Training Course on Cybersecurity Risk Assessment for Boards

Professional Development Training Course Outline

Category	CEOs and Directors	**Duration**	5 Days
Base Fee	$1,500 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

In today's interconnected digital landscape, **cybersecurity risk assessment** has transitioned from a technical IT concern to a paramount **board-level responsibility**. Organizations face an ever-growing array of sophisticated cyber threats, from **ransomware attacks** to **advanced persistent threats (APTs)**, demanding proactive and strategic oversight. This comprehensive training course empowers board members and executive leadership with the critical knowledge and practical tools to understand, evaluate, and govern their organization's cybersecurity posture effectively, ensuring business resilience and safeguarding shareholder value in the face of evolving digital risks.

Training Course on Cybersecurity Risk Assessment for Boards is specifically designed to bridge the gap between technical cybersecurity jargon and strategic business imperatives. Participants will gain actionable insights into identifying, quantifying, and mitigating **enterprise cyber risks**, fostering a robust **cyber governance framework**, and ensuring **regulatory compliance**. By enhancing the board's collective cyber literacy, this course cultivates a **security-aware culture** from the top down, enabling informed decision-making and protecting critical assets against the backdrop of an increasingly complex and dynamic **threat landscape**.

Programme Curriculum

Training Course on Cybersecurity Risk Assessment for Boards

Introduction

In today's interconnected digital landscape, **cybersecurity risk assessment** has transitioned from a technical IT concern to a paramount **board-level responsibility**. Organizations face an ever-growing array of sophisticated cyber threats, from **ransomware attacks** to **advanced persistent threats (APTs)**, demanding proactive and strategic oversight. This comprehensive training course empowers board members and executive leadership with the critical knowledge and practical tools

to understand, evaluate, and govern their organization's cybersecurity posture effectively, ensuring business resilience and safeguarding shareholder value in the face of evolving digital risks.

Training Course on Cybersecurity Risk Assessment for Boards is specifically designed to bridge the gap between technical cybersecurity jargon and strategic business imperatives. Participants will gain actionable insights into identifying, quantifying, and mitigating **enterprise cyber risks**, fostering a robust **cyber governance framework**, and ensuring **regulatory compliance**. By enhancing the board's collective cyber literacy, this course cultivates a **security-aware culture** from the top down, enabling informed decision-making and protecting critical assets against the backdrop of an increasingly complex and dynamic **threat landscape**.

Course Duration

5 days

Course Objectives

1. Equip board members with a clear understanding of trending **cyber threat vectors**, including **ransomware**, **phishing**, **supply chain attacks**, and **zero-day exploits**.
2. Establish effective **cybersecurity governance frameworks** aligning with industry best practices like **NIST Cybersecurity Framework** and **ISO 27001**.
3. Define and articulate the organization's **cyber risk appetite** and tolerance levels for various business units and critical assets.
4. Enhance the board's capacity for robust **cybersecurity oversight**, including understanding key metrics and reporting mechanisms.
5. Introduce methodologies for **quantitative cyber risk assessment**, enabling data-driven decision-making and investment prioritization.
6. Develop strategies for managing and mitigating **third-party cyber risks** and vendor vulnerabilities within the extended enterprise.
7. Ensure the board is prepared for effective **cyber incident response** and **crisis communication** in the event of a breach.
8. Navigate the complex landscape of **data privacy regulations** (e.g., **GDPR**, **CCPA**) and cybersecurity compliance mandates.
9. Foster organizational **cyber resilience** and **business continuity planning** to minimize disruption from cyber incidents.
10. Understand the role of **cyber insurance** in risk transfer and how to optimize coverage based on assessed risks.
11. Analyze the cybersecurity implications of **AI**, **IoT**, **cloud computing**, and other emerging technologies.
12. Recognize and address the **human element** in cybersecurity, including security awareness training and insider threat mitigation.
13. Guide strategic **cybersecurity investment** decisions based on risk assessment outcomes and business impact.

Organizational Benefits

- Boards will be empowered to make informed, risk-aware decisions that align cybersecurity investments with business objectives.
- Proactive identification and mitigation of critical cyber risks, leading to a stronger overall security posture.
- Greater adherence to evolving cybersecurity and data privacy regulations, minimizing legal and financial penalties.

- Effective crisis management and incident response capabilities safeguard the organization's reputation and customer trust.
- Minimized downtime and financial losses during cyber incidents, ensuring continuous operations.
- Strategic allocation of cybersecurity budget and resources to areas of highest risk and impact.
- Demonstrating strong cyber governance can enhance investor confidence and market valuation.
- Fostering a top-down culture of cybersecurity awareness and accountability throughout the organization.

Target Audience

1. Board Members (Executive and Non-Executive Directors)
2. C-Suite Executives (CEOs, CFOs, COOs, CIOs, CISOs)
3. Audit Committee Members
4. Risk Management Professionals
5. Legal and Compliance Officers
6. Senior Business Leaders
7. Corporate Governance Professionals
8. Chief Digital Officers

Course Outline

Module 1: The Evolving Cyber Threat Landscape & Board Accountability

- Understanding the contemporary **cyber threat landscape**: Ransomware, APTs, supply chain attacks, phishing, and social engineering.
- Shifting from IT problem to **board-level fiduciary duty**: Legal and ethical implications.
- Key cybersecurity terminology for non-technical leaders.
- Impact of cyber incidents on **shareholder value** and brand reputation.
- **Case Study: Equifax Data Breach**: Analyze the board's role, the financial fallout, and reputational damage.

