Training Course on Cybersecurity Governance and Risk for Board Members

Professional Development Training Course Outline

Category	CEOs and Directors	**Duration**	10 Days
Base Fee	$3,000 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

In today's hyper-connected world, **cybersecurity** is no longer a purely technical concern but a critical **enterprise risk** demanding robust **board oversight**. Organizations face an ever-evolving landscape of sophisticated **cyber threats**, from nation-state actors to organized cybercrime syndicates. A single **data breach** can lead to devastating financial losses, severe reputational damage, and significant regulatory penalties. Training Course on Cybersecurity Governance and Risk for Board Members is specifically designed for **board members** to equip them with the essential knowledge, strategic frameworks, and practical tools to effectively fulfill their **fiduciary duties** in protecting organizational assets and ensuring **business continuity**.

This comprehensive program empowers **executive leadership** to navigate the complex intricacies of **cyber risk management**. Participants will gain a profound understanding of their strategic role in establishing a resilient **cybersecurity posture**, fostering a strong **security culture**, and implementing effective **governance frameworks**. By focusing on proactive **risk assessment**, compliance with emerging **regulatory requirements**, and strategic **incident response planning**, this course will enable board members to make informed decisions that safeguard their organizations against the escalating wave of **cyberattacks** and build lasting **digital trust**.

Programme Curriculum

Training Course on Cybersecurity Governance and Risk for Board Members

Introduction

In today's hyper-connected world, **cybersecurity** is no longer a purely technical concern but a critical **enterprise risk** demanding robust **board oversight**. Organizations face an ever-evolving landscape of sophisticated **cyber threats**, from nation-state actors to organized cybercrime syndicates. A single **data breach** can lead to devastating financial losses, severe reputational

damage, and significant regulatory penalties. Training Course on Cybersecurity Governance and Risk for Board Members is specifically designed for **board members** to equip them with the essential knowledge, strategic frameworks, and practical tools to effectively fulfill their **fiduciary duties** in protecting organizational assets and ensuring **business continuity**.

This comprehensive program empowers **executive leadership** to navigate the complex intricacies of **cyber risk management**. Participants will gain a profound understanding of their strategic role in establishing a resilient **cybersecurity posture**, fostering a strong **security culture**, and implementing effective **governance frameworks**. By focusing on proactive **risk assessment**, compliance with emerging **regulatory requirements**, and strategic **incident response planning**, this course will enable board members to make informed decisions that safeguard their organizations against the escalating wave of **cyberattacks** and build lasting **digital trust**.

Course Duration

10 days

Course Objectives

1. Enhance understanding of cyber threats, attack vectors, and their potential business impact.
2. Implement and oversee industry-leading frameworks like NIST Cybersecurity Framework, ISO 27001, and COBIT.
3. Develop robust processes for identifying, assessing, mitigating, and monitoring cyber risks.
4. Navigate the complexities of evolving data privacy and security regulations such as GDPR, CCPA, SEC cyber disclosure rules, and industry-specific mandates.
5. Champion organizational-wide cyber awareness and promote best practices from the top down.
6. Develop strategic plans for effective cyber incident response, recovery, and business continuity planning.
7. Understand how to strategically allocate resources for maximum cybersecurity ROI and risk reduction.
8. Manage vendor cybersecurity risk and ensure secure digital supply chains.
9. Grasp the role of cyber insurance and understand legal liabilities associated with data breaches.
10. Align cybersecurity strategy with overall organizational risk appetite and strategic objectives.
11. Understand key performance indicators (KPIs) and metrics for measuring the effectiveness of cybersecurity programs.
12. Comprehend the governance implications of AI, cloud security, and IoT on organizational cybersecurity.
13. Empower board members to confidently challenge, question, and provide oversight on all cyber risk matters.

Organizational Benefits

- Proactive cybersecurity governance safeguards public image and builds confidence with customers, partners, and stakeholders.
- Minimizes the financial impact of data breaches, ransomware attacks, and other cyber incidents.
- Avoids hefty fines and legal penalties associated with non-compliance.
- Ensures operations can quickly recover from cyber disruptions, maintaining critical services.
- Demonstrates a commitment to security, attracting and retaining customers in a risk-averse market.

