Faysal Aziz

Cyber Resilience Awareness for the Boardroom

Understanding the Threat, Governing the Risk, and Protecting Enterprise Value - 1 day

FA-0146 · 1 day

Cybersecurity

Introduction

Cybersecurity has become a matter of corporate resilience rather than technology alone. A serious cyber incident can interrupt essential operations, compromise sensitive information, enable fraud, damage public confidence, expose the organization to regulatory action, and require consequential decisions from directors under intense pressure.

This one-day executive programme provides Board members in the lottery and gaming industry with a focused understanding of the cyber risks that matter at governance level. It connects the global threat landscape with Malaysia's cybersecurity environment, examines the distinctive exposure created by transactional platforms, retail networks, customer information, payment dependencies, and third-party providers, and clarifies the Board's role in overseeing cybersecurity strategy and preparedness.

The programme also explains the strategic value of Security Operations Centre capabilities without overwhelming participants with technical detail. Board members will gain practical visibility into how continuous monitoring, threat detection, escalation, incident response, and executive reporting contribute to organizational resilience.

The content reflects current developments in ransomware, cyber-enabled fraud, identity compromise, social engineering, artificial intelligence-assisted attacks, supply-chain exposure, and operational disruption. It also recognizes Malaysia's strengthened national cybersecurity governance under the Cyber Security Act 2024 and the increasing importance of incident preparedness, risk assessment, and organizational accountability.

The programme will be delivered by an instructor with **over 30 years of industry experience**. The instructor will use practical, industry-demanded content and real operational insights rather than presenting cybersecurity as a purely academic subject.

Learning outcomes

Upon completion of the programme, participants will be able to:

- Understand the major threats shaping the global cybersecurity landscape.
- Recognize the principal cyber threats affecting Malaysian organizations.
- Identify cybersecurity risks relevant to the lottery and gaming industry.
- Understand the potential operational, financial, regulatory, and reputational consequences of a cyber incident.
- Distinguish the Board's governance responsibilities from management's operational responsibilities.
- Ask management more focused questions about cyber risk, preparedness, and investment.
- Understand the strategic purpose of a Security Operations Centre.
- Interpret essential Board-level cybersecurity measures and reports.
- Evaluate whether cybersecurity investments are strengthening organizational resilience.
- Contribute more effectively to executive decision-making before, during, and after a significant cyber incident.

Prerequisites

- No technical cybersecurity knowledge is required.
- Familiarity with corporate governance and enterprise risk management is beneficial.
- Participants should have a general understanding of the organization's business operations and strategic priorities.

Training outline

1. Cybersecurity as a Board-Level Business Risk

1. Evolution of cybersecurity from an IT concern to an enterprise risk
2. Relationship between cyber risk and organizational strategy
3. Operational, financial, regulatory, and reputational consequences
4. Cybersecurity within enterprise risk management
5. Difference between cybersecurity and cyber resilience
6. Board oversight versus management execution

2. Global Cybersecurity Threat Landscape and Emerging

Trends

1. Current cyber threat environment
2. Ransomware and data extortion
3. Cyber-enabled fraud and business email compromise
4. Identity and credential-based attacks
5. Supply-chain and third-party compromise
6. Artificial intelligence-assisted phishing and impersonation
7. Deepfake-enabled executive fraud
8. Cloud and digital service exposure
9. Growing speed and sophistication of cyber attacks
10. Strategic lessons from major cyber incidents

3. Malaysia's Current Cybersecurity Landscape

1. Cyber threats affecting Malaysian organizations
2. Online fraud and social engineering trends
3. Ransomware and malicious software
4. Data breaches and unauthorized information disclosure
5. Attacks against public-facing digital services
6. National cybersecurity governance
7. Cyber Security Act 2024
8. National Critical Information Infrastructure considerations
9. Cyber incident reporting and organizational readiness
10. Implications for Board oversight

4. Cyber Risks in the Lottery and Gaming Industry

1. Dependence on continuously available transactional systems
2. Protection of customer and commercially sensitive information
3. Digital platform and mobile application risks
4. Retail terminal and point-of-sale exposure
5. Payment, settlement, and reconciliation risks
6. Account takeover and credential abuse
7. Cyber-enabled fraud
8. Brand impersonation and customer-targeted scams
9. Third-party technology and service-provider dependencies

10. Insider threats and excessive access privileges
11. Operational disruption and service availability
12. Customer confidence and reputational consequences

