



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

Student name: Hossam Abdalla

Student ID Number: 2416774

Module: Networks and Cyber Security
Essentials

Module code: ACCA4024

Lecturer: Munyaradzi N Murira

Assignment Title: Synthesize a solution
to a potential real-life scenario

Submission Deadline: 15/05/2026

Email address:

2416774@student.uwtsd.ac.uk



Table of Content

- Abstract.....1
- 1.Introduction.....1
- 2.Identification of Modern Threats.....2
 - 2.1External Threats.....2
 - 2.2 Internal Threats.....2
- 3. Modern Security Policies Aligned with Zero Trust and NIST CSF.....3
 - 3.1 Identity and Access Management (IAM) Policy.....4
 - 3.2 Data Classification and Protection Policy.....4
 - 3.3 Device Security and Endpoint Policy.....4
 - 3.4 Third-Party and Supply Chain Security Policy.....5
 - 3.5 Acceptable Use and Hybrid Work Policy.....5
- 4. Technical Mitigation Measures.....5
 - 4.1Multi-Factor Authentication (MFA) 5
 - 4.2 Security Information and Event Management (SIEM) 5
 - 4.3 Cloud Security Posture Management (CSPM) 5
 - 4.4 Immutable Backups and Ransomware Recovery.....6
 - 4.5 Patch Management Based on CISA KEV.....6
 - 4.6 Email Security Enhancement.....6
- 5. Proactive Monitoring and Incident Response.....6
 - 5.1 24/7 Monitoring Architecture.....6

5.2 Incident Response Plan.....	6
5.3 Incident Response Flow Diagram.....	7
6. Continuous Training and Security Awareness Programme.....	8
6.1 Continuous Simulated Phishing and Vishing Campaigns.....	8
6.2 Role-Specific Training Curriculum.....	8
6.3 Security Champions Programme.....	8
6.4 Gamification and Metrics.....	9
7. Conclusion.....	9
References.....	9
Appendix: Board of Directors Presentation — Speaker	
Notes.....	10

Abstract

This report presents a comprehensive cybersecurity framework for Vigilant Trust & Asset Management (VTAM), a medium-sized financial services firm facing escalating threats including sophisticated phishing campaigns and attempted ransomware infections. Drawing on the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF), Zero Trust Architecture principles from the Cybersecurity and Infrastructure Security Agency (CISA), and ISO/IEC 27001:2022, this report identifies modern internal and external threats, proposes aligned security policies, details technical mitigation measures, outlines a 24/7 monitoring and incident response plan, and describes an engaging continuous training programme. The findings demonstrate that a layered, Zero Trust-based approach is both technically feasible and strategically essential for VTAM to protect sensitive client assets and ensure regulatory compliance in an evolving threat landscape.

1. Introduction

The financial services sector remains one of the most targeted industries for cybercriminals. According to IBM's Cost of a Data Breach Report 2023, the average cost of a data breach in financial services reached USD 5.90 million, the second highest of any sector (IBM Security, 2023). VTAM recently experienced a sophisticated phishing campaign that bypassed traditional email filters and an attempted ransomware infection, exposing critical weaknesses in its legacy perimeter-based defences. The board has responded by mandating the development of a modern, Zero Trust-based security framework.

This report is structured to address five key areas as specified in the assignment brief: identification of modern threats, development of aligned security policies, proposal of technical mitigation measures, design of a monitoring and incident response plan, and a continuous training strategy. All recommendations are grounded in credible industry frameworks including NIST CSF 2.0 (NIST, 2024), CISA's Zero Trust Maturity Model (CISA, 2023), and ISO/IEC 27001:2022 (ISO, 2022). The analysis is informed by recent real-world cases including the 2023 MOVEit breach affecting Deutsche Bank, ING, and Putnam Investments, and the 2022 Optus breach demonstrating the consequence of unpatched cloud APIs in financial services which are incidents which share structural similarities with the vulnerabilities VTAM has already experienced (CISA, 2023b).

