

Synthesize a Solution to a Potential Real-life Scenario

Jacob Moseley
BSc Software Engineering
University of Wales Trinity Saint David
Swansea, United Kingdom
2317034@student.uwtsd.ac.uk

Abstract - This report presents a comprehensive cybersecurity strategy for FinSecure Ltd, a financial services provider facing a range of both internal and external threats. Key vulnerabilities include threats from phishing attacks, the misuse of personal devices and malicious insiders. In response, the report proposes security policies aligned with globally recognised standards such as ISO 27001, NIST, and GDPR, which are further supported by targeted mitigation methods. A structured incident response plan and continuous monitoring system are also outlined, alongside a staff training programme to reduce human error. Together, these measures offer a layered, organisation-wide approach with the aim of improving FinSecure's cybersecurity and safeguarding in regard to sensitive financial, company and client data.

I. INTRODUCTION

In the digital age cyber security has emerged as a major concern for businesses worldwide, particularly in the financial sector where the protection of sensitive information is of utmost importance. With the growth of remote work and online connectivity, organizations are under increasing pressure to secure their networks and digital assets from increasingly sophisticated cyber-threats. FinSecure LTD (FSL), a financial services provider, has recently experienced a series of incidents, ranging from phishing attacks to unauthorized access attempts on its network, exposing threats within FSL's security policy.

This report aims to develop a comprehensive cybersecurity solution for FinSecure LTD, addressing both internal and external threats. By first identifying the key threats facing the organization, followed by the proposal of robust security policies, this report outlines a multilayered approach to safeguarding FSL's infrastructure. These policies are supported by mitigation techniques designed to reduce vulnerabilities within their network and reduce the risk of further breaches and incidents. In addition, this report shall also outline an employee training and awareness program, ensuring staff are equipped with the skills necessary to recognize, prevent, and appropriately address potential cyber threats.

II. IDENTIFICATION OF THREATS

As a financial services provider, FinSecure LTD is a prime target for a wide range of cyber security threats. These threats can be classified as both internal and external, each posing significant risks to sensitive data.

A. Internal Threats

Internal threats arise from within an organisation and may be intentional or unintentional. Examples include employees falling victim to phishing emails scams, using weak passwords or accessing sensitive data from unsecure and unauthorized devices and software. Cloud infrastructure is also a point of interest for hackers, where misconfigured permissions can be an entrance for those with the wrong intentions [1]. A more intentional example would be an employee with malicious intent using their position in an attempt to steal or damage data.

B. External Threats

External threats originate from outside of an organisation and tend to be more complex in nature. These attacks can range from forms of social engineering such as phishing campaigns and impersonation to more sophisticated attacks using software bugs, malware. The loss of and corruption of sensitive data is not the only threat faced by FSL. Cyber criminals may also aim to disrupt FSL's operations through Distributed Denial of Service (DDoS) attacks, using large botnets with the aim of overwhelming their network [2].

C. Threat Overview

To provide a clear overview of the risks faced by FinSecure LTD, threats have been grouped into three key threat domains. Each domain is vulnerable to specific internal and external threats as show in Figure 1.

Threat Domain	Internal Threats	External Threats
Individuals	- Employees falling for phishing scams - Weak passwords - Malicious insiders	- Phishing campaigns - Social Engineering tactics such as impersonation
Devices and Networks	- Use of unauthorised devices to access FSL infrastructure	- DDoS attacks on the network
Cloud Infrastructure	- Accessing sensitive cloud data via unsecure connections - Misconfigured cloud permissions	
Software	- Use of unverified software	- Exploitation of software bugs - Malware making its way into the network

[Figure 1]

These classifications shall serve as the foundation for the development of FinSecure LTD's cyber security policies, mitigation methods and staff training programs. Each domain shall be addressed in order to provide an organization wide, layered approach to cyber security.

III. SECURITY POLICIES

In regard to cyber security, a security policy generally refers to a set of guidelines and procedures designed to protect an organizations digital assets and data from cyber threats [3]. These policies form internationally recognised standards such as ISO 27001, NIST and GDPR. Implementing these policies is essential in order to mitigate both internal and external threats, as identified in the previous section.