- Ensures cybersecurity investments are strategic and deliver tangible value.
- Demonstrates strong governance and risk management, appealing to discerning investors.
- Moves from a reactive to a proactive stance against evolving cyber threats.

Target Audience

1. Board Members (Executive & Non-Executive)
2. Audit Committee Members
3. Risk Committee Members
4. Chief Executive Officers (CEOs)
5. Chief Financial Officers (CFOs)
6. Corporate Secretaries & Legal Counsel
7. Senior Executives with Oversight Responsibilities
8. Aspiring Board Members & High-Potential Leaders

Course Outline

Module 1: The Evolving Cyber Threat Landscape for Boards

- Understanding the current global cyber threat intelligence and emerging trends.
- Examining the motivation and capabilities of various threat actors (nation-states, organized crime, insiders).
- Analyzing the growing attack surface due to digital transformation and cloud adoption.
- The profound business, financial, and reputational impacts of significant cyber incidents.
- **Case Study:** The Colonial Pipeline Ransomware Attack: Analyzing the operational disruption and its impact on critical infrastructure.

Module 2: Board's Fiduciary Duties in Cybersecurity

- Legal and ethical obligations of board members regarding cybersecurity oversight.
- Understanding the "duty of care" and "duty of loyalty" in the context of cyber risk.
- Recent regulatory shifts and increased personal liability for board members (e.g., SEC disclosure rules).
- Establishing clear roles and responsibilities for cybersecurity within the board and executive team.
- **Case Study:** The Equifax Data Breach: Examining the board's oversight failures and subsequent legal ramifications.

Module 3: Cybersecurity Governance Frameworks & Best Practices

- Introduction to leading cybersecurity frameworks: NIST Cybersecurity Framework, ISO 27001, COBIT.
- Mapping organizational cybersecurity efforts to recognized governance models.
- Developing a fit-for-purpose cybersecurity governance structure.
- Integrating cybersecurity into the broader enterprise risk management (ERM) framework.
- **Case Study:** Implementing the NIST CSF at a large financial institution to mature their cyber program.

Module 4: Strategic Cyber Risk Assessment & Measurement

- Methods for identifying and prioritizing critical cyber risks relevant to the organization's strategic objectives.
- Understanding risk appetite and tolerance in a cyber context.

- Techniques for quantifying cyber risk and communicating it effectively to the board.
- Distinguishing between technical vulnerabilities and strategic business risks.
- **Case Study:** A manufacturing company's approach to assessing OT (Operational Technology) cybersecurity risks following a supply chain disruption.

Module 5: Building a Resilient Cyber Culture

- The board's role in championing a security-first mindset across the organization.
- Strategies for fostering cyber awareness and accountability at all levels.
- Integrating cybersecurity considerations into employee performance and incentives.
- The importance of "leading by example" in cyber hygiene and awareness.
- **Case Study:** A global retail corporation's initiative to transform its security culture after multiple phishing attacks.

Module 6: Effective Cyber Incident Response & Business Continuity

- Key components of a robust cyber incident response plan (IRP).
- The board's role during a major cyber crisis: communication, decision-making, and oversight.
- Strategies for maintaining business continuity and minimizing disruption post-incident.
- Conducting tabletop exercises and simulations to test incident response capabilities.
- **Case Study:** A healthcare provider's successful navigation of a ransomware attack, emphasizing their pre-planned incident response.

Module 7: Cybersecurity Investment & Resource Allocation

- Evaluating the effectiveness of current cybersecurity spend and identifying gaps.
- Metrics for demonstrating the return on investment (ROI) of cybersecurity initiatives.
- Prioritizing security controls and technologies based on risk and business value.
- Understanding the role of the CISO and adequate resourcing for the cybersecurity function.
- **Case Study:** A technology firm's strategic shift in cybersecurity budgeting, moving from reactive to proactive investments.

Module 8: Third-Party & Supply Chain Cyber Risk Management

- Assessing and managing cybersecurity risks introduced by vendors, partners, and the extended supply chain.
- Establishing due diligence processes for third-party cybersecurity.
- Contractual agreements and service level agreements (SLAs) for security.
- Monitoring and auditing third-party security posture.
- **Case Study:** The SolarWinds Supply Chain Attack: Lessons learned for board oversight of vendor risk.