2. Identification of Modern Threats

2.1 External Threats

Ransomware-as-a-Service (RaaS) represents one of the most pervasive and financially devastating threat vectors facing organisations today. The RaaS model allows technically unsophisticated criminal groups to deploy enterprise-grade ransomware by subscribing to platforms offered by established threat actors such as LockBit and BlackCat/ALPHV (ENISA, 2023). VTAM's attempted ransomware infection is consistent with this trend. ENISA's Threat Landscape 2023 report identified ransomware as the foremost cyber threat across all sectors, with financial organisations suffering disproportionate impact due to the sensitivity and criticality of their data (ENISA, 2023).

Artificial Intelligence (AI)-powered social engineering, particularly vishing (voice phishing), presents an emerging and highly sophisticated threat. Threat actors now utilise generative AI tools to clone the voices of executives or trusted contacts, creating convincing phone-based fraud attempts. The Federal Bureau of Investigation issued a public service announcement in 2023 specifically warning of AI-synthesised voice attacks targeting corporate employees to authorise fraudulent wire transfers (FBI, 2023). For a financial institution like VTAM, this threat directly endangers client funds and firm assets.

Software supply chain attacks have become a systemic concern following high-profile incidents such as the MOVEit Transfer vulnerability exploitation in 2023, where the Cl0p ransomware group leveraged a zero-day SQL injection flaw (CVE-2023-34362) to exfiltrate data from over 600 organisations globally, including major financial institutions such as Deutsche Bank, ING, and Putnam Investments (CISA, 2023b). VTAM's reliance on third-party SaaS platforms and cloud services exposes it to identical supply chain risks, particularly where vendor security controls cannot be directly audited or independently verified.

Cloud misconfiguration remains a leading cause of data exposure. The Verizon Data Breach Investigations Report 2023 identified misconfiguration and human error as contributing factors in 74% of breaches (Verizon, 2023). As VTAM expands its cloud footprint, improperly configured storage buckets, permissive Identity and Access Management (IAM) policies, and unencrypted data-at-rest create substantial external attack surfaces.

2.2 Internal Threats

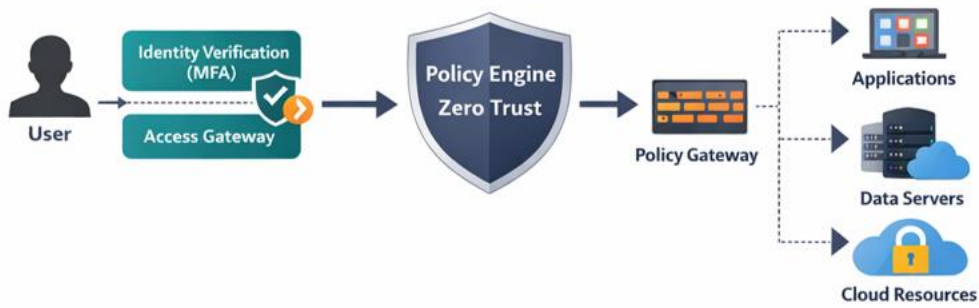
Insider threats, whether malicious or accidental, represent a persistent vulnerability. The hybrid work model adopted post-pandemic has significantly expanded the insider threat surface, with employees accessing sensitive systems from potentially insecure home networks and unmanaged devices. The 2023 Insider Threat Report by CISA highlights that unintentional insider employees, who inadvertently expose credentials or click phishing links, account for most insider-related incidents (CISA, 2023). For VTAM, the successful phishing campaign that bypassed traditional filters represents exactly this category of threat.

Privileged access abuse, where internal users with elevated permissions misuse their access rights, poses a significant risk. The 2023 Verizon DBIR found that privilege misuse was a contributing factor in 17% of insider-related breaches (Verizon, 2023). Without granular access controls and behavioural monitoring, a compromised or rogue privileged account can enable lateral movement across VTAM's entire network, resulting in catastrophic data exfiltration, fraudulent transactions, or full system sabotage.