A. Access Control Policy

Access control is a security mechanism that regulates who or what can view or use resources in a computing environment and is essential to an organisation like FSL where the security of data is paramount. This is achieved through a process of verifying users, determining appropriate access levels and restricting unauthorized access to sensitive data [4] as outlined in ISO 27001 Annex A.9.4.1. In accordance with Annex A.9.4.2, FSL should also look to implement security measures such as multi-factor authentication to add an extra layer of security in the event an employee's password is compromised. Furthermore, following Annex A.9.4.3, the use of a password management system should be adopted to ensure strong password creation and practices [5].

B. Data Protection Policy

To comply with GDPR Articles 5 and 32 as well as ISO 27001 Annex A.8, FinSecure must establish robust procedures aimed at protecting both the personal and financial data of clients and the organisation itself [6]. This means taking steps to ensure that data is encrypted while at rest and in transit, limiting access to data on a need-to-know basis and securely disposing of outdated records in line with A.8.3.2 [7].

C. Incident Response Policy

Following ISO 27001 Annex A.16 and NIST SP 800-61, this policy outlines procedures for identifying, reporting, and responding to cybersecurity incidents. Within accordance to A16.1.2, in the event of an incident, staff within the FSL must be trained to report suspected breaches immediately. A response team should be put in place in order to contain and resolve incidents effectively, with logs available for post-incident analysis with the aim of preventing incidents of a similar nature as stated within Annex A.16.1.6 [8].

D. Device Usage Policy

Based on ISO 27001 Annex A.6.2.1, this policy regulates access to FSLs network from personal devices. This policy involves applying strict restrictions on the types of software that can be installed on devices, as well as ensuring that devices can be wiped remotely in the event of a loss and making sure employees are aware that personal devices can only be used if they meet the security requirements of FinSecure LTD. Employees should also be informed of the dangers of using mobile devices in public, such as connecting to 'free' Wi-Fi that could compromise data, as well as less technical risks like uninvited observers viewing their screen [9].

These policies form FinSecure LTD's cyber security strategies and form the groundwork for the following targeted mitigation and training initiatives.

IV. MITIGATION METHODS

Mitigation measures translate FinSecure LTD's security policies into an effective defence against cybercrime. Each measure below targets a specific risk, ensuring safeguards are in place for a wide range of threats.

A. Access Control Mitigation

To combat against insider misuse and unauthorised access, FSL should look to implement **role-based access control (RBAC)** in order to restrict the network access of employees based on their role [10]. The implementation of RBAC would both improve data security and enhance compliance with data protection regulations [11]. The addition of **phishing resistant multi-factor authentication (MFA)** such as passkeys, where credentials are tied to genuine websites and cannot be used elsewhere, would also add a strong barrier against credential theft via methods such as phishing [12]. Furthermore, deploying a **password manager** ensures staff generate and store complex passwords securely, reducing brute-force and reuse risks.

B. Data Protection Mitigation

In order to protect against data theft or leakage, outdated records and storage devices should be both wiped and destroyed. By limiting access to data through **RBAC**, potential breaches can also be contained within smaller areas in the event of insider misuse or unauthorised access to the network. Data should also be encrypted through methods such as the **Advanced Encryption Standard (AES)** which can range from a 128-bit form to keys as large as 256 bits for more heavy-duty encryption purposes, perfect for an organisation such as FSL where large amounts of sensitive data are held [13].

C. Incident Response Mitigation

To respond effectively to cyber incidents, FSL should aim to implement a **Security Information and Event Management (SIEM)** system that can be used to log events within a network, such as failed logins and unfamiliar IP addresses, and use this data to detect signs of an attack, threat or breach [14]. These logs can be used in post incident reviews in order to refine procedures and avoid repeat incidents.

D. Device Mitigation

To prevent threats stemming from personal devices, FinSecure FSL should ensure that all devices that connect to their network meet strict security requirements. These requirements include ensuring employees are aware of what software can be installed on devices that connect to FSL's network. These devices must include the ability to be wiped in the event they are lost or stolen. These measures also ensure that former employees don't have access to sensitive information in the event that they leave the organization [15]. Further steps could be taken to only allow employees to access FSL's network from company devices, such as work phones that have been configured with software such as antiviruses and activity loggers.

