



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

SYNTHESISE A SOLUTION TO A POTENTIAL REAL LIFE SCENARIO

Networks and Cyber Security Essentials – ACCA4024
Lucy Boyt - 2308345

Contents

- I. INTRODUCTION 0
- II. IDENTIFICATION OF THREATS 0
- III. SECURITY POLICIES 1
 - A. ENTERPRISE INFORMATION SECURITY POLICIES 1
 - B. ISSUE-SPECIFIC SECURITY POLICIES 1
 - C. SYSTEM-SPECIFIC SECURITY POLICIES 2
- IV. MITIGATION MEASURES..... 2
 - A. PREVENTIVE MEASURES 2
 - B. DETECTIVE MEASURES 3
 - C. CONTINUOUS TESTING AND RESPONSE 3
- V. MONITORING AND INCIDENT RESPONSE 3
 - A. CONTINUOUS MONITORING PLAN 3
 - B. INCIDENT RESPONSE PLAN 4
- VI. TRAINING AND AWARENESS PROGRAM 4
 - A. TRAINING FOR ALL STAFF: 5
 - B. TRAINING FOR IT/SECURITY TEAMS: 5
 - C. TRAINING FOR EXECUTIVES AND RISK TEAMS. 5
- VII. CONCLUSION 5
- VIII. REFERENCES 5
- IX. APPENDIX 10

Synthesise a solution to a potential real-life scenario

Lucy Boyt

Student of University of Wales Trinity St David, Swansea, Wales.

2308345@student.uwtsd.ac.uk

Abstract – FinSecure Ltd, a UK financial services firm, has seen an increase in cybersecurity threats from internal and external sources, including phishing, ransomware, insider misuse and cloud or Internet of Things vulnerabilities. FinSecure undertakes implementations of layered security policies focusing on access control, network segmentation, data protection and incident response to address these risks. These implementations align with UK regulations such as GDPR and the NIS regulations. Mitigation measures include AI-powered threat detection, MFA, SIEM, endpoint protection and automated patching. The execution of regular penetration testing and phishing simulations to help identify weaknesses and a strong emphasis on Employee awareness due to human error being the leading cause of security breaches. Staff will undergo Annual training aligned with the FCA and NCSC Guidance, assuring operational resilience, compliance with regulations and customer trust. With continuous monitoring, policy updates, and proactive threat intelligence integration, FinSecure's abilities to adapt to the developing Cyber Threat landscape will be enhanced.

Keywords— *Information Security, Threats, Phishing, Ransomware, Security Policy, Incident Response, Compliance, Governance.*

I. INTRODUCTION

In today's digital financial sector, cybersecurity is essential for protecting sensitive data, preserving customer trust and meeting regulatory standards. Financial companies are highly targeted by cybercriminals due to the substantial value of their data and assets. Innovations such as cloud computing, AI and open banking introduce complex vulnerabilities ready for exploitation.

FinSecure Ltd is a mid-sized UK financial company which has recently fallen victim to various security incidents, including phishing and unauthorised network access attempts. These events have highlighted vulnerabilities within the company's existing infrastructure and underscored the urgency for a comprehensive security strategy.

This report aims to:

- Examine the existing cybersecurity landscape relevant to FinSecure Ltd and the broader UK financial services industry.

- Identifying weaknesses within the company,
- Reviewing policies and procedures,
- Utilise cybersecurity benchmarks such as the NIST Cybersecurity Framework and maturity models to evaluate preparedness.
- Recommend enhancements which will counteract risks, improve resilience and conform to UK legislation and standards.
- Encompass a security-conscious ethos with efficient training, awareness and governance.

II. IDENTIFICATION OF THREATS

The financial services industry currently faces several critical cybersecurity threats, both internally and externally. Internal threats predominantly originate from current and former employees and trusted business partners with privileged system access. Such access creates vulnerabilities that can lead to data breaches, sabotage, fraud, intellectual property theft, and corporate espionage. These internal threats can be particularly challenging to detect since the individuals involved hold legitimate access privileges, making their activity less conspicuous than external threats. [1]

Employee errors, including susceptibility to phishing attacks, unintended sharing of sensitive information and system misconfigurations, significantly heighten risks. An IBM security study found that human error was a contributing factor in 95% of cybersecurity breaches, highlighting the critical role of human behaviour within organisational security. [2]

External threats encompass phishing, social engineering attacks, malware and Advanced Persistent Threats (APT). Phishing and social engineering attacks often rely on deceitful strategies to influence employees and consumers into disclosing confidential information. Often seen within the workscape via impersonation or malicious emails, fraudulent websites which can circumvent conventional safeguards, posing a significant challenge to our defensive effectors.

Malware, such as forms of ransomware and extortion-driven attacks, has significant implications for the industry's digital landscape. The Financial Conduct Authority's (FCA) data from 2023 highlighted this trend, with Ransomware making up 31% of all reported cyber incidents, revealing a significant increase in such attacks. [1] [3]

APT represents another severe external risk which involves sustained, targeted cyberattacks aimed at infiltrating and maintaining long-term, undetected access to a network. This threat is used primarily for espionage, data theft and sabotage. As a result of the complexity and persistence, APTs necessitate advanced detection mechanisms and uninterrupted network monitoring, especially given that they target high-value financial data. [3] [4]

Cloud-based threats are on the rise within the financial industry as institutions adopt cloud services. These challenges involve data breaches originating from inadequate access controls, misconfiguration of the cloud environments and vulnerabilities in the service providers' infrastructures. This necessitates the requirement for stringent cloud security management.