Shadow IT and unmanaged application usage constitute a third category of internal risk with direct relevance to VTAM. Employees who deploy unapproved cloud applications or personal storage services to handle client data circumvent established security controls, creating data leakage vectors that are invisible to standard monitoring tools. A 2023 study by Gartner estimated that shadow IT accounts for 30-40% of IT spending in financial services organisations, with each unapproved application representing a potential compliance violation under GDPR and FCA conduct rules (Gartner, 2023). For VTAM, whose hybrid workforce increasingly relies on consumer-grade collaboration tools, this threat demands dedicated policy enforcement and continuous asset discovery as part of its Zero Trust implementation.

3. Modern Security Policies Aligned with Zero Trust and NIST CSF

The Zero Trust model, as defined by NIST Special Publication 800-207, is predicated on the principle of 'never trust, always verify', no user, device, or network segment is trusted by default, regardless of location (NIST, 2020). The following policies operationalise Zero Trust within VTAM's environment, mapped to the NIST CSF 2.0 Core Functions and ISO/IEC 27001:2022 Annex A controls.



Zero Trust Architecture



Figure 1: Zero Trust Architecture for VTAM

This diagram illustrates how all users and devices must pass identity verification (MFA) before accessing resources through a policy engine. Access is continuously monitored and controlled based on Zero Trust principles.

3.1 Identity and Access Management (IAM) Policy

Aligned with NIST CSF Function 'Protect' (PR.AA) and ISO 27001 Annex A 5.15 (Access Control), this policy mandates that all access to VTAM systems be authenticated through Multi-Factor Authentication (MFA). Privileged access must be governed by Privileged Access Management (PAM) solutions with just-in-time (JIT) provisioning, ensuring elevated privileges are granted only for specific, time-limited tasks. Role-based access control (RBAC) must be applied rigorously to ensure least privilege across all systems (NIST, 2024).

3.2 Data Classification and Protection Policy

This policy, aligned with ISO 27001 Annex A 5.12 (Information Classification), requires VTAM to classify all data assets into tiers (Public, Internal, Confidential, Restricted). Client financial data and personal identifiable information (PII) must be classified as Restricted and subject to encryption both in transit (TLS 1.3 minimum) and at rest (AES-256). Data loss prevention (DLP) controls must be implemented across email, cloud storage, and endpoint devices.

3.3 Device Security and Endpoint Policy

Consistent with CISA's Zero Trust Maturity Model pillar of 'Devices' (CISA, 2023), this policy requires all devices accessing VTAM resources to be enrolled in a Mobile Device Management

(MDM) or Unified Endpoint Management (UEM) platform. Devices must meet minimum security baselines: current OS patching, anti-malware, and endpoint detection and response (EDR) agents before being granted network access, enforced through Network Access Control (NAC).

3.4 Third-Party and Supply Chain Security Policy

Reflecting lessons from the MOVEit breach, this policy mandates that all third-party vendors undergo annual security assessments aligned with ISO 27001 Annex A 5.19 (Information Security in Supplier Relationships). Vendor contracts must include security clauses and the right to audit. Software Bill of Materials (SBOM) requirements must be stipulated for all software suppliers.

3.5 Acceptable Use and Hybrid Work Policy

All remote access to VTAM systems must occur exclusively via a company approved Zero Trust Network Access (ZTNA) solution instead of traditional VPNs. Personal devices are prohibited from accessing Restricted data. This policy aligns with NIST CSF's 'Govern' function (GV.PO) by establishing clear accountability and behavioural expectations (NIST, 2024).

4. Technical Mitigation Measures

4.1 Multi-Factor Authentication (MFA)

MFA must be enforced universally across all VTAM systems, with phishing-resistant FIDO2/WebAuthn hardware tokens mandated for privileged users and those accessing Restricted-tier data. Standard users must utilise authenticator application-based TOTP. This directly mitigates credential theft from the phishing campaign VTAM experienced, as stolen passwords alone would be insufficient to gain access (CISA, 2023).