These measures collectively ensure FinSecure LTD's policies translate into real-world protection.

V. MONITORING AND RESPONSE

Effective cybersecurity requires not only strong policies and mitigation methods, but also continuous monitoring and the ability to respond with haste in the event of an incident. In order to protect both its network and sensitive information, FinSecure LTD must implement an effective monitoring and incident response system in order to detect abnormalities, minimise damage and prevent reoccurrences.

A. Monitoring Tools and Techniques

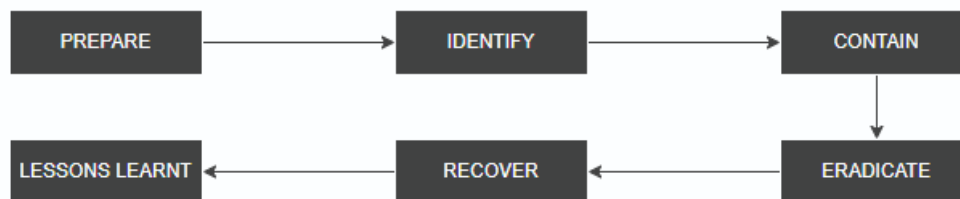
As mentioned in the previous section, FSL should deploy a **Security Information and Event Management (SIEM)** system to collect and analyse data within their network. This includes events from firewalls, servers and user activity which allow FSL to identify threats before they escalate.

B. Incident Response Plan

An incident response plan informs IT and cybersecurity professionals of the steps to take in the event of a breach or leak of sensitive information. Below are six steps that FinSecure LTD should look to implement in order to prevent, defend and learn from cyber security incidents within the organisation [16].

1. Prepare - Develop policies, assign response roles, and train staff to ensure FSL is ready to handle security incidents. Organise simulations in order to further prepare employees.
2. Identify - Detect and confirm potential security events using monitoring tools, logs, and alerts through tools such as SIEM.
3. Contain - Take immediate steps to isolate affected systems and prevent further damage. This may include taking systems offline, blocking malicious activity and creating both a long- and short-term strategy.
4. Eradicate - Remove malicious software, patch vulnerabilities, and update systems to eliminate the root cause. Perform thorough checks to ensure no threats remain.
5. Recover - Restore affected systems back to normal operation after verifying they are secure. Monitor systems closely during and after recovery to prevent recurrence.
6. Lessons Learned - Conduct a post-incident review to evaluate the response and identify areas for improvement. Use findings to strengthen future incident response procedures.

This process should be visually mapped and communicated to all relevant staff. See Figure 2 for a simplified incident response flowchart.



[Figure 2]

C. Accountability and Logging

All actions during an incident should be logged and timestamped to support investigation, reporting and compliance with ISO 27001 Annex A.16 [8]. Regular internal penetration testing should be scheduled in order to test the effectiveness of the monitoring and response plan and process.

VI. TRAINING AND AWARENESS

An effective cybersecurity strategy relies not only on technical controls, but also the awareness of threats within employees of FinSecure LTD. As highlighted throughout this report, many of the risks faced by FSL such as phishing and the misuse of devices stem from human error. In order to combat this, implementing a structured training and awareness programme is critical for ensuring compliance with security policies and reducing internal threats.

In line with ISO 27001 Annex A.7.2.2, FSL should develop a programme with the aim of educating all employees about their responsibilities in maintaining cybersecurity. This programme should be introduced during onboarding and reinforced through regular training sessions and assessments [17].

These training sessions should cover topics such as:

- Identifying phishing emails and social engineering tactics
- Secure password practices and MFA usage
- Proper handling of sensitive data
- Safe use of personal devices and software
- Incident reporting procedures

Interactive methods such as simulated phishing campaigns and online lectures can help to reinforce these principles. Managers and IT administrators should receive more in-depth training regarding areas such as incident response and system monitoring in order to reinforce these principles within their team members.

Ultimately, fostering a security-conscious culture within FinSecure is key to the long-term success of its cybersecurity measures. By equipping employees with the correct knowledge and mindset, the organisation can greatly reduce its vulnerability to both internal and external threats.

