Cyber Risk for Non-Tech Executives Training Course

Professional Development Training Course Outline

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

Course Introduction

In today's digitally driven landscape, cyber risk is no longer a peripheral IT problem but a core business continuity challenge and a matter of fiduciary duty. Non-technical executives and board members are increasingly accountable for organizational cyber resilience and must move beyond basic awareness to strategic oversight. Cyber Risk for Non-Tech Executives Training Course is specifically designed to equip senior leaders with the strategic framework necessary to integrate cybersecurity into enterprise risk management. We demystify complex technical jargon, translating concepts like Zero Trust and Supply Chain Risk into clear, actionable business imperatives that protect shareholder value and ensure data privacy compliance.

The modern threat environment, characterized by sophisticated ransomware-as-a-service attacks and pervasive cloud security vulnerabilities, demands proactive, informed leadership. Failure to adequately address digital transformation risks can lead to catastrophic data breaches, significant regulatory fines, and severe reputational damage. This program provides the essential tools for executives to establish a robust security culture, effectively challenge their security teams, and make informed cyber insurance and incident response investment decisions. By mastering these non-technical, strategic cyber principles, participants will transform cyber risk from a paralyzing threat into a manageable and competitive business advantage

Programme Curriculum

Cyber Risk for Non-Tech Executives Training Course

Introduction

In today's digitally driven landscape, cyber risk is no longer a peripheral IT problem but a core business continuity challenge and a matter of fiduciary duty. Non-technical executives and board members are increasingly accountable for organizational cyber resilience and must move beyond basic awareness to

strategic oversight. Cyber Risk for Non-Tech Executives Training Course is specifically designed to equip senior leaders with the strategic framework necessary to integrate cybersecurity into enterprise risk management. We demystify complex technical jargon, translating concepts like Zero Trust and Supply Chain Risk into clear, actionable business imperatives that protect shareholder value and ensure data privacy compliance.

The modern threat environment, characterized by sophisticated ransomware-as-a-service attacks and pervasive cloud security vulnerabilities, demands proactive, informed leadership. Failure to adequately address digital transformation risks can lead to catastrophic data breaches, significant regulatory fines, and severe reputational damage. This program provides the essential tools for executives to establish a robust security culture, effectively challenge their security teams, and make informed cyber insurance and incident response investment decisions. By mastering these non-technical, strategic cyber principles, participants will transform cyber risk from a paralyzing threat into a manageable and competitive business advantage

Course Duration

5 days

Course Objectives

Upon completion, participants will be able to:

1. Establish effective Cyber Governance structures aligned with Enterprise Risk Management (ERM).
2. Translate technical Cyber Threat Intelligence (CTI) into strategic, board-level business risk reports.
3. Define and enforce key Data Privacy and Regulatory Compliance mandates
4. Evaluate the financial impact and ROI of Cyber Resilience investments.
5. Implement the principles of Zero Trust Architecture from a policy and oversight perspective.
6. Develop robust, organization-wide Incident Response Planning (IRP) and Business Continuity strategies.
7. Assess and mitigate systemic Supply Chain Risk Management and Third-Party Vendor vulnerabilities.
8. Understand and effectively utilize Cyber Insurance policies and coverage.
9. Identify and champion the necessary organizational shift towards a proactive Security Culture.
10. Oversee the security implications of Cloud Migration and Digital Transformation initiatives.
11. Interpret key Security Metrics and KPIs for executive decision-making.
12. Mitigate the specific threat of Ransomware-as-a-Service (RaaS) and extortion demands.
13. Fulfill their Fiduciary Duty concerning cyber oversight and Shareholder Value protection.

Target Audience

1. Chief Executive Officers (CEOs)
2. Board Directors & Non-Executive Directors (NEDs)
3. Chief Financial Officers (CFOs)
4. Chief Operating Officers (COOs)
5. Chief Legal Officers (CLOs) / General Counsel
6. Heads of Business Units & P&L Owners
7. Chief Human Resources Officers (CHROs)
8. Audit and Risk Committee Members

Course Modules

Module 1: The Executive's Cyber Mindset: Risk vs. Technology

- Cybersecurity as a Business Risk, not an IT cost center.
- Understanding the Threat Landscape.

- Fiduciary Duty and Executive Liability in the face of a breach.
- Integrating Cyber Governance into Enterprise Risk Management (ERM).
- Case Study: The Target Data Breach.

Module 2: Governance, Risk, and Compliance (GRC) Essentials

- Translating NIST CSF and ISO 27001 into strategic business actions.
- Data Privacy Legislation.
- Regulatory Compliance oversight and reporting to the board.
- Establishing a Cyber Risk Appetite and tolerance level.
- Case Study: Equifax's regulatory fines.

Module 3: Strategic Threat Intelligence & Metrics

- Understanding and consuming relevant Cyber Threat Intelligence (CTI).
- Key Security Metrics (KPIs) for executive review
- The business-centric view of vulnerability and asset management.
- Effective communication: Reporting cyber status to the Board and investors.
- Case Study: How a major bank translates its daily CTI feed into quarterly risk adjustments and capital allocation.

Module 4: Cloud and Digital Transformation Risk

- Cyber risks specific to Cloud Migration
- Oversight of SaaS, PaaS, and IaaS security responsibilities
- Securing the remote workforce and the Hybrid Work environment.
- The strategic implications of DevSecOps on business agility.
- Case Study: A company's exposure from a publicly accessible S3 bucket following a rapid cloud deployment.

Module 5: Third-Party & Supply Chain Risk Management

- Identifying critical Supply Chain Vulnerabilities
- Due diligence and contractual requirements for third-party vendors.
- Continuous monitoring and auditing of vendor security posture.
- Defining vendor Risk Tiers and acceptable risk levels.
- Case Study: The Colonial Pipeline attack.

Module 6: Incident Response & Business Continuity

- Developing an Executive-led Incident Response Plan
- Critical decision-making during an active Ransomware event
- Maintaining Business Continuity and disaster recovery protocols.
- Crisis communications strategy for internal and external stakeholders.
- Case Study: A global manufacturer’s coordinated response to a massive Wiper malware attack, focusing on communication and recovery.

Module 7: Cyber Insurance and Investment Oversight

- Evaluating Cyber Insurance policy coverage, exclusions, and deductibles.
- The relationship between security maturity and insurance premiums/eligibility.
- Making informed decisions on Security Budget and strategic technology investments.

- Understanding the business case for Zero Trust Architecture implementation.
- Case Study: Analyzing a claim denial scenario due to an organization's failure to maintain "reasonable" security controls required by the policy.

Module 8: Building a Security Culture and Leadership

- The role of executive leadership in fostering a proactive Security Culture.
- Managing the relationship between the CISO and other C-suite roles.
- Addressing the "Human Factor" via continuous Security Awareness Training.
- Implementing governance over Identity and Access Management (IAM).
- Case Study: How a major technology firm successfully integrated security into its performance metrics and corporate values.

Training Methodology

This course employs a participatory and hands-on approach to ensure practical learning, including:

- Interactive lectures and presentations.
- Group discussions and brainstorming sessions.
- Hands-on exercises using real-world datasets.
- Role-playing and scenario-based simulations.
- Analysis of case studies to bridge theory and practice.
- Peer-to-peer learning and networking.
- Expert-led Q&A sessions.
- Continuous feedback and personalized guidance.

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
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