

Student Name: Olcay Sivas

Student ID: 2331962

Module: Networks and Cybersecurity Essentials

Module ID: ACCA4024

Lecturer: Munyaradzi N Murira

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

1. Abstract

This assignment analyzes the growing cybersecurity threats facing modern financial institutions. Increasingly relying on cloud services and interconnected systems, criminals continue and increasingly exploit new vulnerabilities through advanced attacks such as ransomware, AI powered social engineering and supply chain compromises. This report evaluates these threats and proposes a comprehensive strategy using modern security frameworks and best practices.

Herein the implementation of Zero Trust Architecture, Identity and Access Management and NIST protection policies is examined to increase organisational resilience. Mitigation factors such as Multi Factor Authentication (MFA), vulnerability management, cloud security, SIEM monitoring and SOAR automation are similarly discussed. Likewise, the importance of continuous staff development and training is referenced as a central component in this defence.

In total, it concluded that cybersecurity is no longer a technical consideration but also a strategic responsibility that requires continuous monitoring, adaptation and education in order that sensitive organisational assets are protected.

2.Introduction

Cybersecurity has become one of the most sensitive and significant challenges facing modern digitally operating organisations. This is particularly important in the financial sector where highly classified data and assets are continuously targeted by cyber criminals. While the rapid advancement of digital capability and infrastructure has created new opportunity for businesses, it has likewise expanded the arena and targets for malicious action. As a result, organisations must adopt new and reflexive strategies to defend against these sophisticated threats.

Vigilant Trust and Asset Management (VTAM) faces unprecedented and significant risks from cyber attacks such as ransomware, phishing and social engineering. These threats can lead to not just financial losses but also reputational and operational disruption which can lead to legal consequences if these risks are not effectively managed.

This report shall seek to investigate the major cyber threats currently affecting concerned organisations and evaluates how these could impact VTAM. It also looks at contemporary security policies, mitigation measures, proactive monitoring systems and employee awareness strategies that could be implemented to fortify an organisation's security position. Concludingly, this report shall seek to demonstrate how VTAM can improve organisational resilience against ever evolving, ever sophisticated threats and maintain secure operations in an increasingly digital, and potentially hostile, environment.

3. Identification of Modern Threats

3.1 Ransomware-as-a-Service (Raas)

Ransomware-as-a-Service (Raas) is a cybercrime business model. With this model, skilled developers lease their malicious software to the less technical attackers which are also known as affiliates. Raas model lowers the barrier to make entrance easier for cybercriminals and this causes an increase in cyber-attacks. Raas is a big threat for financial institutions like Vigilant Trust and Asset Management (VTAM) (CISA, 2023). VTAM holds sensitive client data and important assets, that's why they are a big target for financially motivated attackers because they know the company can't afford data leaks or prolonged operational downtime (ENISA, 2024)

3.2 AI Powered Social Engineering (Vishing)

Even though AI comes with positive incomes for humanity there is always a downside of it just like every other technological revolution. AI powered vishing represents a sophisticated evolution of social engineering. Nowadays attackers clone voices of the important persons with AI and make fraud phone calls which leads to gaining trust of the person they are speaking with and convinces them. This is a critical risk for a financial services firm like VTAM. The employees who have critical assets can be easily manipulated by attackers who clone their higher manager's voices with the help of AI and with this way the standard safety protocols can be easily bypassed (Microsoft, 2025).

3.3 Supply Chain Compromises

Supply chain compromises happen when cybercriminals infiltrate a primary target. To be able to do that, they first exploit vulnerabilities with the third-party vendor or software provider. Attackers compromise interconnected services which are demonstrated by the MOVEit file-transfer breach rather than attacking a well defended perimeter directly. Relying on SaaS applications and external vendors is a significant third-party risk for Vigilant Trust and Asset Management. When a trusted vendor is compromised, the attackers will gain a chance to exploit that trusted connection and gain backdoor access to VTAM's sensitive financial data by bypassing the organization's internal security controls (NCSC, 2023)..