4.2 Security Information and Event Management (SIEM)

VTAM must deploy a cloud-native SIEM platform (e.g., Microsoft Sentinel or Splunk Enterprise Security) to aggregate, correlate, and analyse logs from all network devices, endpoints, applications, and identity providers. The SIEM must be configured with detection rules mapped to the MITRE ATT&CK framework to identify tactics, techniques, and procedures (TTPs) commonly used by ransomware actors (MITRE, 2023). Dashboards must provide real-time visibility into threat indicators.

4.3 Cloud Security Posture Management (CSPM)

A CSPM tool (e.g., Microsoft Defender for Cloud, Prisma Cloud) must be deployed to continuously assess VTAM's cloud environments against security benchmarks such as the CIS Benchmarks and NIST SP 800-53. The CSPM will automatically identify and alert on misconfigurations such as public storage buckets, over permissive IAM roles, and unencrypted databases, directly addressing the misconfiguration risk identified in Section 2.

4.4 Immutable Backups and Ransomware Recovery

VTAM must implement a 3-2-1-1 backup strategy: three copies of data, on two different media types, with one offsite and one immutable (air-gapped or object-locked) copy. Backups must be encrypted and tested through quarterly restore exercises. This directly mitigates the impact of a successful ransomware attack by ensuring recovery is possible without paying a ransom (CISA, 2023).

4.5 Patch Management Based on CISA KEV

VTAM's patch management programme must prioritise vulnerabilities listed in the CISA Known Exploited Vulnerabilities (KEV) catalogue, applying patches for KEV-listed vulnerabilities within 15 days of publication. An automated vulnerability scanner (e.g., Tenable.io, Qualys) must perform weekly scans and generate prioritised remediation tickets, ensuring the organisation remains ahead of actively exploited flaws like those leveraged in the MOVEit attack.

4.6 Email Security Enhancement

To address the sophisticated phishing bypass VTAM experienced, the organisation must implement advanced email security controls beyond traditional filters. This includes AI-powered anti-phishing solutions that analyse behavioural signals and link reputation at time-of-click, DMARC/DKIM/SPF enforcement to prevent domain spoofing, and sandboxed attachment detonation. Microsoft Defender for Office 365 Plan 2 or Proofpoint Targeted Attack Protection are recommended solutions.

5. Proactive Monitoring and Incident Response

5.1 24/7 Monitoring Architecture

VTAM must establish a 24/7 monitoring capability through either an in-house Security Operations Centre (SOC) or a Managed Detection and Response (MDR) provider. The monitoring stack must include the SIEM described in Section 4, enriched by a Security Orchestration, Automation, and Response (SOAR) platform to automate repetitive analyst tasks and accelerate response times. Integration with threat intelligence feeds (e.g., ISAC feeds for financial sector threats) will enhance the detection of sector-specific TTPs (ENISA, 2023).

5.2 Incident Response Plan

VTAM's incident response plan must follow the NIST SP 800-61r2 framework, covering four phases: Preparation, Detection and Analysis, Containment/Eradication/Recovery, and Post-Incident Activity (NIST, 2012). The plan must include specific playbooks for ransomware and phishing incidents. The SOAR platform automates initial containment actions, such as isolating compromised endpoints and resetting credentials, within seconds of confirmed detection, which drastically reduces the dwell time.