VII. CONCLUSION

In today's digital landscape, cybersecurity is essential for safeguarding sensitive data, particularly within the financial sector where the risks and consequences of breaches, data loss, and operational disruption are high. This report has explored the challenges facing FinSecure Ltd, including both internal and external threats such as phishing attacks, unauthorised device usage, and malware.

To address these challenges, a set of structured security policies were proposed, grounded in internationally recognised standards including ISO 27001, NIST, and GDPR. These policies were supported by targeted mitigation techniques to reduce technical vulnerabilities and limit exposure across FinSecure LTD's network. A comprehensive monitoring and response plan was also outlined, providing a framework for detecting incidents early and responding in an efficient manner. Finally, the importance of employee training and awareness was highlighted, recognising that even the strongest technical defences can be undermined by human error. By adopting this layer approach, FinSecure LTD can minimise the threat and impact of cyber incidents, protecting both client and company data in an increasingly hostile digital environment.

VIII. REFERENCES

- [1] E. Gibbons, "What Are Internal Threats in Cyber Security?," *Aspire Technology Solutions*, Sep. 02, 2022. <https://www.aspirets.com/blog/what-are-internal-threats-cyber-security/> (Accessed 05/05/2025)
- [2] WithSecure, "External and Internal Threats | WithSecure," *www.withsecure.com*, Apr. 24, 2023. <https://www.withsecure.com/en/expertise/blog-posts/external-and-internal-threats> (Accessed 06/05/2025)
- [3] Jennifer L. Bayuk, Jason Healey, Paul Rohmeyer, Marcus H. Sachs, Jeffrey Schmidt, Joseph Weiss, "Cyber Security Policy Guidebook," *John Wiley & Sons*, 2012. https://books.google.co.uk/books?id=E08UPzu42xoC&dq=what+are+cyber+security+policies&lr=&source=gbp_navlinks_s (Accessed 07/05/2025)
- [4] B. Lutkevich, "What is Access Control?," *TechTarget*, Jul. 2022. <https://www.techtarget.com/searchsecurity/definition/access-control> (Accessed 09/05/2025)
- [5] M. Edwards, "Annex A.9 – Access control," *ISMS.online*, Jun. 27, 2018. <https://www.isms.online/iso-27001/annex-a-9-access-control/> (Accessed 09/05/2025)
- [6] ChatGPT. (GPT-4o). OpenAI <https://chat.openai.com/chat> (Accessed 09/05/2025)
- [7] "ISO 27001 Controls: Annex A.8 Asset Management," *ISO Templates and Documents Download*, Jan. 20, 2023. <https://iso-docs.com/blogs/iso-27001-standard/iso-27001-controls-annex-a-8-asset-management> (Accessed 09/05/2025)
- [8] M. Edwards, "ISO 27001 Annex A.16 - Information Security Incident Management," *ISMS.online*, Dec. 14, 2023. <https://www.isms.online/iso-27001/annex-a-16-information-security-incident-management/> (Accessed 09/05/2025)
- [9] "ISO 27001:2022 Annex A 8.25 – Secure Development Life Cycle," *ISMS.online*, 2022. <https://www.isms.online/iso-27001/annex-a-8-25-secure-development-life-cycle-2022/> (Accessed 10/05/2025)
- [10] E. Zhang, "What Is Role-Based Access Control (RBAC)? Examples, Benefits, and More," *Digital Guardian*, Aug. 20, 2018. <https://www.digitalguardian.com/blog/what-role-based-access-control-rbac-examples-benefits-and-more> (Accessed 11/05/2025)
- [11] B. Herzberg, "4 Benefits of Role-Based Access Control (RBAC) and How to Implement It," *DATAVERSITY*, Oct. 16, 2023. <https://www.dataversity.net/4-benefits-of-role-based-access-control-rbac-and-how-to-implement-it/> (Accessed 11/05/2025)
- [12] ChatGPT. (GPT-4o). OpenAI <https://chat.openai.com/chat> (Accessed 11/05/2025)
- [13] Arcserve, "5 common encryption algorithms and the unbreakables of the future," *Arcserve*, Sep. 19, 2023. <https://www.arcserve.com/blog/5-common-encryption-algorithms-and-unbreakables-future> (Accessed 11/05/2025)
- [14] Microsoft, "What is SIEM? | Microsoft Security," *www.microsoft.com*, 2024. <https://www.microsoft.com/en-gb/security/business/security-101/what-is-siem> (Accessed 14/05/2025)
- [15] S. Blanchard, "Managing how employees use their own devices for work," *Data Protection Network*, Nov. 15, 2023. <https://dpnetwork.org.uk/tackling-byod-security-risks/> (Accessed 14/05/2025)
- [16] A. Uberoi, "What are the 6 Phases in a Cyber Incident Response Plan?," *www.cm-alliance.com*, May 06, 2021. <https://www.cm-alliance.com/cybersecurity-blog/what-are-the-6-phases-in-a-cyber-incident-response-plan> (Accessed 15/05/2025)
- [17] isms.online, "Annex A.7 Human resource security," *ISMS.online*, Jun. 27, 2018. <https://www.isms.online/iso-27001/annex-a-7-human-resource-security/> (Accessed 15/05/2025)

