



Introduction – role/dept description

INTRODUCTION

- Cybersecurity is critical in the financial sector.
- The average data breach will cost on average \$6.08M (IBM 2024).
- Goal: Strengthen framework for prevention, detection, and response.

EXTERNAL THREATS

- Phishing: Email, spear, smishing, vishing, whaling.
- Malware & Ransomware: Financial firms as top targets.
- Supply Chain: e.g., SolarWinds breach.
- DDoS: Service disruption and reputational damage.
- Credential Stuffing: Leaked credentials abused.

- Discuss the prevalence and impact of phishing (email, spear, smishing, vishing, whaling).
- Cover how ransomware and malware disproportionately target finance.
- Mention SolarWinds as an example of a supply chain compromise.
- Explain DDoS and Credential Stuffing in financial contexts.

INTERNAL THREATS

- Malicious Insiders: Data exfiltration.
- Unintentional Insider Errors: Misconfigurations.
- Shadow IT: Unauthorised software/devices.
- Privilege Misuse: Excessive access rights.

- Internal risks include both intentional and accidental actions.
- Malicious insiders often go undetected for long periods.
- Shadow IT usage—unapproved apps and hardware—introduces major risk.
- Privilege misuse arises from poor access management.

SECURITY POLICIES

- Align with ISO/IEC 27001, NIST SP 800-53, GDPR.
- Acceptable Use, Access Control, Incident Response.
- Data Classification, Email & Internet, Remote Work.

- Effective security policies underpin cyber resilience.
- FSL uses internationally recognised frameworks (ISO/NIST/GDPR).
- Briefly explain each listed policy and how it supports compliance and security.

GENERAL MITIGATION MEASURES

- Technical:
 - MFA,
 - EDR,
 - IPS,
 - Network Segmentation.
- Administrative:
 - Least Privilege,
 - Vendor Risk Mgmt,
 - Patch & Change Mgmt.

- Technical controls like MFA, EDR, and IPS reduce surface area for attacks.
- Administrative strategies include enforcing least privilege and regular patching.
- Mention NIST 800-171 for third-party vendor assessments.

PHISHING & MALWARE MITIGATION

- User training,
 - Phishing simulations.
- Technical:
 - DMARC,
 - DKIM,
 - Email filtering.

- User awareness and testing (e.g., phishing simulations) are essential.
- Technical countermeasures: DMARC, DKIM, email filtering tools.
- Training should be continuous, practical, and measurable.

MONITORING & INCIDENT RESPONSE

- Use of Microsoft Sentinel SIEM.
- Monthly reporting to CISO/CTO.
- Follows NIST SP 800-61 IR Lifecycle.

- Microsoft Sentinel is the current SIEM in place.
- Discuss how real-time alerting and centralised dashboards support incident handling.
- Mention the monthly reporting to senior stakeholders.

INCIDENT RESPONSE LIFECYCLE

- vPreparation: Policies, roles defined.
- Detection & Analysis: Logs, threat intel.
- Containment/Eradication/Recovery: Isolate, restore, verify.
- Post-Incident Review: Learn, adapt, improve.

- Introduce the NIST SP 800-61 lifecycle: Prepare, Detect/Analyse, Contain/Recover, Post-Review.

- Describe real-world value: limiting damage, restoring services quickly, and learning from incidents.

- Stress that incident logging and breach notification (72 hours under GDPR) are vital.

TRAINING AND AWARENESS

- vSecurity Induction Training.
- Phishing Simulations.
- Policy Acknowledgement.
- Role-Specific Workshops.

- Employees are the first line of defence.
- Training includes onboarding, workshops, and phishing simulations.
- Explain the importance of tracking results (e.g., click rates) to adapt content.

CONCLUSION

- FSL adopts multi-layered defence strategy.
- Compliance with ISO/NIST/GDPR.
- Focus: Prevention, Response, Awareness.

- Recap FSL's commitment to layered security.
- Emphasis on regulatory alignment and forward-looking strategies.
- Reiterate that security is a shared responsibility—technology, policy, and people all matter.