SYNTHESIZE A SOLUTION TO A REAL LIFE SCENARIO

ACCA4024

Networking and Cyber Security Essentials

Cybersecurity Strategy for FinSecure Ltd 2
1. Introduction 2
2. Identification of Threats 2
2.1 Internal Threats 2
2.2 External Threats 4
3. Security Policies 6
3.1 Acceptable Use Policy (AUP) 6
3.2 Password Policy 6
3.3 Data Protection and Classification Policy 7
3.4 Incident Response Policy 7
4. Mitigation Measures 7
5. Monitoring and Response 8
5.1 Monitoring Tools 8
5.2 Incident Response Plan (IRP) 8
6. Training and Awareness 9
6.1 Training Program Components 10
6.2 Awareness Campaigns 10
6.3 Evaluation 10
7. Conclusion 10

Cybersecurity Strategy for FinSecure Ltd

1. Introduction

For businesses everywhere, cybersecurity is a major concern, particularly in the financial services industry. This report presents a thorough cybersecurity plan in response to recent phishing attacks and unauthorised network access attempts, as reported by the IT Security Manager of FinSecure Ltd.

2. Identification of Threats

2.1 Internal Threats

Since internal threats come from people who have legal access to organisational resources, they can be just as harmful as external threats, if not more so. These threats are frequently more difficult to identify and may be purposeful or inadvertent.

Insider Threats
These occur when contractors, business partners, or current or former employees who have access to internal systems abuse their privileges. Insider threats can be motivated by money or personal grievances. For example, a disgruntled worker may sabotage systems or steal customer information before quitting the company. Because insiders frequently know where important data is kept and how to get around security measures, insider threats are especially dangerous. [1]

Examples*:*

- An employee downloads client financial data and shares it with a competitor.
- A contractor with elevated permissions deletes sensitive files upon termination.

Preventive Measures:

- Role-based access control (RBAC)
- Regular audits of user access and activity logs

- Strict offboarding procedures

Human Error

Not every internal threat is malicious. Many are the result of unintentionally acts by well-intentioned staff members. Typical mistakes include mishandling private documents, falling for phishing scams, or incorrectly configuring cloud storage (such as making S3 buckets publicly accessible).

Examples*:*

- An HR manager inadvertently sends a file containing payroll information to the wrong email address.
- An employee clicks on a phishing link and unknowingly provides their login credentials to an attacker.

Preventive Measures:

- Regular security awareness training
- Clear user guidelines and policies
- Multi-layered authentication and email filtering systems

Shadow IT

The term "shadow IT" describes the use of software, hardware, or apps that have not received IT department approval. Even though these tools are frequently well-meaning (for example, utilising a file-sharing app to boost productivity), they can introduce vulnerabilities, particularly if they are out-of-date or lack enterprise-level security. [2]

Examples*:*

- Employees using personal Dropbox accounts to share work documents.
- Staff installing unauthorized browser extensions that collect user data.

Preventive Measures:

- Enforce endpoint security and device management policies
- Regular network scans to detect unauthorized software
- Promote secure, approved alternatives for collaboration and file sharing

2.2 External Threats

External threats come from outside the organisation and are usually motivated by activism, sabotage, espionage, or financial gain. Individuals, organised crime groups, and even nation-state actors are frequently responsible for these growing threats. For FinSecure, which handles sensitive financial data, these threats pose serious risks to confidentiality, integrity, and availability.

Phishing
Phishing is the practice of deceiving people into disclosing private information, like bank account information, login credentials, or customer information. Usually, fake websites that look authentic or misleading emails or messages are used to accomplish this. [3]

Examples*:*

- An attacker sends a fake invoice to the finance department with a malicious attachment.
- A fraudulent email that appears to come from the CEO requests an urgent wire transfer.

Preventive Measures:

- Advanced email filtering and anti-phishing tools
- User training to identify suspicious emails

Malware and Ransomware
Malware is software intended to harm, interfere with, or access systems without authorisation. A type of malware known as ransomware encrypts files and requests a ransom to unlock them. These are frequently distributed through malicious links, email attachments, or compromised websites. [3]

Examples*:*

- A staff member downloads a file labeled “invoice.pdf” that installs ransomware and locks all shared network drives.
- Malware embedded in a fake job application email harvests credentials and sends them to the attacker.