3.4 Cloud Adoption and Hybrid Work Risks

The attack surface of modern organizations has been expanded due to the rapid transition to cloud services and hybrid work models. Nowadays corporate data is accessed with mobile devices, home networks and SaaS applications instead of confined within a traditional secure network perimeter. This infrastructure comes with vulnerabilities for Vigilant Trust and Asset Management. When cloud environments are configured or when remote employees access

financial systems over unsecured networks without identity verification the attackers can easily hijack the credentials .

4. Modern Security Policies

4.1 Zero Trust Architecture Framework

In order to ensure that the VTAM's infrastructure is protected against ever evolving cyber threats, a zero trust architecture must be adopted. This procedure adopts the concept of 'never trust, always verify' and assumes zero internal network trust. The process of authentication must be continuous and any device, user or app that seeks access is constantly re-authenticated and re-authorised. To be able to protect the asset management data VTAM makes sure that even if external perimeter defences are bypassed the attacker's movement in the network is highly restricted (NIST, 2020)..

4.2 Identity and Access Management (IAM)

VTAM must enforce a strict Identity and Access Management (IAM) policy centralized around the Principle of Least Privilege and strong authentication in order to operationalize the Zero Trust architecture. This policy helps all internal employees and external vendors to be granted with the minimum system permissions required to execute their duties. And more than that, this policy makes sure that all access requests are being verified by the Multi-Factor Authentication (MFA). VTAM effectively controls and checks identity and access rights contained breaches and minimizes the impact of compromised credentials. That leads to preventing the lateral movement towards critical finance databases.

4.3 Asset Management and Data Protection (NIST)

VTAM must implement comprehensive asset management and data protection policies to be able to be aligned with the NIST Cybersecurity Framework (CSF). VTAM will demand strict and automated inventory tracking of hardware and software to eliminate the blind spots and unauthorized applications by addressing the CSF's Identify function. The policy requires that all financial data must be heavily encrypted both at rest and transit to satisfy the protect and recover functions. And most importantly, VTAM must establish isolated and immutable backups. This makes sure that in the event of successful ransomware infection; backup data can not be maliciously encrypted or deleted and guarantees rapid organizational recovery (NIST, 2024).

5. Technical Mitigation Measures

5.1 Multi Factor Authentication (MFA)

Jeopardised credentials, whether they come from leaks, AI-augmented social engineering or phishing attacks, are a problematic risk that VTAM's must guard against. Passwords on their own are not enough and phishing resistant Multi Factor Authentications (MFA) methods are needed across all organisational domains to ensure secure system boundaries. Using a second factor, whether it be biometric or a time limited token from an authenticator app, MFA can effectively mitigate attacks using stolen passwords. This additional control layer is an obligatory mechanism for VTAM's identity and access management policy so that even if the initial login layers are breached, no unpermitted users can access sensitive financial systems (NCSC, 2024).

5.2 Vulnerability and Patch Management (CISA KEV)

VTAM must implement a risk based vulnerability and patch management program to be able to defend against external intrusions and supply chain compromises. The old fashioned and traditional patching schedules are not sufficient enough to prevent rapidly moving attackers anymore. So VTAM will mandate that all remediation efforts be prioritized based on the Cybersecurity and Infrastructure Security Agency (CISA) Known Exploited Vulnerabilities (KEV) catalogue. VTAM will reduce its attack surface and close the security gaps that ransomware affiliates seek to exploit by continuously scanning its infrastructure and taking immediate action against attackers by deploying patches for software flaws that are actively being weaponized in the wild (CISA, 2026).

5.3 Cloud Security Posture Management (CSPM)

Due to VTAM's reliance on cloud service support, a hybrid workforce securing this infrastructure is vital. VTAM must deploy Cloud Security Posture Management tools to be able to directly access the risks of cloud misconfigurations and data exposure. Uninterrupted and automated monitoring of cloud environments is provided by CSPM so that security flaws are promptly detected and remedied, these could be incorrectly secured storage buckets or unauthorised access configurations. Utilising these protocols, VTAM consistently maintains its cloud architectures security and compliance, thus removing any unforeseen blind spots that external actors could exploit (Microsoft, n.d.)

