

Full name: Alaina Verity

Student number: 2407695

Module: Networks and Cyber Security Essentials

Module code: ACCA4024

Campus location: Birmingham UWTSD

- Deliverables: 2000 Report

Table of Contents

Task 1 :	2
2. Monitoring and Response:	5
3. Training and Awareness:	6
4. Deliverables:	7
5. Illustration diagram	8
6. Mitigation Measures:	9

Background:

Cyber Security has become one of the major threats globally. The increase in cybercrime has become a major concern to companies, organisations and countries in general. The rise in staff working from home and the proliferation of mobile Internet devices such as laptops, tablets, smartphones, mobile phones, to connect to the Internet for work, make payments for services, email, blogging, social interaction, shopping, entertainment, research etc. has put immense pressure on IT managers and IT policy makers in corporate environments to protect data, devices and other resources.

Scenario:

You are the IT Security Manager for FinSecure Ltd (FSL), a medium-sized financial services company. Recently, the company has experienced a series of security incidents, including phishing attacks and unauthorized access attempts on its network. As a result, the board has mandated the development of a comprehensive security policy aimed at mitigating internal and external threats.

Task 1 :

You are required to conduct relevant research using credible sources and appropriate diagrams to synthesize a solution that addresses the following aspects:

- Identification of Threats: **Clearly identify** potential internal and external threats facing FSL
- Security Policies: **Develop** a set of security policies that align with best practices in network and cyber security.

Brief Summary:

Security policies should include to influence settings such as data prevention, manipulation, and other vulnerable tactics that could arise even without common usages. Generations now have evolved, and networks/cyber security should upgrade further to minimise attackers and leakages. To overcome this, policies will be needed to encourage firm, grounded, strategic and logical methods. Understanding the methods and consequences vulnerable companies should strictly practice and train to prevent sudden confusions/sudden delays.

1. Network > Firewall management:

- All incoming traffic must be filtered through a centrally managed firewall.
- Default-deny policy should be enforced unless specifically permitted.
- Firewall rules should be reviewed quarterly or unless otherwise

2. Network > Remote Access:

- Apply VPN for all remote connections with multifactor authentication (MFA)
- Disable split tunnelling to prevent traffic leakage.
- Log and monitor all remote activity

3. Cyber Security > Password management

- Use passwords that it's less easy to remember, and if able, be more complex to secure your data.
- Change password per month to avoid unnecessary logins.
- Never share details to any individuals even if you may trust.

4. Cyber Security > Incident Reporting

- If there is something unusual about the activity you're facing e.g. popups, slow systems, lags, errors, or unauthorized access, directly report these signs right away. Reporting these inconsistencies can help and improve performance, so do not entirely ignore these faults.

5. Cyber Security > Software and Updates:

- Remain all software's, operating systems, and applications up to date
- Only install software's approved by the company

Mitigation Measures:

Propose specific measures to mitigate identified threats, detailing how each

measure will be implemented.

1. Threat 1 > Network Security Monitoring

Mitigated > External malware > C2 communication > Data exfiltration

Measures:

Intrusion detection/Prevention Systems (IDS/IPS): Detect and block malicious traffic.

Implementation: Deploy Snort, Suricata, or commercial equivalents with internet gateways.

2. Threat 2 > Patch and Configuration Management

Mitigated > Exploits (external/internal) > Ransomware propagation > Supply chain compromise

Measure:

patch rollouts

Automated Vulnerability Scanning and Patch Deployment: Weekly vulnerability scans and monthly

Implementation:

management.

Use tools like Qualys, Nessus for detection; deploy via SCCM, WSUS or third-party patch