Preventive Measures:

- Up-to-date antivirus and endpoint protection tools
- Network segmentation and restricted file permissions
- Regular data backups and offline storage

Brute Force

These attacks use previously leaked credentials (credential stuffing) or repeatedly try different passwords (brute force) in an effort to access systems. Targets often include financial services platforms, particularly online portals. [4]

Examples*:*

- A hacker uses automated scripts to try thousands of username-password combinations on the company's client login page.
- Previously stolen credentials from another breached service are used to access internal systems due to password reuse.

Preventive Measures:

- Multi-Factor Authentication (MFA)
- Account lockout policies after repeated failed attempts
- Continuous monitoring for unusual login behavior

Distributed Denial-of-Service (DDoS) Attacks

The goal of DDoS attacks is to overload a system or website with traffic so that users are unable to access it. These attacks can seriously impair company operations and undermine customer trust, even though they are not always data destructive. [5]

Examples*:*

- The FSL customer page becomes inaccessible during a promotional campaign due to a coordinated DDoS attack.
- Attackers demand a ransom to stop flooding the network with junk traffic.

Preventive Measures:

- Use of Web Application Firewalls (WAFs)
- Rate-limiting and traffic filtering
- DDoS mitigation services from ISPs or cloud providers

3. Security Policies

FinSecure Ltd must put in place a set of thorough, legally binding security policies in response to recent security incidents and the growing number of cyber threats. These guidelines need to serve as a foundation for directing employee conduct, controlling IT operations, and guaranteeing adherence to legal obligations.

3.1 Acceptable Use Policy (AUP)

The first step is to establish an Acceptable Use Policy (AUP) that outlines acceptable uses for company-owned digital assets, such as computers, smartphones, and internet services. Workers must refrain from installing unauthorised software, visit malicious websites, and use work resources only for business purposes. All devices must be required to use strong passwords and receive regular updates. FSL can greatly lower the risks associated with user carelessness or abuse by establishing these limits. [6]

3.2 Password Policy

FinSecure must implement a strong password policy in order to preserve strong authentication and lower the possibility of unwanted access. Every employee must create a complex password that combines capital and lowercase letters, digits, and special characters. It is not permitted to reuse passwords across accounts, and they must be changed every 60 to 90 days. Access to company systems, especially those containing sensitive financial data, will require Multi-Factor Authentication (MFA) in order to further improve security. By taking these precautions, the likelihood of brute force attacks and credential theft is greatly reduced.

3.3 Data Protection and Classification Policy

All organisational data is handled in accordance with its sensitivity and legal requirements thanks to a thorough data protection and classification policy. Information will be categorised as public, internal use only, confidential and restricted. Personal Information and client financial records are examples of confidential data that needs to be encrypted both while it is being transmitted and while it is at rest. Depending on an employee's role and need-to-know, access to this data will be limited. FSL can guarantee compliance and lower the risks of data exposure by putting this framework into practice. [7]

3.4 Incident Response Policy

FinSecure will put in place a clear and organised incident response policy in order to be ready for any security incidents that may arise. How to identify, report, contain, and recover from cyber threats is described in this policy. Every employee must notify the IT security team of any suspicious activity right away. Predetermined roles and responsibilities will be activated during an incident to guarantee a well-coordinated and effective response. Every event will be followed by a post-incident review to determine lessons learnt and enhance readiness for the future. The response plan will remain relevant and effective with regular testing and simulations. [6]

4. Mitigation Measures

To effectively safeguard FinSecure from evolving cyberthreats, each recognised threat must be combined with practical and effective mitigation techniques. They should be implemented via administrative controls, technical tools, and staff interaction. The table below lists the main risks, recommended safeguards, and specific implementation strategies.