Internet of Things (IoT) threats have emerged due to the integration of IoT devices within financial service environments. IoT vulnerabilities can lead to unauthorised access, data interception, or disruption of critical business operations, emphasising the importance of comprehensive IoT security frameworks. To ensure these threats are addressed, a holistic cybersecurity strategy is required which includes staff training, stringent access controls, advanced threat detection technologies, ongoing monitoring and regular risk evaluations. [5]

III. SECURITY POLICIES

Policies represent a set of guiding principles that inform decision-making across an organisation. They define behavioural expectations for senior management and employees in day-to-day operations. Human fallibility contributes to more than ninety percent of cybersecurity breaches. It is essential that FinSecure establish a comprehensive policy framework to minimise risks. This approach not only safeguards clients' data but also aligns the business with legal and regulatory requirements. [5]

According to the National Institute of Standards and Technology (NIST) Special Publication 800-53, security policies can be grouped into three categories: (A) Enterprise Information Security Policies, (B) Issue-Specific Policies, and (C) System-Specific Policies. [1]

A. Enterprise Information Security Policies

These policies articulate FinSecure's strategic direction for information security. They apply organisation-wide and establish the tone for a risk-aware culture. [6]

a) Access Control Policy

This policy enforces the principle of least privilege to restrict access to authorised personnel only. It applies to all staff, contractors, and third-party entities. [7]

- Access to systems will be governed by a Role-Based Access Control (RBAC) model.
- Access privileges will be reviewed quarterly.
- Multi-factor authentication (MFA) is mandatory for all systems and remote access.
- Privileged access will be logged and authorised by the IT Security team.
- Departing employees and contractors will have access revoked within 24 hours.

b) Network Security Policy

This policy aims to protect FinSecure's network infrastructure through layered security mechanisms.

- Firewalls and Intrusion Prevention Systems (IPS) will be deployed across all internal and external network segments.
- Security Information and Event Management (SIEM) tools will monitor logs in real-time.
- Sensitive systems (e.g. Finance, HR) will be isolated via network segmentation.
- Penetration testing and vulnerability assessments will be conducted bi-annually.

B. Issue-Specific Security Policies

Though not universally applicable across all systems, these policies address specific risk domains critical to compliance or operations.

a) Data Protection Policy

The Data Protection Policy ensures personal and financial data's confidentiality, integrity, and availability.

Applies to all personal and sensitive data processed by FinSecure.

- All data must be encrypted at rest and in transit using industry standards (e.g., AES-256).
- Access to sensitive data must be logged and limited to job necessity.
- Regular Data Protection Impact Assessments (DPIAs) will be conducted.

- In the event of a breach, the Information Commissioner's Office (ICO) must be notified within 72 hours.[8]

b) *Acceptable Use Policy (AUP)*

The AUP outlines acceptable behaviours regarding IT systems and data usage. Applies to all employees, contractors, and third parties.

- Prohibits use of company systems for illegal activity, personal financial gain, or offensive content.
- Devices must be locked when unattended and never shared.
- Remote access is permitted only via company-managed VPNs.
- All users must complete AUP training at onboarding and annually thereafter.
- Mobile devices must adhere to Mobile Device Management (MDM) protocols.

C. *System-Specific Security Policies*

System-specific policies define technical controls for specific systems, platforms, or configurations.

a) *Incident Response Policy*

This policy provides structured procedures for identifying, responding to, and recovering from security incidents. Applies to all systems, data, users, and third-party services.

- All suspected incidents must be reported to the IT Security team within one hour.
- The response team will categorise, contain, eradicate, and recover from incidents in line with defined playbooks.
- Digital forensics must be conducted on all critical or legally sensitive incidents.
- Lessons learned will be documented and reviewed monthly to refine response plans.

All policies are subject to review annually or following significant changes or incidents. Compliance will be audited quarterly. Consistent with internal governance and regulatory obligations, non-compliance may lead to disciplinary or legal action.

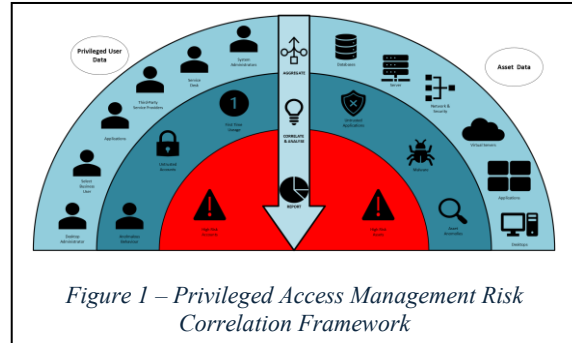
IV. MITIGATION MEASURES

FinSecure Ltd. must adopt a blend of proactive and reactive measures to ensure the confidentiality, integrity, and availability of personal and financial data. Their implementation relies on layered technical and procedural controls. [9][10]

A. *Preventive Measures*

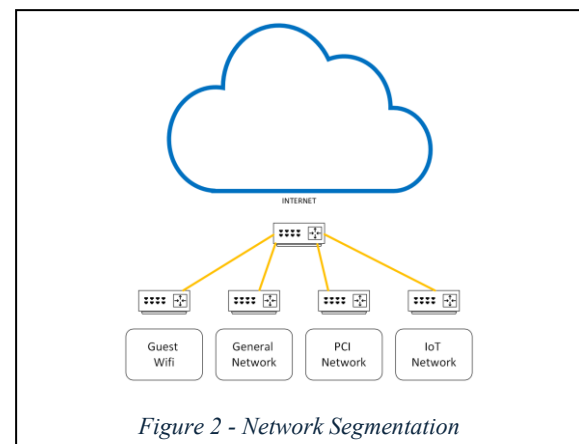
Preventative strategies can minimise exposure to internal and external threats:

Privileged Access Management (PAM) can be deployed to manage administrator accounts. Any privileged sessions can be logged and monitored with just-in-time access provisioned via approval workflows. A review quarterly of elevated accounts would also be enforced.



Multi-factor authentication (MFA) will be enforced organisation-wide using an authenticator app or hardware token. It will be integrated with cloud platforms, remote VPN access, internal admin portals, and the email system.

Internal Networks will be segmented by Function (Finance, HR, Data) using VLANs and Firewalls. Access between segments will require rule-based policies, minimising lateral movement. Sensitive systems will be isolated on dedicated subnets.



All user devices will be installed with a next-generation endpoint protection platform such as SentinelOne. Control will be managed using Mobile Device Management (MDM) to restrict USB access and enforce encryption.