Appendix: Summary Presentation

Potential Cybersecurity Solution for FinSecure LTD

Jacob Moseley

IT Security Manager, FinSecure LTD

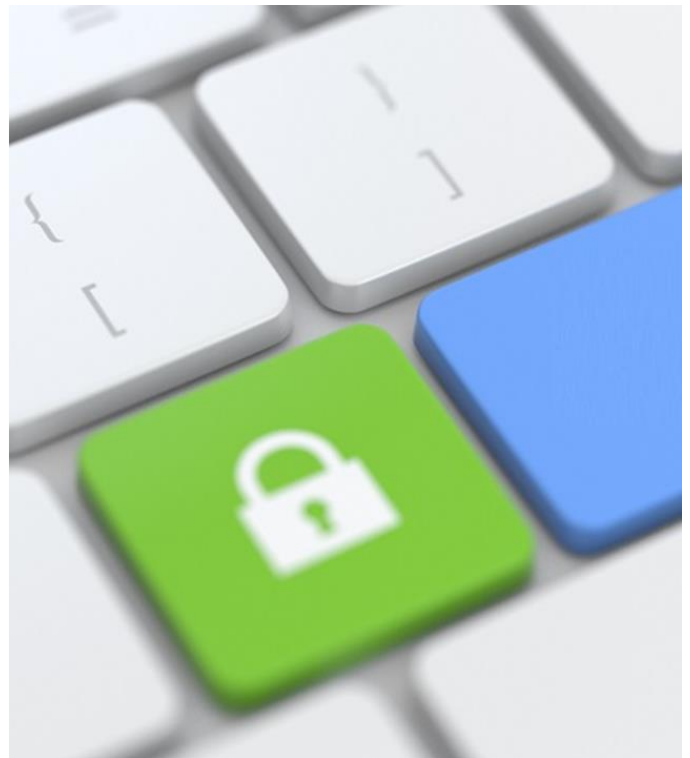
May 2025

[Figure 1]

Introduction

FinSecure Ltd has recently faced a series of cyber incidents, including phishing attacks and unauthorized access attempts. In response, as IT Security Manager I have been tasked with developing a cybersecurity strategy to combat these attacks. This presentation outlines the key threats we face and proposes the policies, mitigation measures and staff training needed to protect our systems and data.

[Figure 2]



Threats

It is important that FSL identifies the key threats facing our organization. These threats can be grouped into both internal and external threats.

Internal Threats

Internal threats can be described as threats that arise from within our organization. These can be both intentional, stemming from bad actors, and unintentional, stemming from issues such as poor employee training.

External Threats

External threats are threats that arise from outside of our organization and tend to be more sophisticated in nature.



[Figure 3]

Key Threats

Internal Threats

- Malicious insiders abusing their position
- Use of unauthorised software
- Weak credentials
- Use of unauthorised devices on FSL's network

External Threats

- Distributed Denial of Service (DDoS) attacks
- Phishing campaigns and Social Engineering
- Malware
- The exploitation of software bugs



[Figure 4]

Policies

To address identified threats, it is important to implement security policies aligned with industry standards such as ISO 27001, NIST and GDPR.