Threat	Mitigation Measure	Implementation Strategy
Phishing	- Email filtering - Employee awareness training	Run phishing exercises and train employees on how to spot shady emails every three months. [8]
Malware	- Up to date antivirus - Segment Networks	Installing up to date anti-virus software on all computers makes viruses hardened to penetrate each system. Running a segmented network will limit access to critical systems and make it harder for attacks to move in FinSecures network. [9]

Insider Threats	- Role-Based Access Control - Activity monitoring	Make sure users only have the permissions required for their roles by implementing role based access through Active Directory. For sensitive systems, enable auditing and log monitoring to keep an eye out for odd activity. [10]
Distributed Denial of Service (DDoS)	- Web Application Firewall (WAF) - Network redundancy via cloud CDN	Deploy a cloud-based WAF (such as Cloudflare) to filter malicious traffic before it reaches internal servers. [5]

5. Monitoring and Response

FinSecure Ltd must put in place a strong monitoring system and a well-defined incident response plan to guarantee ongoing defense against both internal and external threats. To reduce damage, early detection, quick containment, and coordinated resolution are essential.

5.1 Monitoring Tools

In order to identify irregularities and indications of a compromise, monitoring entails the methodical gathering, examination, and correlation of system logs, network traffic, and user activity.

Important Tools and Techniques for Monitoring:

Security Information and Event Management, or SIEM is a centralised system for gathering and examining network, endpoint, firewall, and application logs. Splunk and Microsoft Sentinel are examples of tools that can be used. [12]

Endpoint Monitoring: All endpoints are equipped with EDR tools that monitor questionable activity, such as ransomware activity, privilege escalation, or file tampering.

Network Traffic Analysis: Intrusion Detection Systems keep an eye on all incoming and outgoing traffic for signs of data stealing or attacks.

5.2 Incident Response Plan (IRP)

Effective threat containment and cleanup are guaranteed by a documented and implemented IRP. Every incident type, including malware infections, phishing, and data breaches, need to follow an established process.

Important Components of the IRP: Prepare Contact lists, asset classification, system baselines, and staff awareness are kept up to date.

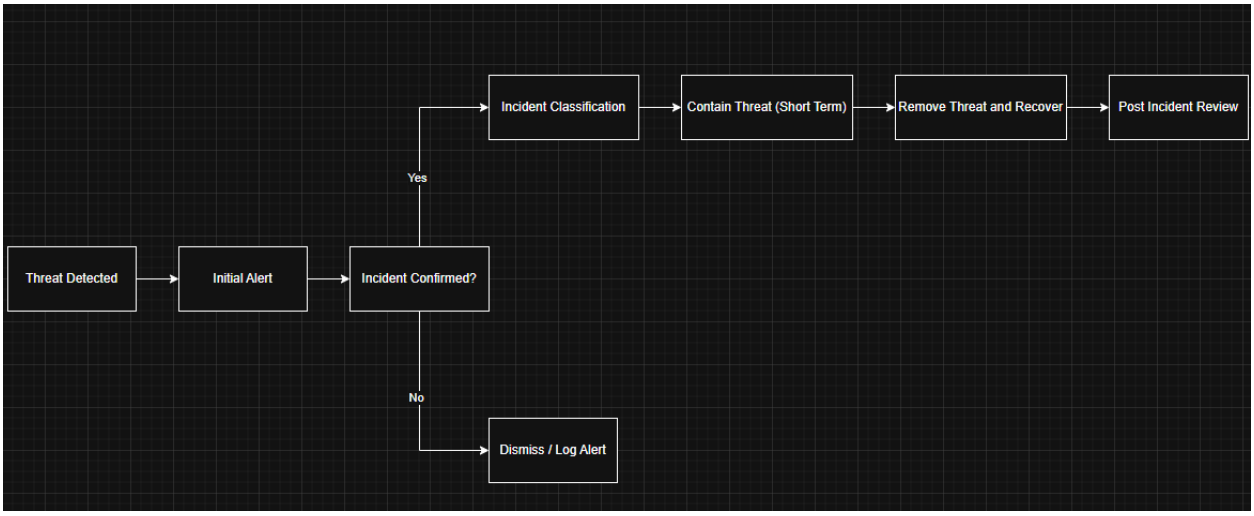
Detection & Analysis: The threat's type, extent, and severity are assessed by human review and automated alerts.

Containment includes both short-term measures (like separating accounts or systems) and long-term ones (like patching or eliminating malware).

Eradication and recovery include removing threats and bringing systems back to a clean state or backup.

Post-Incident Review: Documentation, improvements, and lessons learnt to avoid recurrence. [11]

Here is a basic flowchart outlining FSL's incident response process:



This structured approach will make sure that FSL reacts swiftly, minimises impact, and uses each incident as a learning opportunity.