Module 2: Cybersecurity Governance & Frameworks

- Establishing an effective **cybersecurity governance structure** within the organization.
- Overview of leading frameworks: **NIST Cybersecurity Framework**, **ISO 27001**, COBIT.
- Defining roles, responsibilities, and accountability for cybersecurity at all levels.
- Integrating cybersecurity into enterprise risk management (ERM).
- **Case Study: Target Data Breach**: Examine governance failures and the importance of integrated risk management.

Module 3: Cybersecurity Risk Assessment Methodologies for Boards

- Introduction to qualitative and quantitative **cyber risk assessment** approaches.
- Understanding risk identification, analysis, and evaluation at a strategic level.
- Key risk indicators (KRIs) and metrics for board reporting.
- Developing a **risk register** tailored for board oversight.
- **Case Study: Maersk Cyber Attack (NotPetya)**: Discuss the impact of a widespread attack and the need for comprehensive risk assessment.

Module 4: Defining & Communicating Cyber Risk Appetite

- Translating technical risks into business language for board understanding.
- Establishing organizational **cyber risk appetite** and tolerance levels.
- Communicating risk effectively to stakeholders, including investors and regulators.
- Balancing risk acceptance, mitigation, transfer, and avoidance strategies.
- **Case Study: Colonial Pipeline Ransomware**: Evaluate the trade-offs in risk acceptance and the real-world impact of operational disruption.

Module 5: Third-Party & Supply Chain Cyber Risk Management

- Identifying and assessing **third-party cyber risks** from vendors, partners, and cloud providers.
- Implementing due diligence processes for third-party security.
- Contractual agreements and service level agreements (SLAs) for cybersecurity.
- Managing the risks inherent in complex **supply chain ecosystems**.
- **Case Study: SolarWinds Supply Chain Attack**: Explore the systemic vulnerabilities and far-reaching consequences of supply chain compromise.

Module 6: Cybersecurity Incident Response & Crisis Management

- Board's role in **cyber incident response planning** and execution.
- Developing a robust **crisis communication strategy** for cyber breaches.
- Legal and forensic considerations during and after a cyber incident.
- Post-incident review and continuous improvement processes.
- **Case Study: WannaCry Ransomware**: Analyze multi-national responses and the importance of global collaboration in incident management.

Module 7: Regulatory Compliance & Data Privacy

- Overview of key **data privacy regulations**: **GDPR**, **CCPA**, HIPAA, etc.
- Board's responsibility in ensuring **data protection** and privacy.
- Understanding compliance frameworks and audit requirements.
- Consequences of non-compliance: Fines, legal action, and reputational damage.
- **Case Study: Marriott Data Breach**: Discuss regulatory scrutiny and the implications of massive data compromise under new privacy laws.

Module 8: Emerging Technologies & Future Cyber Risks

- Exploring the **cybersecurity implications of AI** and machine learning.
- Risks and opportunities presented by **Internet of Things (IoT)** deployments.
- Securing **cloud computing environments** at an executive level.
- Anticipating future **cyber threat vectors** and technological shifts.
- **Case Study: Deepfake & AI-Powered Fraud**: Illustrate the new frontiers of cyber threats and the need for proactive strategic foresight.

Training Methodology

This course employs a highly interactive and practical training methodology, designed for executive-level engagement. It combines:

- **Interactive Workshops**: Facilitated discussions, group exercises, and strategic simulations.
- **Real-World Case Studies**: In-depth analysis of high-profile cyber incidents, focusing on board-level implications.

- **Expert-Led Presentations**: Concise and impactful presentations from leading cybersecurity governance specialists.
- **Q&A Sessions**: Dedicated time for addressing specific concerns and challenges faced by board members.
- **Practical Framework Application**: Hands-on exercises applying governance and risk assessment frameworks to organizational scenarios.
- **Peer-to-Peer Learning**: Opportunities for participants to share experiences and best practices.

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.org or call *+254769199797*

Certification

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

a. The participant must be conversant with English.

b. Upon completion of training the participant will be issued with an Authorized Training Certificate

c. Course duration is flexible and the contents can be modified to fit any number of days.

d. The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

e. One-year post-training support Consultation and Coaching provided after the course.

f. Payment should be done at least a week before commence of the training, to Fineskill Training Center account, as indicated in the invoice so as to enable us prepare better for you.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
23 Nov 2026	27 Nov 2026	Online	$1,000

Start Date	End Date	Location	Price
23 Nov 2026	27 Nov 2026	Physical	$1,500
23 Nov 2026	27 Nov 2026	Physical	$3,000
23 Nov 2026	27 Nov 2026	Physical	$3,000
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 Nov 2026	Physical	$4,500
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 Nov 2026	Physical	$6,000

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now

Email: info@fineskilltrainingcenter.com | Website: www.fineskilltrainingcenter.com