|  |
| --- |
| **Title:** Cybersecurity Board Report Template |
| **Date:** | **Author:**  |
|  |
| **Executive summary**A concise narrative of the current cyber-risk posture of <company>, highlighting key insights, critical developments and strategic recommendations requiring board attention. This section connects cybersecurity directly to business outcomes and financial performance. |
| **Cyber-risk overview****Enterprise risk context*** How cybersecurity risks align with and impact broader enterprise risk landscape
* Current risk rating and trend analysis compared to previous quarter
* Financial impact quantification of top cyber-risks

**Risk quantification dashboard*** Cyber-risk quantification metrics with business impact assessment
* Maturity assessment against industry frameworks
* Peer comparison and industry benchmarking

**Third-party risk exposure*** Critical-vendor security posture summary
* Supply chain vulnerabilities with potential business impact
* Remediation status of high-risk third-party findings
 |
| **Threat landscape****Industry threat intelligence*** Emerging attack trends relevant to sector
* Notable attacks on peer organizations and lessons learned
* Geopolitical developments affecting cyber-risk profile

**Scenario analysis*** Summary of cyber-risk scenarios and stress tests conducted
* Business continuity implications of critical scenarios
* Recommended risk mitigation strategies
 |
| **Key risk metrics****Security posture metrics*** Phishing simulation success rates and trend analysis
* Vulnerability management effectiveness (mean time to patch)
* Security awareness program effectiveness

**Operational security metrics*** Intrusion attempts and detection effectiveness
* Insider threat alerts and investigations
* Cloud security posture status

*Note: All metrics should directly tie to business objectives and outcomes* |
| **Incident response overview****Response readiness*** Current incident response plan status
* Board escalation thresholds and notification protocols
* Tabletop exercise results and improvements

**Incident summary*** Significant security incidents since last report
* Business impact assessment and response effectiveness
* Post-incident remediation status and lessons implemented
 |
| **Regulatory updates****Oversight structure*** Board cybersecurity oversight responsibilities and structure
* Engagement frequency between security leadership and board/committees
* Documentation of board cybersecurity competency initiatives

**Regulatory updates*** Changes to cybersecurity laws and industry standards
* Compliance status and gap assessment
* Required actions to maintain regulatory compliance
 |
| **Strategic initiatives****Security program roadmap*** Progress on key cybersecurity initiatives
* Alignment with business strategy and digital transformation
* Zero-trust implementation status

**Budget and resource allocation*** Current budget utilization against plan
* ROI analysis of security investments
* Resource requirements with business case justification
 |
| **Board actions and recommendations****Required decisions*** Items requiring board approval
* Risk acceptance considerations
* Strategic security decisions needed

**Strategic recommendations*** CISO's prioritized recommendations with business rationale
* Resource requests with cost-benefit analysis
* Proposed enhancements to security governance
 |
| **Appendix*** **Detailed technical metrics**
* **Comprehensive risk assessment data**
* **Board cybersecurity training materials**
 |