as well as a systematic framework (with a forward-looking approach) that will facilitate board oversight of cyber risk;
- The management should have an integrated approach to cyber risk in order to establish a clear accountability framework, clear processes and communication guidelines;
- The management should opt for a bottom-up aggregation approach;
- The board and the management should set the tone at the top and develop the right culture and raise awareness to develop Cyber-resilience.

Principle 5

Board discussion about cyber risk should include strategies on their management (mitigation, transfer through insurance or partnerships, etc).

Key recommendations:

- The board should consider the return on cyber investments and shift to a risk-based approach;
- Cybersecurity must be conceptualised as a measure of future loss.

For more information about the handbook please contact the Internet Security Alliance.

Mark Camillo
Head of Cyber, EMEA
AIG
T +44 (0)20 7651 6304
M +44 (0)78 6026 1692
mark.camillo@aig.com

Sebastian Hess
Cyber Risk Advisor, EMEA
AIG
T +49 69 97113-572
M +49 159 04611288
sebastian.hess@aig.com

Larry Clinton
President
Internet Security Alliance
T (001) 703-907-7090
lclinton@isalliance.org

Béatrice Richez-Baum
Director General
ecoDa
T +32 2 231 58 11
M +32 498 502 687
beatrice.richez-baum@ecoda.org