These policies are focused on controlling access, protecting data, responding to incidents, and managing device usage.



[Figure 5]

Policies

Access Control Policy

- Aligned with ISO 27001 Annex A.9
- Use of multi-factor authentication (MFA)
- Determine appropriate access levels for sensitive data
- Use of a password management system

Incident Response Policy

- Aligned with Annex A.8 and NIST SP 800-61
- Staff must be trained on how to respond to incidents
- A response team must be ready to respond to incidents
- Logs must be maintained for post incident analysis

Data Protection Policy

- Aligned with Annex A.8 and GDPR Article 5 and 32
- The Proper disposal of data
- The encryption of data at rest and in transit
- Limiting access of data on a need-to-know basis

Device Usage Policy

- Aligned with ISO 27001 Annex A.6
- Implementing strict restrictions on software
- Ensuring devices can be wiped remotely
- Ensuring employees are aware of the dangers that personal devices present to FSL

[Figure 6]

Mitigation

Mitigation measures translate FinSecure LTD's security policies into effective defences against cybercrime.

Each measure targets a specific risk, ensuring safeguards are in place for a wide range of threats.



[Figure 7]

Mitigation Methods

Access Control Mitigation

- Implement role-based access control (RBAC)
- Use phishing-resistant multi-factor authentication
- Use password managers for secure credential storage and creation

Incident Response Mitigation

- Use a SIEM system to monitor and log network events
- Store logs for post-incident analysis
- Refine procedures to prevent repeat incidents

Data Protection Mitigation

- Wipe and destroy outdated records and storage devices
- Restrict data access using RBAC
- Encrypt sensitive data using AES standards

Device Usage Mitigation

- Enforce security standards on all connected devices
- Allow only approved software on devices
- Enable remote wipe capability for lost/stolen devices
- Issue company devices that can be used instead of personal devices

[Figure 8]

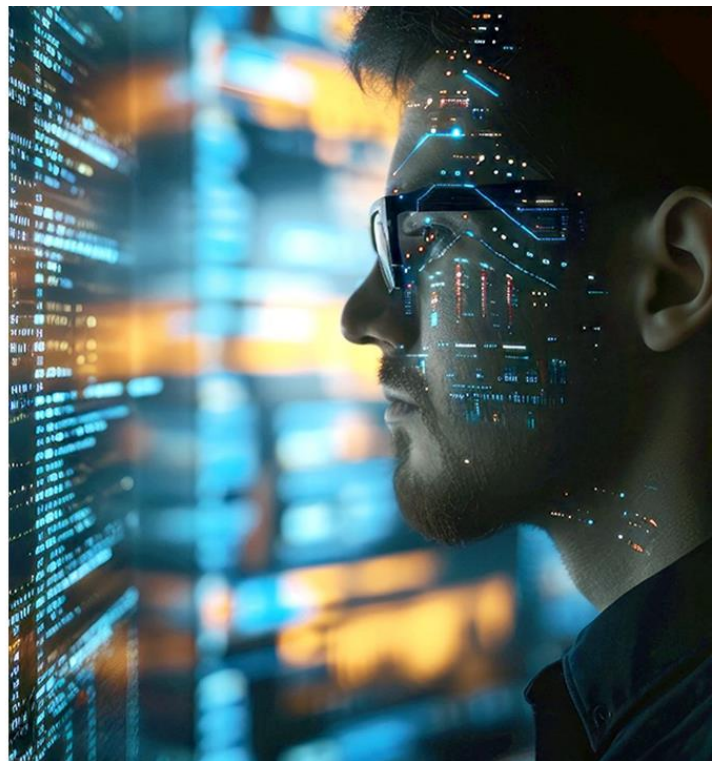
Monitoring and Response

In order to protect both systems and data, FinSecure LTD's network requires continuous monitoring.

This includes a clear response plan to detect threats early, minimize damage, and prevent future incidents.