6. Proactive Monitoring and Incident Response

6.1 Continuous Monitoring and Threat Detection (SIEM)

A 24/7 active monitoring system must be used by VTAM via an SIEM solution so that the continuous effectiveness of the Zero Trust Architecture is ensured. The SIEM collects and analyses, in real time, log data from all connected devices, cloud environments and system end points and functions as a sort of centralised intelligence hub. Through the utilisation of behavioural analytics to identify anomalies, the SIEM detects threats like ransomware or unauthorised access before any significant damage can occur (Microsoft, 2026).

6.2 Automated Incident Response (SOAR)

Since relying on human intervention alone is not enough to protect against fast moving threats such as ransomware, in order to fully ensure that threats are contained, VTAM must combine SIEM with a Security Orchestration, Automation and Response (SOAR). This integration with the SIEM ensures a rapid automated response to any incident. For example, the SOAR system would rapidly isolate any compromised terminals from the network and remove any affected users access credentials. This would occur before any human analyst could even begin their investigation after detecting unauthorised activity (Microsoft, 2026).



7. Continuous Training and Awareness

7.1 Continuous Phishing and Vishing Simulations

Any forms of static compliance videos or training must be replaced with a continuous, dynamic and interactive program so that sophisticated social engineering threats are constantly combated. At its core, this will include regular and unplanned phishing and AI-powered vishing simulations which are designed to replicate the exact tactics used by modern threats. Any interaction of an employee with these simulated threats will result in them being forwarded to a micro learning environment so that their skills and resilience are updated and reinforced. This ensures that staff remain capable and vigilant and will be able to proactively identify any subtle indications of advanced threats in their routine operations (CISA, 2023)

7.2 Role-Specific Security Training

Utilising a universally implemented security architecture is often insufficient against modern and highly targeted threats. To maximise integrity, VTAM must adopt a role specific security strategy targeted to the specific risk profile of each department. For example, managerial and financial personnel might need specialised instruction on recognising Business Email Compromise (BEC) and deepfake executive vishing trying to authorise fraudulent transactions. While similarly, VTAM's IT and engineering personnel might require technical training focussed on securing cloud infrastructure, vulnerability management and how to effectively operate the newly developed and implemented SIEM and SOAR platforms (NIST, 2024).

Against modern, sophisticated and highly targeted threats, a universally implemented security architecture is often [insufficient](#). In order to maximise system and network integrity, a role specific security strategy must be adopted by VTAM for the individual risk profiles of each department. For example, managerial and financial workers might often require specialised instruction on Business Email Compromise (BEC) and deepfake executive vishing attempting to authorise fraudulent transactions. Likewise, IT and engineering personnel might need technical training focussing on security cloud infrastructure, vulnerability management and how to effectively operate and navigate newly integrated SIEM and SOAR platforms (NIST, 2024)

7.3 Fostering a Proactive Security Culture

VTAM must evolve beyond mandatory training and foster a proactive security culture to be able to truly solidify its defences. This process requires a paradigm shift which is explained as security must be viewed as a shared organizational responsibility rather than an isolated IT function. And most importantly VTAM must establish a no blame reporting system where employees are encouraged for flagging suspicious activities rather than concealing them out of fear of punitive action. By rewarding positive security behaviours and maintaining transparent communication VTAM can transform its workforce into an engaged and highly effective first line of defence (NCSC, 2023).

8. Conclusion

To conclude, it will be noted that modern cybersecurity threats are continuing to evolve in sophistication, ferocity and frequency, therefore making financial organisations such as VTAM perfect targets for cybercriminals. The threats previously discussed demonstrate that more traditional security models are no longer sufficient to protect sensitive assets.