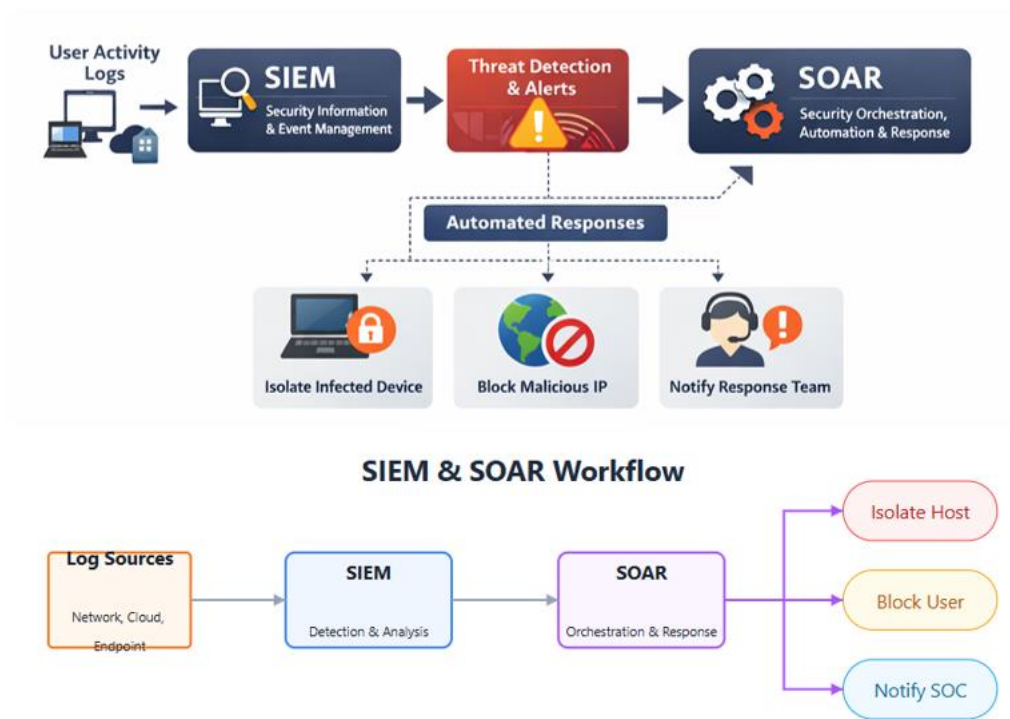


Figure 2: SIEM and SOAR Incident Response Workflow

This diagram shows how logs are collected and analyzed by SIEM, followed by automated response actions using SOAR to contain and mitigate threats in real time.

5.3 Incident Response Flow Diagram

The following table represents the structured Incident Response workflow for VTAM, illustrating the sequential phases and key actions aligned with NIST SP 800-61r2:

PHASE	KEY ACTIVITIES	TOOLS / RESPONSIBILITY
1. Preparation	Define playbooks, assign CSIRT roles, conduct tabletop exercises	IT Security Manager, CISO, Legal, HR Quarterly Reviews
2. Detection & Analysis	SIEM alerts triggered; SOC analyst triages severity; SOAR auto-enriches with threat intel	Microsoft Sentinel / Splunk + SOAR platform (Palo Alto XSOAR) SOC L1/L2 Analysts
3. Containment	Isolate affected endpoints; block malicious IPs/domains; reset compromised credentials	EDR (CrowdStrike Falcon) auto-isolate; Firewall policy push SOC L2, Incident Commander

4. Eradication & Recovery	Remove malware; rebuild from clean images; restore from immutable backups; verify integrity	Backup solution (Azure Immutable Blob / Veeam) IT Operations, Security Team
5. Post-Incident	Root cause analysis; lessons-learned report; update playbooks; notify regulators if required (GDPR Art. 33)	CISO, Legal, Compliance Within 72 hours of breach confirmation

Table 1: VTAM Incident Response Process Flow (Adapted from NIST SP 800-61r2)

6. Continuous Training and Security Awareness Programme

Research consistently demonstrates that human error remains the largest factor in successful cyberattacks. Verizon DBIR 2023 reports that 74% of all breaches involve the human element (Verizon, 2023). A one-size-fits-all, annual compliance video is wholly inadequate for the sophisticated social engineering threats VTAM faces. The following programme is designed to create a genuine and sustained security conscious culture.