Mitigated: External malware, Command & Control

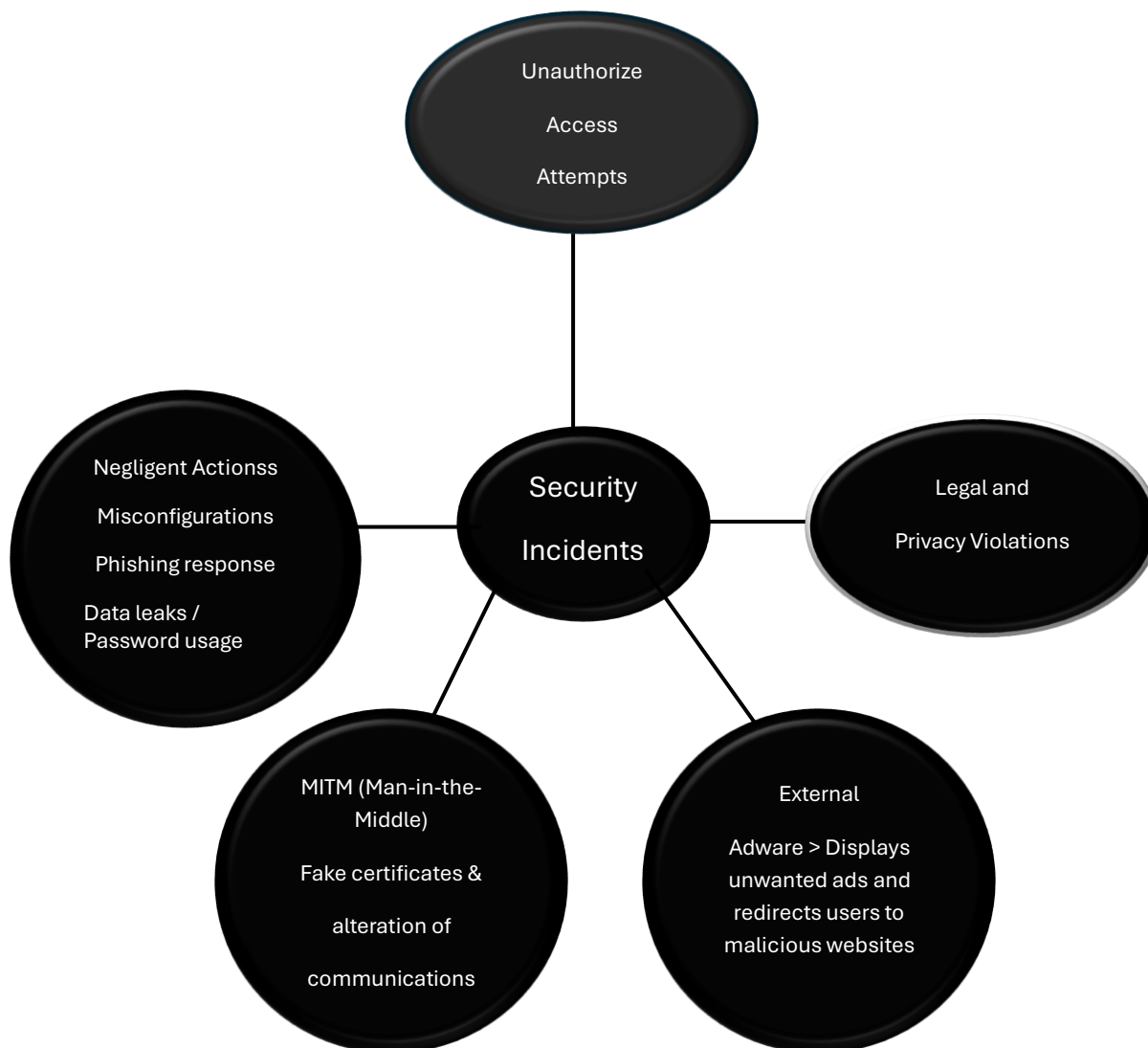
Measure: Deploy Intrusion Detection/Prevention Systems

Implementation: Use Snort or Suricata at internet gateways.

Minor traffic continuously and alert on anomalies.

2. Monitoring and Response:

Outline a plan for monitoring the network and responding to security incidents (flow chart or diagram would be useful).



3. Training and Awareness:

Describe a training program for staff to ensure compliance with the new security policies.

Brief Summary:

Training program would be needed to include firm and grounded approaches. Staffs/Employees need to be up to date to their new security policies, which also includes their tools, and potential data to avoid the prevention of loss/risk breaches.

This can ensure all Staffs/Employees engage, adhere, and actively support their organizations.

1. What should the training program include?

- Familiarize all employees with the updated security policies
- Acknowledge understanding of individual and departmental Responsibilities
- Minimize risk due to human error or negligence
- Promote a culture of security awareness and accountability.

2. Program structure:

- Overview of security policies and compliance obligations
- Password routine 2FA/MFA, and device security
- Reporting procedures for suspicious activity
- Delivery: Interactive content such as producing into free courses and online quizzes can imply efficient use and of knowledge.