AI-Power Email Security will be implemented using an Email gateway (Microsoft Defender), which will be configured to use machine learning to detect phishing, spoofing and malicious attachments. Emails flagged will be quarantined for review by the security team. [3]

Automated patching will be managed using Microsoft Endpoint Configuration Manager (or something similar). Critical vulnerabilities will be patched within 48 hours of identification and monthly patch status reports will be reviewed by IT Leadership.

B. Detective Measures

A Security Information and Event Management (SIEM) platform like Microsoft Sentinel will ingest logs from firewalls, endpoints, and cloud environments. It will then monitor rules and alerts to detect suspicious behaviour and trigger automated response workflows. [11]

The use of User and Entity Behaviour Analytics (UEBA) within the SIEM will be enabled to track baselines of user behaviour and to identify deviations such as large data transfers and irregular log in times.

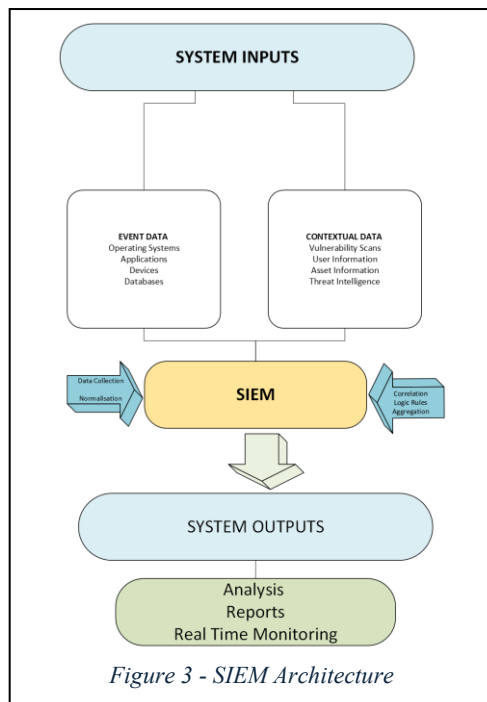


Figure 3 - SIEM Architecture

Intrusion Detection and Prevention Systems (IDS/IPS) can be implemented at network security points using cloud native tools like Azure Network Watcher. They can detect threats, which will be logged and automatically blocked or quarantined based on severity.

File integrity Monitoring (FIM) monitors changes to critical configuration files and sensitive directories. Any Alerts can be sent to the SIEM for review and validation.

Decoy servers and data traps could be deployed to attract threat actors. These systems should be monitored to detect any reconnaissance or lateral

movement activity. Certified professionals should conduct internal and External penetration tests bi-annually. Simulated phishing campaigns should also be conducted quarterly to test employees' awareness and response.

C. Continuous Testing and Response

The implantation of digital forensics and post-incident review following any major incidents can be performed using tools such as EnCase. Following which root cause analysis and lessons learned should be formally documented and utilised to improve response plans. [9]

FinSecure will subscribe to commercial threat intelligence feeds and integrate them with the SIEM to correlate indicators of compromise (IOCs) with internal events. Any Relevant data will be used to adjust detection rules in a proactive manner.

Every organisation is a potential victim of cyber-attacks. Unfortunately, it is often difficult to accurately assess the specific threats an organisation will face. However, there are practical and affordable ways to reduce exposure to the most common types of attacks. FinSecure Ltd can strengthen its security posture and resilience against current and emerging threats by implementing layered technical controls, supported by continuous monitoring and intelligence-led detection.

V. MONITORING AND INCIDENT RESPONSE

UK regulatory bodies such as the FCA and NCSC, as well as compliance mandates such as the NIS Regulations, emphasise the importance of proactive detection and rapid mitigation strategies.

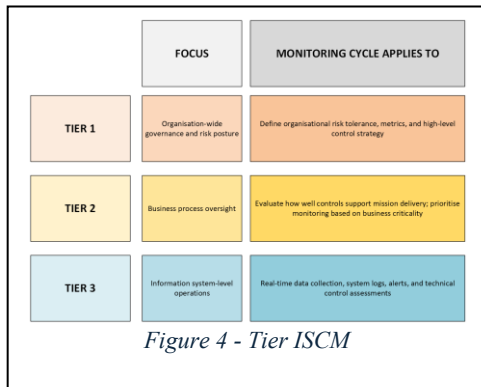
Continuous Monitoring Plans aim to ensure real-time visibility, threat detection, and anomaly analysis across the businesses' network environments.

An Incident Response (IR) Plan details the stages of identification, containment, eradication and recovery to effectively manage and mitigate security incidents.

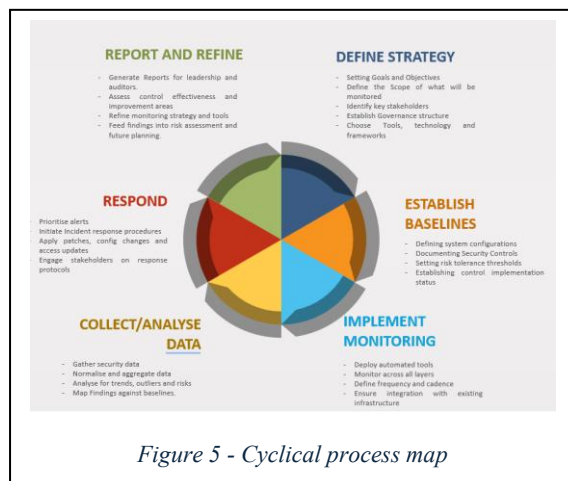
Together, these strategies will form a proactive and resilient framework for defending critical financial systems and data in accordance with industry best practices.

A. Continuous Monitoring Plan

A combination of the tier-based model and the cyclical Information Security Continuous Monitoring (ISCM) process is considered best practice as it provides strategic alignment via the tier model and operational efficiency via the cyclical model.



The cyclical process is to be applied with different focus, scope, and granularity at each tier of the organisation.