6.1 Continuous Simulated Phishing and Vishing Campaigns

VTAM must deploy monthly simulated phishing campaigns using a platform such as KnowBe4 or Proofpoint Security Awareness Training. Crucially, these simulations must evolve in sophistication to mirror current attacker TTPs, including AI-generated spear-phishing emails tailored to individual roles and simulated vishing calls using voice synthesis. Employees who fail simulations must be immediately directed to targeted, contextual microlearning modules rather than punitive measures, creating a positive learning experience (FBI, 2023).

6.2 Role-Specific Training Curriculum

Generic training is insufficient. VTAM must implement role-specific curricula: the finance team must receive dedicated training on Business Email Compromise (BEC) and wire transfer fraud; IT administrators on secure configuration and privileged access hygiene; executive leadership on deepfake and vishing targeting; and all staff on data classification and incident reporting procedures. This aligns with the NIST CSF 'Govern' function (GV.AT) regarding workforce training (NIST, 2024).

6.3 Security Champions Programme

VTAM should designate Security Champions within each department such as employees who receive advanced security training and act as first-line security advocates and peer educators. This peer-based approach has been shown to significantly improve security culture metrics by decentralising security awareness beyond the IT department (ENISA, 2023). Champions will

provide monthly department-level briefings on emerging threats relevant to their specific business function.

6.4 Gamification and Metrics

To maintain engagement, training must incorporate gamification elements such as leaderboards, achievement badges, and inter-departmental security competitions. The programme's effectiveness must be measured through quantitative metrics: phishing simulation click rates (baseline measured at launch, target reduction to below 5% within 12 months), mean time to report a suspicious email (target: under 5 minutes), and training completion rates (target: 100% mandatory, 80% voluntary advanced modules). These metrics must be fed into a quarterly Security KPI dashboard reported to the board, enabling evidence-based investment decisions and demonstrating tangible return on the training programme (IBM Security, 2023). Annual red team exercises will provide independent validation of real-world effectiveness beyond self-reported metrics.

7. Conclusion

VTAM faces a complex and evolving threat landscape characterised by RaaS, AI-powered social engineering, supply chain risks, and cloud misconfigurations. The traditional perimeter-based security model that allowed a sophisticated phishing campaign to succeed is fundamentally inadequate for the current environment. The Zero Trust framework is designed to give VTAM a modern, multilayered defence. By combining strict identity management and advanced monitoring tools such as SIEM and CSPS with a NIST-aligned incident response plan and hands on simulation training, we can ensure the organization stays resilient against evolving threats.

Critically, these recommendations are not merely technical investments but strategic business decisions. A successful ransomware attack on a financial institution of VTAM's profile could result in regulatory penalties under GDPR and FCA regulations, reputational damage leading to client attrition, and direct financial losses far exceeding the cost of implementing these measures. The Zero Trust journey is continuous; VTAM must commit to regular framework reviews as the threat landscape evolves, ensuring its resilience remains current. By grounding all recommendations in NIST CSF 2.0, CISA guidance, and ISO 27001:2022, this report ensures VTAM's security posture is both robust and internationally recognised.

References

[1] CISA (2023) Zero Trust Maturity Model Version 2.0. Cybersecurity and Infrastructure Security Agency. Available at: <https://www.cisa.gov/zero-trust-maturity-model> (Accessed: 10 April 2026).