4. Deliverables:

Report:

Produce a detailed report (2000 words) addressing the above aspects.

Ensure that your report is well-structured, with clear headings and subheadings. Use diagrams where appropriate to illustrate your points.

Background and Scenario:

The rise in cybercrime has made cybersecurity a critical concern for companies globally. FinSecure Ltd (FSL), a medium-sized financial institution has recently suffered wave of security incidents; including phishing attacks, unauthorized access attempts, and exposure to malware threats.

Given the high volume of remote work, the proliferation of mobile devices, and the evolving threat landscape, the board has mandated the development of a robust security framework.

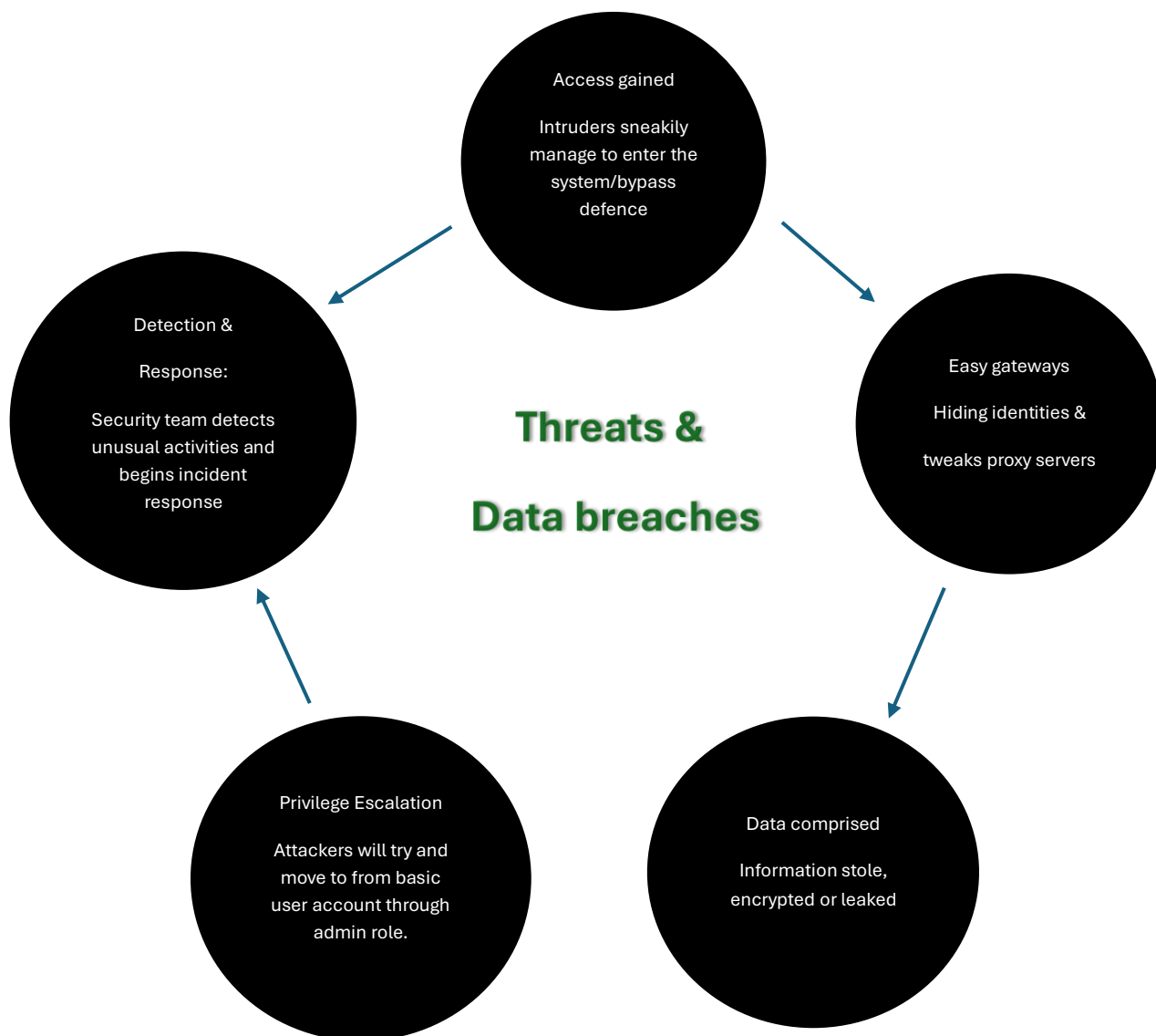
1. Internal threats:

- Malicious insiders misusing privileged access
- Negligent staff clicking phishing links or misconfiguring systems
- Unauthorized escalation and access violations
- Use of shadow IT (unsanctioned tools or apps)
- Weak password practices and policy violation

2. External threats:

- Phishing and spear-phishing campaigns
- Ransomware and malware infiltration via emails or websites
- Credential stuffing using leaked passwords
- Exploitation of unpatched systems (remote exploits)
- Supply chain compromise from third-party software

5. Illustration diagram with risk methods how they're used, highlighting danger zones and behavioural usage.



6. Mitigation Measures:

1. Network Security Monitoring:

Threats mitigated:

External malware, Command & Control (C2) communication, Data exfiltration.

Measure: Deploy Intrusion Detection/Prevention Systems (IDS/IPS)

Implementation: Use Snort or Suricata or internet gateways. Monitor traffic continuously and alert on anomalies.

2. Patch and Configuration Management:

Threats mitigated:

Exploits, ransomware propagation, supply chain compromise.

Measure: Weekly vulnerability scanning and monthly patch deployment.

Implementation: Use Qualys/Nessus for detection and SCCM for patch rollout.

3. **Security Policies:**

Policies to be implemented:

- Acceptable Use Policy (AUP).
- Password Policy (minimum complexity, MFA enforced).
- Data Classification and Handling Policy.
- Remote Work Policy.
- Incident Response and Reporting Policy.

4. Training and Awareness:

A quarterly training program is mandatory for all employees.

This includes:

- Phishing simulations.
- Secure handling of data.
- Role-specific security training.
- Policy acknowledgment and compliance confirmation.

5. Monitoring and Response:

Monitoring will be performed through EDR systems, SIEM platforms, and real-time alerts.

A formal incident response flow is in place to ensure fast containment and recovery.

Incident Response Flow:

1. Detection
2. Alert Triage
3. Containment
4. Eradication
5. Recovery
6. Lessons Learned

6. Threat Impact Examples:

Example 1:

An employee at FSL unintentionally opened a phishing email disguised as an internal IT notification. This resulted in credential compromise, giving the attacker access to internal email systems, where they launched further social engineering attempts.

Example 2:

FSL's third-party invoice processing vendor was compromised, allowing attackers to inject a malicious macro into a legitimate Excel document. When opened by finance staff, ransomware was executed, encrypting payroll data.

7. Email Security and Phishing Defence:

Threats mitigated:

Phishing attacks, Business Email Compromise (BEC), Malware delivery.

Measure:

Deploy Secure Email Gateway (SEG) with sandboxing for attachments and link re-writing.

Implementation:

Use tools such as Proofpoint or Mimecast. Enable DMARC, DKIM, and SPF to prevent spoofing

8. Endpoint Security:

Threats mitigated:

Malware infections, fileless attacks, unauthorized software use.

Measure:

Deploy Endpoint Detection and Response (EDR) with AI-based behaviour analytics.

Implementation:

Use solutions such as CrowdStrike Falcon or Microsoft Defender for Endpoint.

Configure automatic isolation and remediation workflows.

Each policy must be approved by executive management and reviewed bi-annually. Staff must digitally sign acknowledgment forms. Policy enforcement is supported by system configuration, training, and monitoring tools. Exceptions are logged and reviewed monthly by the IT governance committee.

The training plan includes:

- Monthly micro-learning modules (approximately 10-25 minutes each).
- Simulated phishing tests every quarter with results shared by department.
- Annual refresher training that includes real-world breach case studies.
- Onboarding security briefing for all new hires within the first week of employment.

Performance metrics:

Training completion rate, phishing test pass rate, reduction in user-reported incidents.

Key Monitoring Tools:

- Security Information and Event Management (SIEM): Aggregates logs from firewall, endpoint, and application systems.
- User Behaviour Analytics (UBA): Detects anomalies such as abnormal login times or data access.
- Threat Intelligence Feeds: Real-time updates on global threat indicators.