CONCEPT

Cybersecurity Governance and Cyber Risk Management for Executives and Boards

CONCEPT

Cybersecurity Governance and Cyber Risk Management for Executives and Boards

Technical depth: Conceptual · **Practical mode:** Case study

Introduction

Cyber incidents now halt operations, trigger disclosure duties and move share prices, yet many boards still receive technical reports they cannot act on. Security budgets are approved without a stated risk appetite, and accountability between executives, the security function and assurance remains blurred. This Core Concept course equips executives to direct and oversee cyber risk as an enterprise risk, using recognised governance frameworks and quantified risk information. Participants examine case material from several sectors and leave with a Cyber Risk Governance Pack ready for their own board or executive committee.

Course Objectives

- Evaluate the maturity of an organisation's cyber governance using the NIST CSF 2.0 Govern function and the Three Lines Model
- Direct cyber risk governance through ISO/IEC 27014, COBIT 2019 and recognised board oversight principles
- Set a cyber risk appetite and interpret quantified risk information to prioritise security investment
- Challenge management on third-party, ransomware, insurance and emerging technology exposures
- Specify the dashboard, indicators and reporting cycle the board needs for effective oversight
- Approve a Cyber Risk Governance Pack that clarifies accountabilities and decision rights

Target Audience

- Board and audit or risk committee members overseeing cyber risk
- Chief executives and general managers accountable for enterprise resilience
- Chief information, digital and technology officers directing technology strategy
- Chief risk, compliance and legal officers integrating cyber risk into enterprise risk management
- Chief information security officers reporting to executive committees and boards
- Chief financial and operating officers approving security investment and risk transfer

Course Outline

Day 1: Cyber Risk as an Enterprise Risk

- Board-Level Threat Briefing Using MITRE ATT&CK Adversary Profiles
- Integrating Cyber Risk into ISO 31000:2018 and COSO ERM
- Accountability Design with the IIA Three Lines Model and CISO Reporting Lines
- Cyber Governance Maturity Baseline Using the NIST CSF 2.0 Govern Function
- Comparative Disclosure and Resilience Regimes: NIS2, DORA and Listed-Company Rules

Day 2: Governance Frameworks and Oversight Principles

- ISO/IEC 27014:2020 Governance Processes: Evaluate, Direct, Monitor and Communicate
- COBIT 2019 Governance and Management Objectives EDM03, APO12 and APO13
- NACD-ISA Director's Handbook on Cyber-Risk Oversight: Six Oversight Principles
- World Economic Forum Principles for Board Governance of Cyber Risk
- Cyber Governance Charter and Committee Terms of Reference

Day 3: Directing Cyber Risk Decisions

- Cyber Risk Appetite and Tolerance Statement
- Cyber Risk Quantification with the FAIR Model
- Enterprise Cyber Risk Register and Heat Map Aligned to ISO/IEC 27005:2022
- Security Investment Case: Risk Reduction per Unit of Spend
- Key Risk Indicators and Board Cyber Dashboard Design

Day 4: Exposures, Crises and Emerging Risk

- Supply Chain Cyber Risk Oversight with NIST SP 800-161 Rev. 1
- Cyber Insurance Evaluation and Risk Transfer Decisions
- Ransomware Crisis Decisions: Payment, Disclosure and Recovery Trade-offs
- AI Risk Oversight with ISO/IEC 42001:2023
- Security Culture Assessment and Leadership Tone Indicators

Day 5: Case Work and the Cyber Risk Governance Pack

- Financial Services Case Study: Board Oversight after a Customer Data Breach
- Manufacturing Case Study: Operational Shutdown and Recovery Governance
- Cyber Risk Appetite Calibration for an Own Organisation
- Cyber Risk Governance Pack Drafting
- Executive Panel Challenge and Governance Pack Defence

Skills You Will Gain

- Cyber Risk Oversight
- Risk Appetite Setting
- Cyber Risk Quantification Literacy
- Security Investment Prioritisation
- Governance Structure Design
- Crisis Decision-Making
- Board Reporting Evaluation

Why Attend This Course

- Return with a Cyber Risk Governance Pack ready to table at your board or executive committee
- Ask the questions that expose weak assumptions in security reports and investment proposals
- Recognise which cyber decisions belong to the board and which belong to management
- Test your views against executives from other sectors and countries facing comparable exposures

Conclusion

Cyber risk is governed well when leaders set clear appetite, assign accountability and receive information they can act on. This course moves from positioning cyber risk within enterprise risk management, through the principal governance frameworks and board oversight principles, to quantified decision-making and the supply chain, ransomware and emerging technology exposures that test governance most. The final day produces a Cyber Risk Governance Pack that participants take back to their board, giving them a defensible basis for directing and overseeing cyber risk.