B. Incident Response Plan

The Incident Response plan outlines any actions required in the event of an incident. The Pipkin Method outlines 8 phases, which are ideal for the company.

a) Preperation

In this stage Policies, teams, tools and training needs must be established to manage incidents. In FinSecure this would be defining the IR policy which will be aligned with the FCA and NCSC guidelines. The creation of IR Team Roles and the deployment of SIEM.

b) Identification

This is the stage where an incident has been detected and confirmed. This will be completed by the use of logs and alerts. The severity will be classified, and data will be correlated across the systems.

c) Containment

The aim of this stage is to limit the scope and spread of the incident by isolating infected endpoints,

utilising network firewall rules and suspending any compromised accounts.

d) Eradication

This is the stage where the root cause and any artefacts are removed. Such as the deletion of malware, the registry is cleaned and any backdoors are removed.

e) Recovery

The restoration of any affected systems from backups, systems are rebuilt.

f) Lessons Learned

The incident is reviewed and the IR plan performance is assessed. This can be completed with a workshop to discuss lessons learned. The IR playbooks would be updated and any reports are filed with the FCA and ICO if required.

g) Damage Assessment

The review of what was compromised or lost by assessing what data was stolen or leaked. The identification of any financial impact and analysis of the downtime and reputational risk.

h) Evidence Collection

The stage of gathering and preserving forensic artefacts such as capturing disk images, logging network traffic and ensuring change of custody for any legal use.

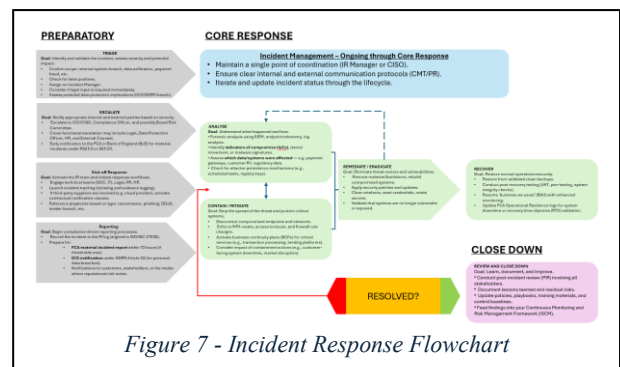


Figure 7 demonstrates the NCSC key ingredients for a basic response plan with added context for FinSecure's business.

VI. TRAINING AND AWARENESS PROGRAM

To ensure the effective roll-out of the proposed strategies, it is essential that comprehensive education is provided to all employees, irrespective of their role or position within the company. The training will empower each participant with the skills needed to identify and actively respond to potential cyber risks. In doing so, FinSecure will cultivate an environment where every member of staff contributes to strengthen the cybersecurity resilience and create a collective mindset of vigilance and readiness.

A. Training for all staff:

A SETA initiative run on a quarterly basis and during each colleague's induction. The initiative is designed to provide all members of the team with a firm understanding of cybersecurity risks, obligations to regulatory bodies, and their distinctive duties within the company.

Phishing simulations will be rolled out every month with the intention of reinforcing awareness and allow the company to assess any vulnerability from the results.

Best practices will be promoted daily with key emphasis on critical areas such as password etiquette, the use of MFA, mobile device safeguarding, and secure remote access.

The training content for all members of staff will include:

- Recognising various forms of phishing methodologies
- Protocols for reporting suspicious activity
- Cultivating security practices in all work environments (from home, the office and on the go).
- Understanding data classification and management, adhering to the FCA and GDPR standards.
- Insider threat behaviour mitigation strategies.

B. Training for IT/Security Teams:

The IT and Security team are the bulwark defending the company from cyber threats. These members of staff will be provided with specialised training sessions on a quarterly basis, complemented by any additional training required following developments within the cyber world.

Workshops will be scheduled in the following areas:

- Optimal SIEM utilisation and tuning
- Advanced endpoint protection and response mechanisms
- Cloud security architecture and management
- Comprehensive log analysis and threat hunting
- Compliance with regulatory logging and reporting requirements (PS21/3, NIS).

C. Training for Executives and Risk teams.

FinSecure will host annual table top exercises inspired by NCSC's Exercise in a box, with the aim of enhancing the readiness of senior leaders and risk managers in the face of potential data breaches, DDoS incidents, and insider threats.

Additional training topics will include:

- The significant impact of cyber incidents on business continuity
- FCA notification obligations in the event of a security breach
- Strategic communication and coordination with media and stakeholders
- Legal and reputational ramifications of such occurrences.

The aim of this educational plan is to foster a workforce that is knowledgeable and vigilant, which will in turn strengthen the company's defences and prepare it for a range of cyber-related contingencies.

VII. CONCLUSION

In Conclusion, the implementation of a comprehensive cybersecurity strategy is of paramount importance for FinSecure Ltd as it navigates an increasingly complex threat landscape within the financial domain. The outlined policies provide a systematic framework that encompasses vital areas such as access control, incident response, data fortification and acceptable use of systems.

This methodology establishes clear organisation-wide guidelines which ensure a uniform and consistent approach to cybersecurity.

However, reliance upon policies cannot ensure absolute protection. Given the ever-evolving nature of technology, the business strategies must be agile and forward-thinking.

Continuous improvement is vital and can be achieved through regular policy review, the deployment of advanced threat detection tools and ongoing training to keep staff alert and informed. The integration of new technologies and fostering a strong culture of cybersecurity awareness across all levels of the organisation will enhance defence capabilities. By maintaining a proactive and adaptive approach, FinSecure can safeguard its data, ensuring operational continuity and upholding its regulatory and reputational responsibilities.