To overcome these challenges, VTAM must adopt a layered, reflexive and proactive strategy built upon Zero Trust principles, strong IAM and NIST focussed security policies. Furthermore, implementation of technical solutions such as MFA, CSPM, SIEM and SOAR systems significantly enhances an organisation's ability to detect and respond to attacks in real time.

The technical aspects aside, the most important consideration is that of continuous employee education. Utilising lifelike simulations and role specific training, the development of a proactive security culture is essential in both reducing human error and fortifying organisational resilience. Therefore, by integrating both the technical and human components, VTAM will be better able to protect its critical assets, limit operational disruption and maintain its posture in an increasingly hostile environment.

9. References

CISA (2023) *Security Awareness and Training Program*. Available at: CISA Security Awareness Training Program (Accessed: 8 May 2026).

CISA (2023) *StopRansomware Guide*. Available at: <https://www.cisa.gov/stopransomware/ransomware-guide> (Accessed: 8 May 2026).

CISA (2026) *Known Exploited Vulnerabilities Catalog*. Available at:
<https://www.cisa.gov/known-exploited-vulnerabilities-catalog> (Accessed: 8 May 2026).

ENISA (2024) *ENISA Threat Landscape 2024*. Available
at:<https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024> (Accessed: 9 May
2026).

Microsoft (n.d.) *What is CSPM?*. Available at:
<https://www.microsoft.com/en-gb/security/business/security-101/what-is-cspm> (Accessed: 9
May 2026).

Microsoft (n.d.) *What is SOAR?*. Available at:
<https://www.microsoft.com/en-us/security/business/security-101/what-is-soar> (Accessed: 9
May 2026).

Microsoft (2025) *Microsoft Digital Defense Report 2025*. Available
at:[https://www.microsoft.com/en-us/corporate-responsibility/cybersecurity/microsoft-digital-de
fense-report-2025/](https://www.microsoft.com/en-us/corporate-responsibility/cybersecurity/microsoft-digital-defense-report-2025/) (Accessed: 9 May 2026).

Microsoft (2026) *Microsoft Sentinel overview*. Available
at:<https://learn.microsoft.com/en-us/azure/sentinel/overview> (Accessed: 9 May 2026).

NCSC (2023) *People and Security: The Human Element*. Available at:
<https://www.ncsc.gov.uk/collection/people-and-security> (Accessed: 10 May 2026).

NCSC (2023) *Supply Chain Security Guidance*. Available at:
<https://www.ncsc.gov.uk/collection/supply-chain-security> (Accessed: 10 May 2026).

NCSC (2024) *Recommended types of MFA*. Available at:
[https://www.ncsc.gov.uk/collection/mfa-for-your-corporate-online-services/recommended-typ
es-of-mfa](https://www.ncsc.gov.uk/collection/mfa-for-your-corporate-online-services/recommended-types-of-mfa) (Accessed: 12 May 2026).

NIST (2020) *SP 800-207: Zero Trust Architecture*. Available
at:<https://csrc.nist.gov/pubs/sp/800/207/final> (Accessed: 10 May 2026).

NIST (2024) *The NIST Cybersecurity Framework (CSF) 2.0*. Available at:
<https://csrc.nist.gov/pubs/cswp/29/the-nist-cybersecurity-framework-csf-20> (Accessed: 12
May 2026).

Cybersecurity: Increasing organisational resilience

Olcay Sivas
2331962

Introduction

A cybersecurity event can impact not only revenue BUT trust, regulation impact and operational workflow

- VTAM is a tempting target: Client & Financial data.
- Main risk - operational impact and loss of client confidence.
- Requirement - Resilience. This means Prevention, Detection, Remedy/Recovery & Accountability.
- Solution - Reduce risk while supporting growth

Main threats

Type	Implication	Impact
Ransomware	System paralysed and blackmail. Potential data leaks.	Operational paralysis, cost, data exposure
Voice/email imitation	Manager or client identity fraud	Loss of control. Unauthorised access.
Supplier hacking	A 3rd party becomes compromised. Unauthorised entry.	Operational and service impact. Unauthorised access
Cloud infiltration	Weak authorisation protocols.	Unauthorised access, data breach

