JUPITER PRIME

Consulting • Training • Advisory

جوبيتر برايم للاستشارات والتدريب

COURSE BROCHURE

Advanced Cybersecurity Leadership and Board Strategy Course

31 January – 11 February 2027
Muscat

Advanced Cybersecurity Leadership and Board Strategy Course

Ref: 199_6054 **Date:** 31 January – 11 February 2027 **Location:** Muscat **Fees:** 11700 GBP

Cybersecurity Leadership and Board Strategy is a 2-week advanced training course for CISOs, IT directors and non-technical executives who answer to the board for cyber risk, and it ends with a three-horizon cyber security strategy roadmap. Boards now treat a major breach as a business continuity and reputation event rather than an IT fault, so the quality of security leadership shows up in valuation and trust. Jupiter Prime Training runs this course for leaders who carry that accountability.

Why Cybersecurity Leadership and Board Strategy Matters Now

Three groups are reshaping the role: directors who expect cyber exposure explained in the same language as credit or market risk, insurers and investors who price an organisation's security posture before they commit, and attackers who time extortion to coincide with results announcements or mergers. Leaders who set a clear risk appetite and fund controls against it keep incidents contained and disclosures orderly; those who do not face surprise losses and lost confidence. The course rests on the NIST Cybersecurity Framework 2.0 NIST CSF 2.0, whose Govern function places cyber risk inside enterprise strategy, and refers to ISO/IEC 27001:2022 for management system structure.

Who Gains Most from Cybersecurity Leadership and Board Strategy

- Security chiefs who set the cyber strategy and defend its budget before the executive committee
- Technology directors who balance digital transformation speed against control coverage
- Risk and audit committee members who challenge management on cyber exposure
- Operating executives who own the business services an attack would disrupt
- Chief financial and legal officers who weigh cyber insurance, disclosure and liability

An executive committee that sends its security chief alongside finance, legal and operations leaders gains most, because the roadmap needs agreement on risk appetite across those functions.

Cybersecurity Leadership and Board Strategy Capabilities

Participants leave able to translate threat and control facts into choices a board can approve, fund and track.

- Calculate cyber risk exposure in financial terms using scenario-based quantification — board risk appetite decisions
- Align the security strategy with business priorities and digital investment plans — chief executive and strategy office
- Weigh budget options across prevention, detection and recovery — finance committee approval
- Design governance structures, committee charters and decision rights for cyber risk — directors and audit committee
- Apply crisis leadership routines during a major breach — executive crisis team and communications
- Communicate cyber posture through concise board metrics and narratives — non-executive directors and investors

Key Cybersecurity Leadership and Board Strategy Terms

- Cyber risk appetite — The amount and type of cyber-related loss an organisation's board is willing to accept in pursuit of its objectives.
- Cyber risk quantification — Expressing likely cyber losses as financial ranges so they can be compared with other enterprise risks and investments.
- Security posture — The overall strength of an organisation's defences, detection and recovery capability at a given point in time.
- Govern function — The part of NIST CSF 2.0 that sets cyber strategy, roles, policy and oversight within enterprise risk management.
- Key risk indicator — A metric that signals rising exposure early, such as unpatched critical systems or privileged accounts without review.
- Cyber resilience — The ability to keep critical services running through an attack and restore them quickly afterwards.

Cybersecurity Leadership and Board Strategy Day by Day

Day 1: The Board's View of Cyber Exposure

- Director Duties and Cyber Oversight — Accountability at Board Level
- Threat Actor Motives and Business Models — Exposure by Sector
- Cyber Risk in Enterprise Risk Registers — Comparison with Other Principal Risks
- Investor and Insurer Expectations — Signals That Affect Valuation and Cover
- Leadership Self-Assessment — Current Gaps in Security Oversight

Day 2: Frameworks for Executive Oversight

- NIST CSF 2.0 Govern Function — Strategy, Roles and Oversight Expectations
- NIST CSF Profiles and Tiers — Target State Ambition
- ISO/IEC 27001:2022 Management System Structure — Assurance for Directors
- Three Lines Model for Cyber — Separation of Ownership and Challenge
- Framework Selection Criteria — Fit with Organisation Size and Sector

Day 3: Setting Cyber Risk Appetite

- Risk Appetite Statements — Tolerance Levels for Critical Services
- Scenario-Based Loss Estimation — Ransomware, Data Theft and Fraud Cases
- Cyber Risk Quantification Methods — Financial Ranges for Decisions
- Crown Jewel Asset Identification — Protection Priorities for the Board
- Risk Acceptance and Exception Process — Who Signs Off Residual Exposure