VIII. REFERENCES

- [1] F. Whitelaw, J. Riley and N. Elmrabit. F. Whitelaw, J. Riley and N. Elmrabit. A review of the insider threat, a practitioner perspective within the U.K. financial services. A review of the insider threat, a practitioner perspective within the U.K. financial services. *IEEE Access* *IEEE Access* 1212pp. 34752–34768. pp. 34752–34768. 2024. . DOI: 10.1109/ACCESS.2024.3373265.
- [2] Anonymous . *IBM Report: Half of Breached Organizations Unwilling to Increase Security*

- Spend Despite Soaring Breach Costs*. Available: <https://newsroom.ibm.com/2023-07-24-IBM-Report-Half-of-Breached-Organizations-Unwilling-to-Increase-Security-Spend-Despite-Soaring-Breach-Costs>.
- [3] A. Deshpande. A. Deshpande. Cybersecurity in financial services: Addressing AI-related threats and vulnerabilities. Cybersecurity in financial services: Addressing AI-related threats and vulnerabilities. April 1, 2024, Available: https://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=10616498. DOI: 10.1109/ICKECS61492.2024.10616498.
- [4] A. Siam, M. Alazab, A. Awajan and N. Faruqi. A. Siam, M. Alazab, A. Awajan and N. Faruqi. A comprehensive review of AI's current impact and future prospects in cybersecurity. A comprehensive review of AI's current impact and future prospects in cybersecurity. 2025 Available: https://www.researchgate.net/publication/387915732_A_Comprehensive_Review_of_AI's_Current_Impact_and_Future_Prospects_in_Cybersecurity. DOI: 10.1109/ACCESS.2025.3528114.
- [5] A. A. Darem, A. A. Alhashmi, T. M. Alkhaldi, A. M. Alashjaee, S. M. Alanazi and S. A. Ebad. A. A. Darem, A. A. Alhashmi, T. M. Alkhaldi, A. M. Alashjaee, S. M. Alanazi and S. A. Ebad. Cyber threats classifications and countermeasures in banking and financial sector. Cyber threats classifications and countermeasures in banking and financial sector. *IEEE Access* 11(1) pp. 125138–125158. pp. 125138–125158. 2023. Available: https://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=10292652. DOI: 10.1109/ACCESS.2023.3327016.
- [6] Anonymous Anonymous NIST special publication 800-53 revision 5. NIST special publication 800-53 revision 5. 2020. Available: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf>.
- [7] W. Stallings. W. Stallings. *Cryptography and Network Security : Principles and Practice* *Cryptography and Network Security : Principles and Practice* 2016.
- [8] Anonymous Anonymous GDPR - regulation 2016/679. GDPR - regulation 2016/679. *Article 33* Article 33 2016. Available: <https://www.legislation.gov.uk/eur/2016/679/article/33/2020-12-31>.
- [9] K. Nwafor, A. Ikudabo, C. Onyeje and D. Ihenacho. K. Nwafor, A. Ikudabo, C. Onyeje and D. Ihenacho. Mitigating cybersecurity risks in financial institutions: The role of AI and data analytics. Mitigating cybersecurity risks in financial institutions: The role of AI and data analytics. *International Journal of Science and Research Archive International Journal of Science and Research Archive* 13(3) 2024. Available: https://www.researchgate.net/publication/385217807_Mitigating_cybersecurity_risks_in_financial_institutions_The_role_of_AI_and_data_analytics. DOI: 10.30574/ijrsra.2024.13.1.2014.
- [10] P. Klumpes. P. Klumpes. Coordination of cybersecurity risk management in the U.K. insurance sector. Coordination of cybersecurity risk management in the U.K. insurance sector. *Geneva Pap Risk Insur Issues Pract Geneva Pap Risk Insur Issues Pract* 48(48(2)), pp. 332–371. pp. 332–371. 2023. Available: <https://doi.org/10.1057/s41288-023-00287-9>. DOI: 10.1057/s41288-023-00287-9.
- [11] M. Cinque, D. Cotroneo and A. Pecchia. M. Cinque, D. Cotroneo and A. Pecchia. Challenges and directions in security information and event management (SIEM). Challenges and directions in security information and event management (SIEM). October 1, 2018, Available: https://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=8539170. DOI: 10.1109/ISSREW.2018.00-24.

Presentation Slides and Notes



Welcome, everyone, and thank you for taking the time to watch this presentation.
My Name is Lucy, I am the IT Security Manager at FinSecure for x duration.
My Expertise are
We are here today to discuss (Click to next slide)



The purpose of today's session is to present a detailed and strategic plan to enhance FinSecure Ltd's cybersecurity posture.
This plan responds directly to the increasing complexity of threats and the changing regulatory landscape in the UK financial sector.
These recommendations are grounded in leading frameworks like NIST and are adapted to FinSecure's unique risk profile and organisational context.
The proposal is designed to ensure that we not only comply with legal obligations but also position the firm as a proactive leader in the cybersecurity space.

5 Emerging Threats

Shaping the
Cybersecurity
Landscape in
Financial Services

1

INSIDER THREATS ARE ESCALATING

Privileged Users like IT staff, contractors and former employees are now seen as one of the most dangerous risk. With motivators such as financial gain, personal grievances and coercion – Insider fraud accounts for 31% of reported financial crimes.

To provide a sharper view of today's cyber threat landscape, let's walk through five key areas that demand immediate strategic focus. These aren't theoretical risks—they're backed by evidence from PwC, IEEE, and frontline research in UK financial institutions.

Insiders remain one of the most concerning vectors. According to PwC, internal actors account for 31% of financial fraud. The real challenge is that they operate within expected systems and privileges—meaning they often go undetected. Whether it's contractors, sysadmins, or disgruntled staff, these actors have the access and knowledge to inflict serious damage. Factors like financial pressure, addiction, or a simple click on a phishing link can trigger an incident. Psychological and behavioural indicators, like entitlement or reduced loyalty, are increasingly important in threat detection frameworks.

INSIDER THREATS ARE ESCALATING

Insider Users like IT staff, contractors and former employees are seen as one of the most serious risks. With motivators of financial gain, personal grudges and coercion – Insider threats account for 31% of reported financial crimes.