Module 9: Data Privacy, Regulatory Compliance & Legal Landscape

- Deep dive into major data privacy regulations (GDPR, CCPA, HIPAA, PIPEDA).
- Understanding breach notification requirements and their implications.
- The evolving landscape of cyber liability and litigation.
- Best practices for demonstrating compliance and preparing for audits.
- **Case Study:** A multinational company's journey to achieve GDPR compliance and the role of the board in overseeing this transformation.

Module 10: Cyber Insurance and Risk Transfer

- Understanding the scope and limitations of cyber insurance policies.

- Key considerations when purchasing or renewing cyber insurance.
- The interplay between cyber insurance, incident response, and legal counsel.
- Assessing the adequacy of current cyber insurance coverage.
- **Case Study:** An organization's experience with a cyber insurance claim following a significant data breach, highlighting coverage nuances.

Module 11: Cybersecurity Reporting & Board Engagement

- Effective communication strategies for reporting cyber risk to the board.
- Developing clear, concise, and actionable cybersecurity dashboards and metrics.
- Asking the right questions to challenge management on cybersecurity posture.
- Fostering productive dialogue between the board, CISO, and IT leadership.
- **Case Study:** How a progressive board implemented a regular cyber risk reporting cadence, leading to more informed decisions.

Module 12: Emerging Technologies & Future Cyber Risks (AI, Cloud, IoT)

- The cybersecurity implications of Artificial Intelligence (AI) and Machine Learning (ML).
- Governance considerations for secure cloud adoption and multi-cloud environments.
- Managing the security risks of the Internet of Things (IoT) and Operational Technology (OT).
- Anticipating and preparing for future cyber threats stemming from technological advancements.
- **Case Study:** A smart city initiative's challenges in securing its IoT infrastructure and leveraging AI for threat detection.

Module 13: Mergers, Acquisitions & Divestitures: Cyber Due Diligence

- Integrating cybersecurity risk assessment into M&A due diligence processes.
- Identifying hidden cyber liabilities in target companies.
- Strategies for post-merger integration of cybersecurity frameworks and controls.
- Managing cyber risks during divestitures and asset sales.
- **Case Study:** A corporate acquisition that uncovered significant cybersecurity weaknesses in the target company, impacting valuation.

Module 14: Crisis Communications & Stakeholder Management

- Developing a strategic communication plan for cyber incidents.
- Managing internal and external communications during a crisis.
- Engaging with regulators, law enforcement, and legal counsel.
- Protecting organizational reputation through transparent and timely communication.
- **Case Study:** A high-profile company's public relations response to a major data breach, evaluating effective and ineffective strategies.

Module 15: Board Resilience & Continuous Learning

- Strategies for ongoing board education and development in cybersecurity.
- Leveraging external experts and independent assessments.
- Building a culture of continuous improvement in cyber governance.
- The role of the board in championing organizational resilience beyond technical security.
- **Case Study:** A board's commitment to regular cybersecurity workshops and external advisory, leading to demonstrable improvements in posture.

Training Methodology

This course will employ an **interactive and experiential learning approach** tailored for board members. It will combine:

- **Expert-led lectures and discussions** (minimizing jargon, focusing on strategic implications)
- **Real-world case studies** (analyzing high-profile breaches and successful governance models)
- **Interactive group exercises** (simulating board-level decision-making scenarios)
- **Q&A sessions with industry leaders** (facilitating direct engagement and insights)
- **Practical frameworks and tools** (providing actionable takeaways for immediate application)
- **Peer-to-peer learning and networking** (fostering collaborative problem-solving)

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

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
23 Nov 2026	04 Dec 2026	Online	$2,000

Start Date	End Date	Location	Price
23 Nov 2026	04 Dec 2026	Physical	$3,000
23 Nov 2026	04 Dec 2026	Physical	$6,000
23 Nov 2026	04 Dec 2026	Physical	$6,000
23 Nov 2026	04 Dec 2026	Physical	$12,000
23 Nov 2026	04 Dec 2026	Physical	$9,000
23 Nov 2026	04 Dec 2026	Physical	$12,000
23 Nov 2026	04 Dec 2026	Physical	$12,000

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

Register Online Now

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