Allianz für Cyber-Sicherheit

INTERNET SECURITY ALLIANCE

Managing Cyber Risk

A Handbook for German Boards of Directors

PRINCIPLE 1

Boards need to understand that cybersecurity is not just an IT issue

Directors need to understand and approach cybersecurity as a strategic, enterprise risk, not just an IT risk.

PRINCIPLE 2

Boards should be aware of existing legal issues in cybersecurity

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

PRINCIPLE 3

Boards should have adequate access to cyber expertise

Boards should have adequate access to cybersecurity expertise, and discussions about cyber-risk management should be given regular and adequate time on board meeting agendas.

PRINCIPLE 4

Boards should demand from management a framework for cybersecurity

Directors should require that management provide an enterprise-wide technical and structural framework for cyber-risk management with adequate staffing and budget.

PRINCIPLE 5

Boards should demand from management a clear and comprehensive cyber risk assessment

Board-management discussions about cyber risk should include identification and quantification of financial exposure to cyber risks and which risks to accept, mitigate, or transfer, such as through insurance, as well as specific plans associated with each approach.

PRINCIPLE 6

Boards should encourage systemic collaboration

Boards should encourage collaboration and sharing of best practices.