6. Training and Awareness

FinSecure is aware that employees are essential to preserving cybersecurity. A strong training and awareness program is essential to reduce human error and foster a security-conscious culture.

6.1 Training Program Components

- During onboarding training, new employees are introduced to important security guidelines, secure data processing practices, and reporting protocols.
- Continuous Workshops: Using real-world examples, quarterly sessions address password hygiene, phishing awareness, and secure remote working.
- Attacks Simulated: Regular phishing simulations assist in assessing employee awareness and offer focused input for enhancement. [13]

6.2 Awareness Campaigns

- Monthly Alerts: To keep employees informed, include case studies, threat updates, and advice.
- Visual Reminders: In public spaces, security messages are reinforced by posters, screensavers, and digital signage. [14]

6.3 Evaluation

- Quizzes: Quick tests make sure that the training material is understood.
- Tracking: A learning management system tracks every training activity, giving managers the ability to keep an eye on compliance and progress. [14]

7. Conclusion

FinSecure prioritizes cybersecurity due to growing threats like insider threats, phishing, and persistent threats. The company has outlined a comprehensive security framework with strong policies, mitigation techniques, ongoing monitoring, and a proactive incident response plan. The report also highlights the importance of establishing a culture of security awareness through employee education and awareness campaigns. FinSecure hopes to lower its exposure to cyber risk by putting these recommendations into practice, strengthening its security posture, exhibiting good administration and adhering to legal requirements.

References

[1] E. Gibbons and E. Gibbons, "What are internal threats in cyber security?," *Aspire Technology Solutions*, Jul. 24, 2024. https://www.aspirets.com/blog/what-are-internal-threats-cyber-security/

[2] Talend, "What is Shadow IT? Definition, Risks, and Examples," *Talend - a Leader in Data Integration & Data Integrity*. https://www.talend.com/resources/what-is-shadow-it/

[3] "What are external threats to a business? (With examples)," Indeed, https://uk.indeed.com/career-advice/career-development/external-threats Mar. 2025.

[4] S. Yerushalmi, *What is Credential Stuffing | Attack Example & Defense Methods | Imperva*. 2023. [Online]. Available: https://www.imperva.com/learn/application-security/credential-stuffing/

[5] "What is a DDoS Attack? DDoS Meaning, Definition & Types | Fortinet," *Fortinet*. https://www.fortinet.com/uk/resources/cyberglossary/ddos-attack#:~:text=DDoS%20Attack%20means%20%22Distributed%20Denial,connected%20online%20services%20and%20sites.

[6] SentinelOne, "What is Security Policy? Types, Compliance & Strategies," *SentinelOne*, Mar. 31, 2025. https://www.sentinelone.com/cybersecurity-101/cybersecurity/what-is-security-policy/

[7] M. Sullivan, "Understanding data classification: Enhance security & efficiency," *Transcend*, Dec. 08, 2023. https://transcend.io/blog/data-classification

[8] "Phishing attacks: defending your organisation." https://www.ncsc.gov.uk/guidance/phishing

[9] T. Olaes, “9 common cyber attack methods & How to prevent them | Balbix,” *Balbix*, May 01, 2025. https://www.balbix.com/insights/attack-vectors-and-breach-methods/

[10] “Insider Threat prevention best practices,” *Netwrix*. https://www.netwrix.com/insider-threat-prevention-best-practices.html

[11] CISA, “Incident Response Plan (IRP) basics,” report, Nov. 2021. [Online]. Available: https://www.cisa.gov/sites/default/files/publications/Incident-Response-Plan-Basics_508c.pdf

[12] andrew.hamilton@cybriant.com, “The ultimate list of effective cyber security monitoring tools,” *Cybriant*, Dec. 11, 2024. https://cybriant.com/2018/10/25/cyber-security-monitoring-tools/

[13] D. Gupta, “14 Types of employee training programs (+Benefits, Examples),” *The Whatfix Blog | Drive Digital Adoption*, Mar. 18, 2025. https://whatfix.com/blog/types-employee-training-programs/

[14] CybSafe, “Raise the bar: 50 creative Cybersecurity Awareness Month ideas,” *CybSafe*, Jun. 18, 2024. https://www.cybsafe.com/blog/cybersecurity-awareness-month-ideas/