Day 4: Building the Security Strategy

- Business Alignment Interviews — Linking Controls to Revenue and Operations
- Capability Maturity Assessment — Baseline Against Target Profile
- Zero Trust Principles — Architecture Direction for Leadership
- Digital Transformation Security Gates — Speed Versus Control Trade-Offs
- Strategic Initiative Portfolio — Sequencing Across Three Horizons

Day 5: Funding and Investment Decisions

- Security Budget Benchmarks and Drivers — Defending Spend to Finance
- Return on Security Investment Cases — Prioritising Competing Proposals
- Build, Buy or Outsource Choices — Managed Security Service Options
- Cyber Insurance Strategy — Retention, Cover and Exclusions
- Technical Debt and Legacy Systems — Retirement Versus Compensating Controls

Day 6: Governance Structures and Decision Rights

- Board and Committee Charters — Where Cyber Oversight Sits
- CISO Reporting Line Options — Independence Versus Influence
- Policy Hierarchy and Approval — Executive Ownership of Standards
- Third-Party and Supply Chain Oversight — Contract and Assurance Expectations
- Security Talent and Succession — Leadership Bench Strength

Day 7: Crisis Leadership in a Major Breach

- Executive Crisis Team Design — Roles, Authority and Escalation
- Ransom Payment Decision Framework — Legal, Ethical and Operational Factors
- Stakeholder and Media Communication — Disclosure Timing and Tone
- Business Continuity Activation — Service Priorities Under Attack
- Board Crisis Simulation — Decisions Under Incomplete Information

Day 8: Reporting Cyber Posture to the Board

- Board Metrics and Key Risk Indicators — Signals Directors Can Act On
- Cyber Posture Narrative — Translating Technical Findings into Business Impact
- Assurance Mapping — Internal Audit, External Testing and Certification
- Heat Maps Versus Quantified Reports — Choosing the Right Format
- Banking and Energy Board Reporting Cases — Sector Lessons

Day 9: Culture, Influence and Emerging Risk

- Security Culture Leadership — Tone from the Top and Accountability
- Executive Influence Techniques — Winning Support Without Fear Tactics
- AI and Automation Risks — New Exposure in Strategic Plans
- Mergers and Acquisitions Cyber Due Diligence — Deal Value Protection
- Geopolitical and Supply Disruption Scenarios — Strategy Stress Tests

Day 10: Practising the Cyber Security Strategy Roadmap

- Risk Appetite Applied to a Case Organisation — Tolerance Set by Service
- Initiative Prioritisation and Budget Allocation — Funded Horizon Plan
- Governance and Reporting Design — Committee Charter and Metric Set
- Board Presentation Rehearsal — Peer Challenge on Clarity and Ask
- Cyber Security Strategy Roadmap Completion — Initiatives, Owners and Milestones

Applying Cybersecurity Leadership and Board Strategy After the Course

- Draft a cyber risk appetite statement for the three most critical services and take it to the risk committee for challenge
- Replace the current board security report with a one-page posture narrative and a short set of key risk indicators

Cybersecurity Leadership and Board Strategy Questions FAQ

What is cybersecurity leadership and board strategy and why does it matter now?

Cybersecurity leadership and board strategy is the practice of setting cyber risk appetite, funding defences and overseeing security at executive level. It matters now because breaches affect valuation, insurance and trust, and directors are expected to show informed oversight.

Which roles gain most from cybersecurity leadership and board strategy training?

Security chiefs, technology directors, risk committee members and operating executives gain most. You benefit if you approve security budgets, report cyber exposure upward or would lead decisions during a major breach.

How does cybersecurity leadership and board strategy training differ from a technical security management course?

It focuses on decisions, funding and oversight rather than configuring controls or running operations. You work with risk appetite, quantification, governance design and board reporting, and leave technical depth to specialist courses.

What do you bring back from cybersecurity leadership and board strategy training?

You bring back a roadmap that ties security initiatives to business priorities and risk appetite. It lists funded initiatives, owners, milestones and the metrics the board will use to track progress.

Cybersecurity Leadership and Board Strategy: The Way Forward

The cyber security strategy roadmap first informs which initiatives the next budget cycle funds and which risks the board formally accepts. Security chiefs maintain it, executive owners deliver its initiatives and directors track it through quarterly metrics. After its first board review, revisit the risk appetite statements, because directors' questions usually show where tolerance was set too loosely or too tightly.