2

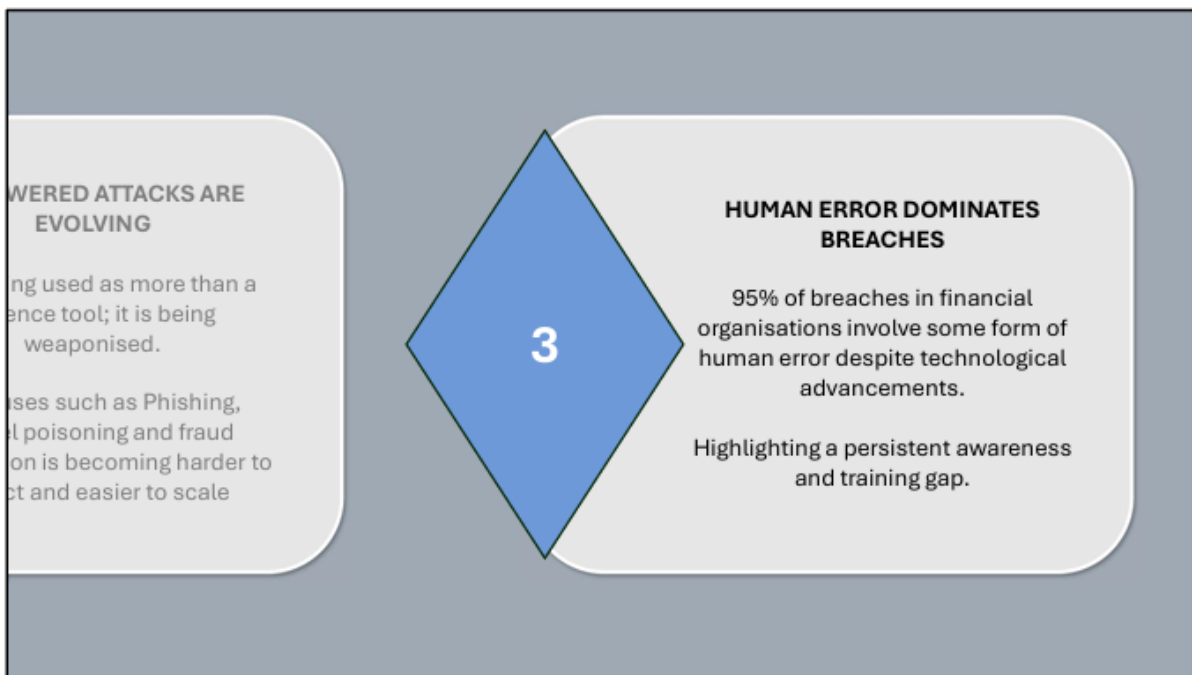
AI-POWERED ATTACKS ARE EVOLVING

AI is being used as more than a defence tool; it is being weaponised.

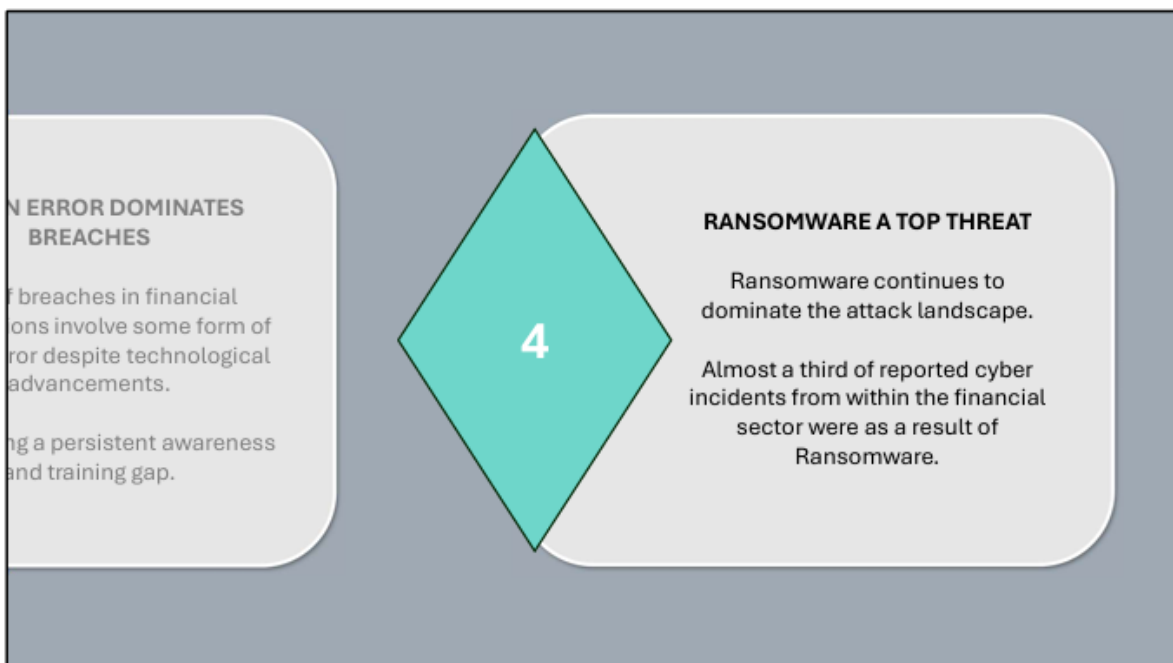
With uses such as Phishing, Model poisoning and fraud automation is becoming harder to detect and easier to scale

AI is a double-edged sword. It gives us speed, accuracy, and real-time detection—but attackers now use it too. We're seeing automated phishing, deepfake spoofing, and even AI model poisoning.