- [2] ENISA (2023) ENISA Threat Landscape 2023. European Union Agency for Cybersecurity. Available at: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023> (Accessed: 10 April 2026).
- [3] FBI (2023) Criminals are Impersonating Executives and Employees Using AI Voice Cloning. Internet Crime Complaint Center (IC3) Public Service Announcement. Available at: <https://www.ic3.gov> (Accessed: 10 April 2026).
- [4] IBM Security (2023) Cost of a Data Breach Report 2023. IBM Corporation. Available at: <https://www.ibm.com/reports/data-breach> (Accessed: 10 April 2026).
- [5] ISO (2022) ISO/IEC 27001:2022 — Information security, cybersecurity and privacy protection: Information security management systems — Requirements. Geneva: International Organization for Standardization.
- [6] MITRE (2023) MITRE ATT&CK Framework v14.0. The MITRE Corporation. Available at: <https://attack.mitre.org> (Accessed: 10 April 2026).
- [7] NIST (2012) Computer Security Incident Handling Guide. Special Publication 800-61r2. National Institute of Standards and Technology. Available at: <https://doi.org/10.6028/NIST.SP.800-61r2> (Accessed: 10 April 2026).
- [8] NIST (2020) Zero Trust Architecture. Special Publication 800-207. National Institute of Standards and Technology. Available at: <https://doi.org/10.6028/NIST.SP.800-207> (Accessed: 10 April 2026).
- [9] NIST (2024) The NIST Cybersecurity Framework (CSF) 2.0. National Institute of Standards and Technology. Available at: <https://doi.org/10.6028/NIST.CSWP.29> (Accessed: 10 April 2026).
- [10] Verizon (2023) 2023 Data Breach Investigations Report. Verizon Business. Available at: <https://www.verizon.com/business/resources/reports/dbir/> (Accessed: 10 April 2026).
- [11] CISA (2023b) Alert AA23-158A: CL0P Ransomware Gang Exploits MOVEit Vulnerability. Cybersecurity and Infrastructure Security Agency. Available at: <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-158a> (Accessed: 10 April 2026).
- [12] Gartner (2023) Managing Shadow IT Risk in Financial Services Organisations. Gartner Research Note G00779234. Stamford, CT: Gartner Inc.

Appendix: Board of Directors Presentation — Speaker Notes

The following section provides structured talking points for the 10-minute board presentation on VTAM's Zero Trust Security Framework. The presentation is designed to translate technical risks into business impacts for a non-technical executive audience.

Slide 1: The Threat Is Real — And Costly

Key Message: VTAM has already been targeted. The attempted ransomware infection and phishing bypass are not hypothetical. They are confirmed attack attempts against our firm. The

average financial sector data breach costs USD 5.90 million (IBM Security, 2023). A successful attack on VTAM would trigger FCA regulatory investigation, potential GDPR fines of up to 4% of global turnover, mandatory client notification, and severe reputational damage that would drive client attrition. The question is not whether we invest in security, it is whether we invest now or after a catastrophic breach.

Slide 2: Our Current Exposure

Key Message: Our traditional perimeter-based defences failed. Sophisticated phishing bypassed our email filters. Ransomware almost encrypted our client data. We are also exposed to AI-generated voice fraud targeting our treasury team, supply chain attacks through our SaaS vendors, and cloud misconfigurations creating invisible data leakage points. These are the four threat categories actively being exploited against financial firms today.

Slide 3: The Solution — Zero Trust Architecture

Key Message: We are proposing a Zero Trust framework, the gold standard endorsed by CISA, NIST, and adopted by leading global financial institutions. The principle is simple: no user, device, or system is trusted by default. Every access request is verified. This is not a single product purchase; it is a strategic architectural shift that dramatically reduces our attack surface. Key investments include phishing-resistant MFA for all staff, 24/7 threat monitoring via SIEM/SOAR, cloud security management, and immutable backups guaranteeing recovery without ransom payment.

Slide 4: Investment vs. Risk

Key Message: The proposed investment in our security framework is a fraction of the cost of a single successful attack. Beyond financial protection, this framework supports our regulatory compliance obligations under GDPR, FCA cybersecurity rules, and ISO 27001 certification. Which our largest institutional clients increasingly require as a condition of engagement. Security is no longer just an IT function; it is a business enabler and competitive differentiator.

Slide 5: Our Roadmap

Key Message: We are proposing a 12-month phase implementation. Phase 1 (Months 1-3): Deploy MFA, SIEM, and email security hardening. Phase 2 (Months 4-6): Implement CSPM, EDR, and immutable backup strategy. Phase 3 (Months 7-9): Deploy SOAR and formalise incident response playbooks. Phase 4 (Months 10-12): Launch continuous security awareness programme and

conduct board-level tabletop exercise. We request board approval and budget allocation to proceed to Phase 1 at once.