5. Cybersecurity Governance and Board Responsibilities

1. Establishing clear oversight and accountability
2. Aligning cybersecurity strategy with business priorities
3. Defining cyber risk appetite and tolerance
4. Identifying critical business services and technology dependencies
5. Oversight of cybersecurity investment priorities
6. Oversight of third-party cyber risk
7. Oversight of incident preparedness and recovery capability
8. Board participation in cyber crisis exercises
9. Independent assurance and validation
10. Management accountability for unresolved cyber risks

6. Cybersecurity Best Practices for Board Members

1. Directors as high-value cyber targets
2. Executive identity and account protection
3. Multi-factor authentication
4. Secure handling of Board papers and confidential information
5. Secure use of email, mobile devices, and Board portals
6. Recognition of executive phishing and impersonation attempts
7. Verification of unusual financial or information requests
8. Deepfake voice and video awareness
9. Responsible use of generative artificial intelligence
10. Immediate reporting of suspected compromise

7. Questions the Board Should Ask Management

1. Most significant cyber risks facing the organization
2. Critical services most vulnerable to disruption
3. Current exposure compared with approved risk appetite
4. Adequacy of identity and privileged access controls
5. Visibility across critical systems and third-party connections

6. Effectiveness of threat detection and incident escalation
7. Readiness to contain and recover from ransomware
8. Integrity and recoverability of backups
9. Results of recent cybersecurity and crisis exercises
10. Status of material vulnerabilities and overdue remediation
11. Adequacy of cybersecurity resources and expertise
12. Evidence that cybersecurity investments are reducing risk

8. Strategic Value of Security Operations Centre Capabilities

1. Purpose of a Security Operations Centre
2. Continuous monitoring of critical technology environments
3. Collection and analysis of security events
4. Identification of suspicious behavior
5. Threat intelligence and emerging threat awareness
6. Detection of compromised accounts and malicious activity
7. Investigation and validation of security alerts
8. Prioritization of significant incidents
9. Escalation to operational and executive management
10. Coordination of containment and incident response
11. Support for regulatory and audit requirements
12. Contribution to organizational resilience

9. Understanding SOC Effectiveness

1. Visibility across critical business systems
2. Monitoring of customer-facing and transactional environments
3. Monitoring of privileged and administrative activities
4. Quality of threat detection
5. Speed of incident identification
6. Speed of escalation and containment
7. Coverage of critical assets and services
8. Quality of incident investigation
9. Capability to support major incident response
10. Internal, outsourced, and hybrid SOC operating models
11. Limitations of technology without skilled people and effective processes

12. Board-level reporting on SOC performance

10. Board-Level Cybersecurity Reporting

1. Business-focused cybersecurity reporting
2. Principal cyber risks and changes in exposure
3. Material incidents and near misses
4. Critical vulnerabilities
5. Third-party risk exposure
6. Detection and response performance
7. Recovery preparedness
8. Outstanding corrective actions
9. Regulatory readiness
10. Independent assurance findings
11. Decisions and risk acceptances requiring Board attention
12. Avoiding technical measures that do not demonstrate business value

11. Cyber Incident and Crisis Oversight

1. Board responsibilities before a cyber incident
2. Executive escalation and notification criteria
3. Crisis decision-making authority
4. Business continuity activation
5. Regulatory, legal, and stakeholder considerations
6. Customer and public communication
7. Oversight without interfering in operational response
8. Service restoration and recovery priorities
9. Post-incident review
10. Accountability for corrective actions
11. Lessons learned and future investment priorities

12. Strengthening Organizational Cyber Resilience

1. Moving beyond prevention
2. Protection of critical business services
3. Preparation for realistic cyber scenarios
4. Detection and response readiness

5. Tested backup and recovery capability
6. Third-party resilience
7. Executive crisis preparedness
8. Independent validation of controls
9. Risk-based cybersecurity investment
10. Continuous improvement
11. Board visibility into residual risk
12. Cyber resilience as a foundation for stakeholder confidence

Disclaimer

This training outline is provided as an indicative framework for the proposed executive programme and is intended to guide its overall scope and direction. The trainer reserves the professional discretion to amend, consolidate, reorder, expand, reduce, substitute, or otherwise adapt the content according to participant needs, organizational priorities, prevailing threat intelligence, regulatory developments, industry conditions, and the circumstances of delivery. Such modifications may be made without prior notice where the trainer considers them necessary to preserve the relevance, accuracy, balance, and effectiveness of the programme.

© 2026 Faysal Aziz · Kuala Lumpur