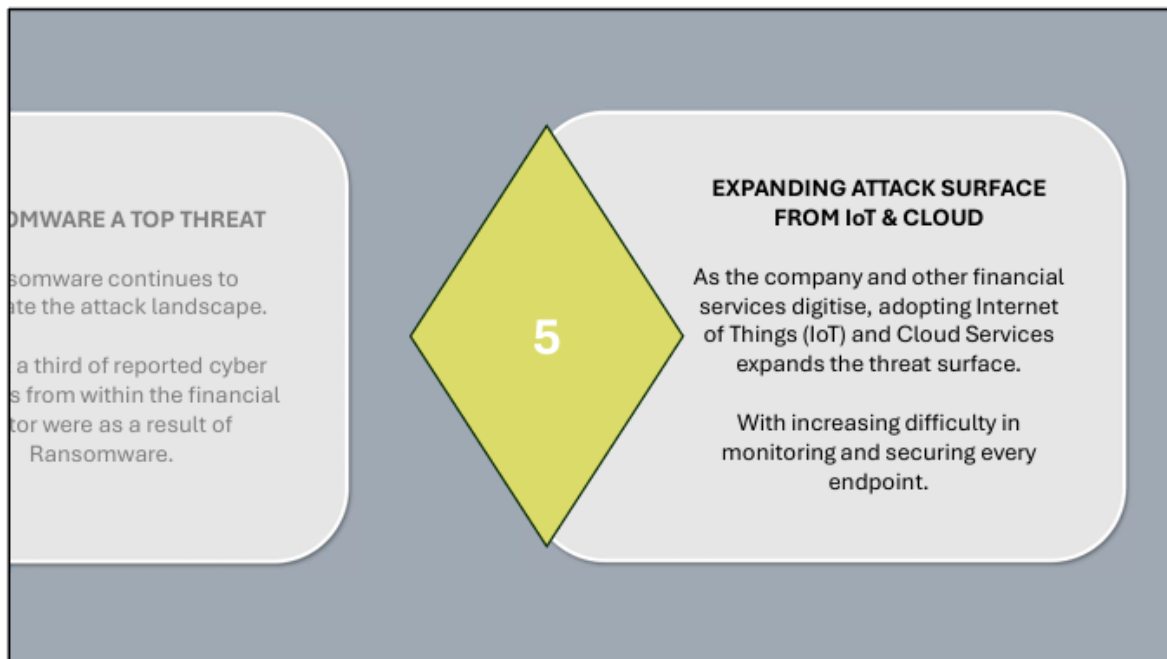
This raises the stakes. We need AI-literate security teams, explainable AI tools, and strict governance. And we must stay ahead of the ethical and regulatory curve—because when AI gets it wrong, the cost isn't just technical, it's reputational and financial.



It's startling but not surprising: 95% of breaches still come down to human mistakes. This underlines the importance of continuous Security Education, Training and Awareness (SETA) programmes—especially with hybrid working environments



Ransomware remains dominant—accounting for nearly a third of all reported incidents. What's evolving is the insider's role. Some insiders knowingly or unknowingly assist in attacks by weakening defences, disabling logs, or introducing malicious payloads. The overlap of ransomware and insider activity is making attacks more stealthy and devastating.



As our digital footprint expands with the use of cloud services, remote endpoints and IoT devices the attack surface grows. 74% of UK institutions report feeling vulnerable to insider threats (IEEE, 2023), reinforcing the need for proactive surveillance. Traditional perimeters are not enough we require layered and continuous surveillance and behaviour analytics.

Legal & Regulatory Considerations	
	Data Protection Act 2018 (UK GDPR)
	FCA's Senior Managers & Certification Regime (SM&CR)
	AI Governance

Legal & Regulatory Considerations	
	Data Protection Act 2018 (UK GDPR)
▪ Emphasises data minimisation and purpose limitation ▪ Requires clear consent and accountability for processing ▪ Enforced by the Information Commissioner’s Office (ICO)	

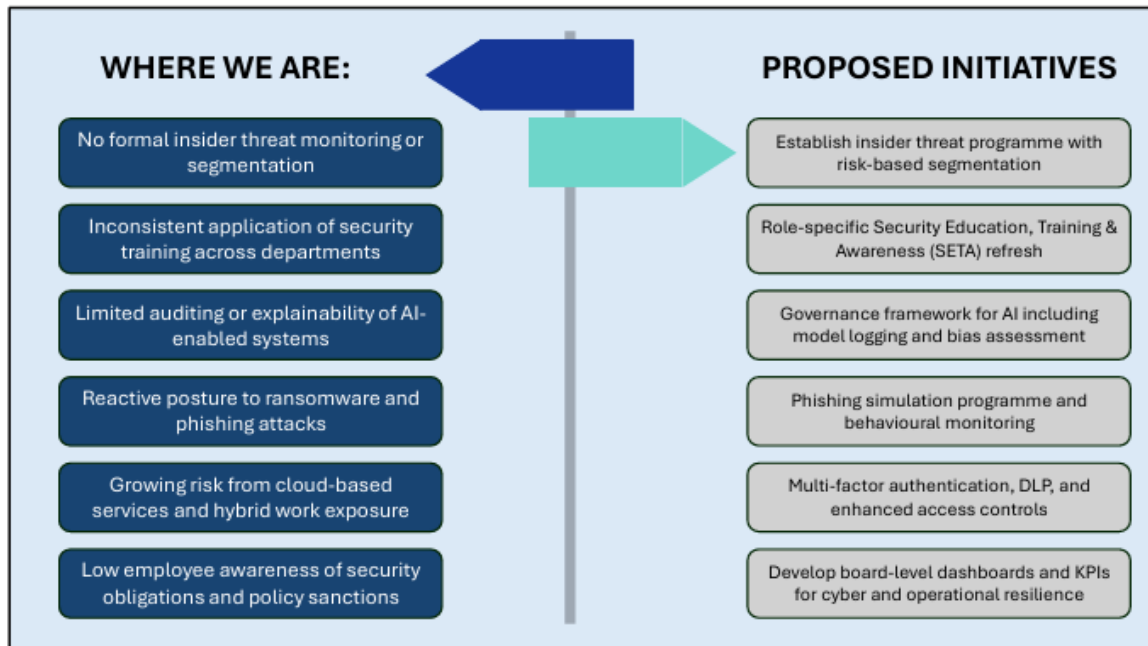
Legal & Regulatory Considerations	
	FCA’s Senior Managers & Certification Regime (SM&CR)
▪ Board-level accountability for operational resilience and data integrity ▪ Senior leaders can be held personally liable for failures in governance ▪ Aligns with FCA’s emphasis on cybersecurity as a conduct issue	

Legal & Regulatory Considerations	
	AI Governance
▪ ICO guidance on explainability and bias in AI systems ▪ EU AI Act will influence UK approaches, especially around high-risk AI ▪ Boards must ensure transparency, fairness, and lawful AI use	

Cybersecurity is no longer just an IT concern—it’s a boardroom issue. Under the UK’s Data Protection Act 2018, we’re expected to minimise data use, define clear purposes, and maintain tight controls. Failure to do so risks ICO enforcement and reputational damage.

