LES CONSULTANTS
CONSEIL & FORMATION

EN

CYBERSECURITY · RISK MANAGEMENT

Introduction to Cyber Risk Management

▲ 7 chapters ▲ Identifying, assessing, mitigating and governing cyber risk

7 CHAPTERS

▲ Training programme

1 Introduction to Cyber Risk

1.1 Cyber Risk Management
- Current challenges
- Training objectives

2 Cyber Threat Landscape

2.1 Main cyber threats
- Phishing
- Ransomware
- Business Email Compromise
- DDoS attacks
- Data breaches

2.2 Threat drivers
- Human weaknesses
- Organisational gaps
- System complexity

3 Cyber Risk Identification

3.1 Critical assets
- Data
- Systems
- Services

3.2 Vulnerabilities
- Technical
- Organisational
- Human

3.3 Incident scenarios
- Likelihood
- Impact

4 Cyber Risk Assessment

4.1 Risk assessment objectives
- Criticality
- Prioritisation

4.2 Risk evaluation
- Probability
- Impact

5 Risk Mitigation and Management

5.1 Prevention measures
- Access controls
- System updates
- Encryption

5.2 Detection mechanisms
- Monitoring
- Alerts
- Logging

5.3 Incident response
- Response plans
- Testing and drills

5.4 Recovery
- Business continuity
- Disaster recovery
- Backups

6 Cyber Governance and Awareness

6.1 Cyber governance
- Management oversight
- Security roles
- Compliance functions

6.2 Security culture
- Awareness
- Daily vigilance
- Incident reporting

7 Conclusion

SECURITY CULTURE

Awareness, daily vigilance and incident reporting.