3

Business Impacts

- Operational impacts: System downtime, impaired service delivery.
- Financial impacts: Response cost, legal fees, lost income and client compensation.
- Reputational: Loss of trust

Recommended strategic investment

- Zero Trust Principles: Verify and authenticate every user, access point and access requirement in real time.
- Fortify access and identity requirements
- Harden critical data protection: Encrypt, secure, backup
- Identify weaknesses: Protect vulnerabilities

Operational resilience capabilities

- Identify incidents before they become incidents.
- Central and pervasive monitoring to identify threatening activity
- Automated response to events to mitigate harm. Isolation & quarantine.
- Culture of continuous testing and education

Reduce system downtime, operational costs and systemic & reputational damage.

People, culture and governance

- Continuous training: Regular and realistic training scenarios and simulations
- Role specific training for managerial and executive positions
- Create a culture of accountability so that suspicious activity is promptly reported

Action required

Phase	Action	Value
1	Review current state, incident log and planning. Implementation strategy	Preliminary risk reduction
2	Cloud security management and vulnerability characterisation/mitigation strategies	Cut exposure
6–12 months	Maturity. Monitoring and automated response. Realistic and role based training	Detection & recovery

References

NIST (2024) *The NIST Cybersecurity Framework (CSF) 2.0*. Available at: <https://csrc.nist.gov/pubs/cswp/29/the-nist-cybersecurity-framework-csf-20> (Accessed: 11 May 2026).

ENISA (2024) *ENISA Threat Landscape 2024*. Available at: [ENISA Threat Landscape 2024 | ENISA](#) (Accessed: 9 May 2026).

CISA (2023) *StopRansomware Guide*. Available at: [#StopRansomware Guide | CISA](#) (Accessed: 8 May 2026).

NCSC (2023) *Supply Chain Security Guidance*. Available at: [Supply chain security guidance | National Cyber Security Centre](#) (Accessed: 10 May 2026).

NIST (2020) *SP 800-207: Zero Trust Architecture*. Available at: [SP 800-207, Zero Trust Architecture | CSRC](#) (Accessed: 10 May 2026).

Microsoft (n.d.) *What is SOAR?* Available at: [What Is SOAR? Technology and Solutions | Microsoft Security](#) (Accessed: 9 May 2026).

CISA (2023) *Security Awareness and Training Program*. Available at: <https://www.cisa.gov/resources-tools/resources/security-awareness-training-program> (Accessed: 8 May 2026).

NCSC (2023) *People and Security: The Human Element*. Available at: <https://www.ncsc.gov.uk/collection/people-and-security> (Accessed: 10 May 2026).

Cisco
Networking
Academy

Getting Started with Cisco Packet Tracer

Getting Started with Cisco Packet Tracer

Module 1: Download and Use Cisco Packet Tracer

Due 27 Sep 2026 11:59 PM

Module 2: Create a Cisco Packet Tracer Network

Due 27 Sep 2026 11:59 PM

Getting Started with Cisco Packet Tracer - Instructor-Activated Final Exam

Getting Started with Cisco Packet Tracer Course Final...

Prerequisites
End of Course...

Due 27 Sep 2026 11:59 PM

Graded

End of Course Survey

Due 27 Sep 2026 11:59 PM

Cisco
Networking
Academy

Getting Started with Cisco Packet Tracer

27 September 2026, 11:59 PM

29 January 2026, 01:18 AM

POINTS
100

CATEGORY
Assessment

ATTEMPTS
8 / Unlimited

PREREQUISITE

End of Course Survey (Assignment Submission)

INSTRUCTIONS

Getting Started with Cisco Packet Tracer Course Final Exam

Course Final Exam

1 Prerequisite

Q1

Q2

Q3

Q4

Q5

Result page

100%

You've scored 100%.
Congratulations, you have passed the exam.

Reset