The FCA’s SM&CR goes further. It puts personal accountability on senior managers for ensuring operational resilience, data protection, and robust risk oversight. If something goes wrong, regulators won’t just ask what happened—they’ll ask who was responsible.

And looking forward, AI regulation is on the horizon. The ICO and EU AI Act both stress transparency, non-discrimination, and accountability in how we build and deploy intelligent systems. If we wait for enforcement to catch up, we’ll be too late. Now’s the time to shape our governance practices—because regulation is coming.



This is a snapshot of where we are now—and where we need to go.

Our posture is currently reactive. We lack formal insider threat detection, our training is patchy, and there's minimal control over AI tool governance. Hybrid working and increased cloud exposure have stretched our monitoring capability.

The initiatives proposed are strategic: aligned to regulatory expectations and tailored to the actual threat landscape we've described.



Security Education, Training & Awareness (SETA)

AWARENESS

- Regular Internal Campaigns
- Gamified Modules and microlearning formats
- Posters, internal screen savers, security champions



Security Education, Training & Awareness (SETA)

TRAINING

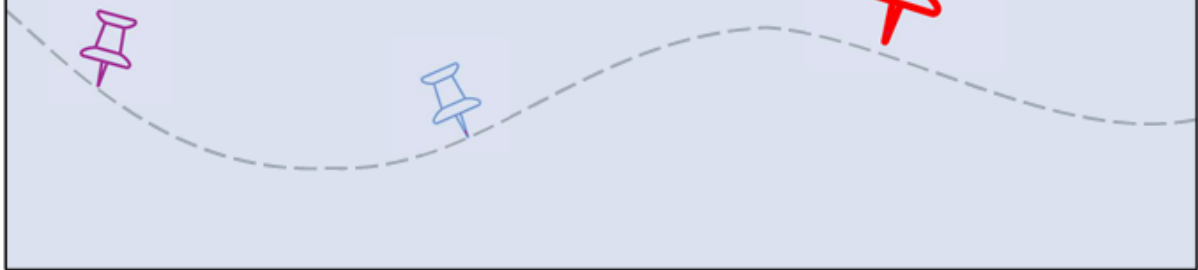
- Role-specific tailored training
- Monthly Phishing Simulations with feedback loops
- Mandatory onboarding and annual refresher modules



Security Education, Training & Awareness (SETA)

ACCOUNTABILITY

- Training Compliance tracked and reported to leadership
- Policy sign-offs
- Clear sanctions for repeat policy violations
- Behavioural monitoring linked to training gaps



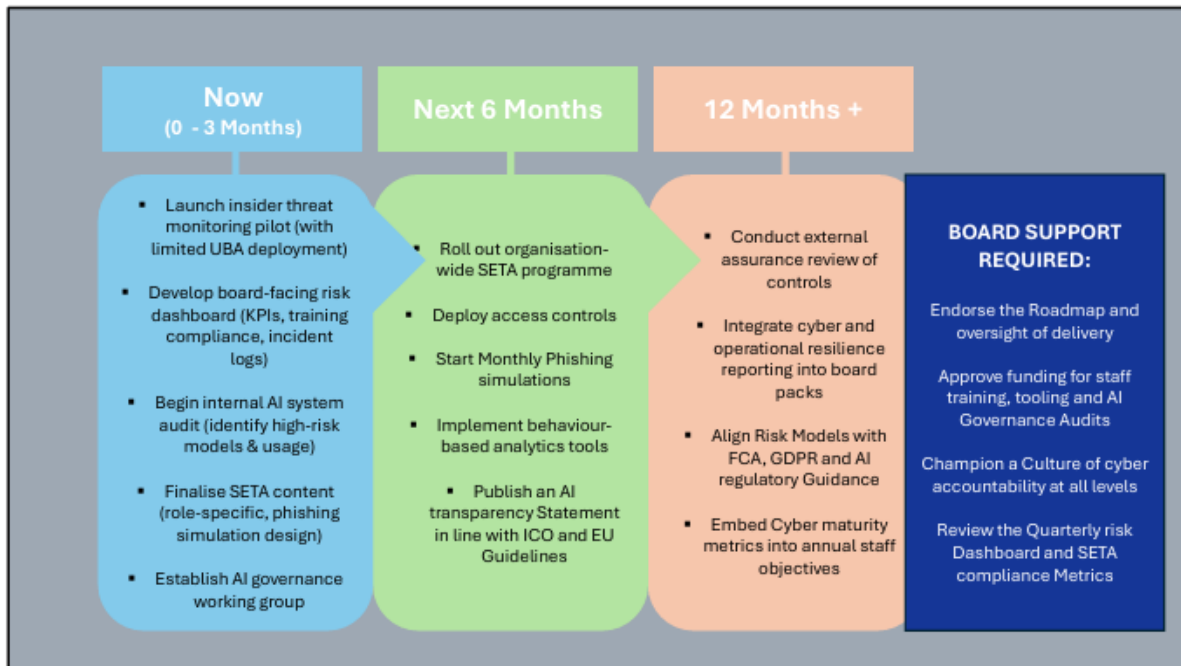
Our people are our greatest risk—and our greatest defence. FCA guidance and SETA research emphasise role-based, sustained, and measurable training.

We'll embed SETA into our organisational culture—not just as a once-a-year compliance exercise, but as a live behavioural programme.

We'll target training just like attackers do—based on access, role, and exposure.

And we'll close the loop by tracking compliance and awareness impact, with executive oversight.

This is not just awareness. It's operational resilience through people.



This roadmap takes us from reactive to resilient.

In the next three months, we lay the foundations—monitoring insider risk, auditing AI systems, and refining our SETA content.

By six months, we'll have training and analytics live across the business, with clearer visibility at board level.

Within a year, we expect to embed cyber maturity into both our culture and reporting framework, in line with FCA and GDPR obligations.

For this to succeed, we need more than operational execution—we need leadership. Board endorsement, funding, and cultural ownership are all essential.



That concludes the strategic overview. I now invite your questions, concerns, or recommendations—particularly around board-level priorities and next steps.

Thank you for your engagement.