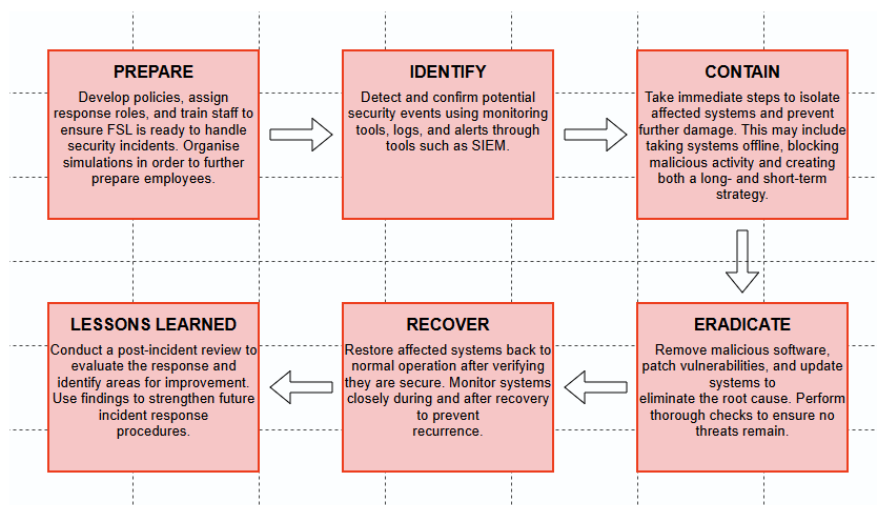
This response plan includes six steps, prepare, identify, contain, eradicate recover and lessons learnt.

This plan should be distributed to staff in order to raise awareness within FSL.



[Figure 9]

Monitoring and Response Plan



[Figure 10]

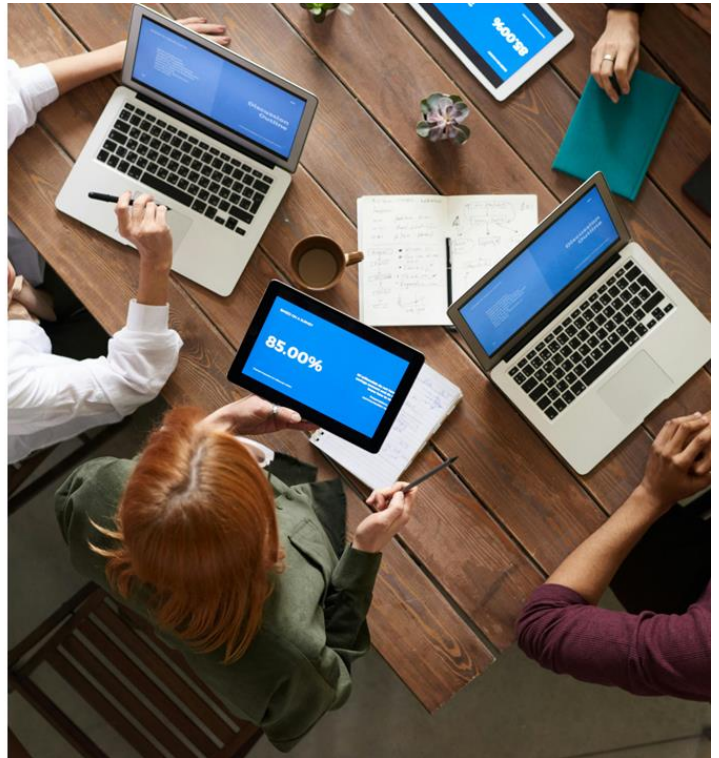
TRAINING AND AWARENESS

Training and awareness ensures involves educating staff in order to reduce human error and ensure compliance with security policies.

Key topics would include; Phishing recognition, secure passwords, device safety and incident reporting.

Staff would take part in onboarding sessions, regular training and simulated threats.

This would foster a security conscious culture within FSL and is key to the long term success of its cyber security measures.



[Figure 11]

CONCLUSION

With growing threats facing FinSecure LTD's infrastructure, it is imperative that a layered approach to cybersecurity, including new policies, mitigation measures, monitoring and staff training are implemented.

Together, these measures shall help to protect FSL's systems and sensitive data, reduce the risk of future breaches, ensure compliance with regulatory standards, and maintain the trust of clients and in an increasingly hostile digital age.



[Figure 12]



[Figure 13]



Thank you

Jacob Moseley

2317034@student.uwtsd.ac.uk