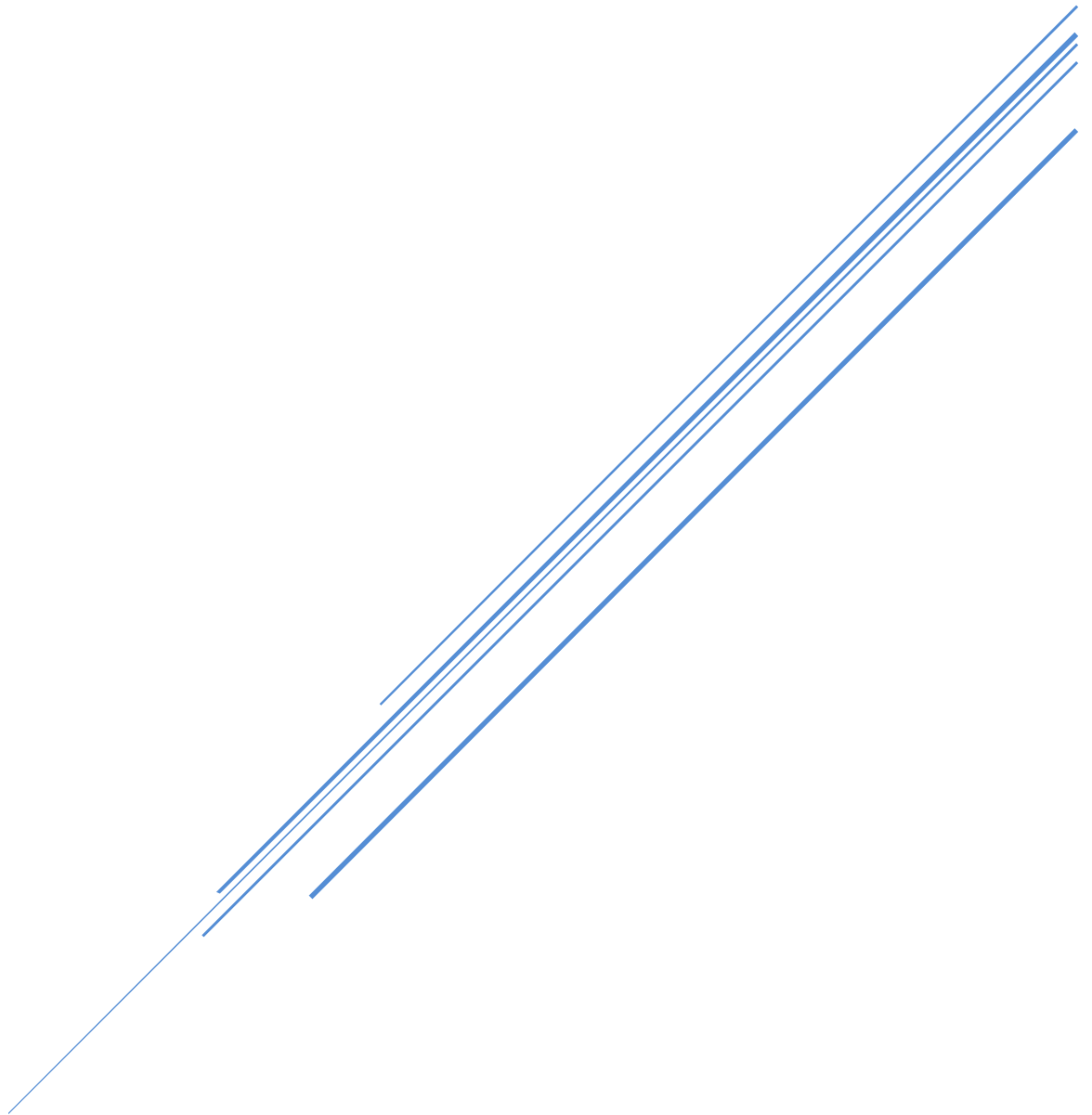


NETWORKS AND CYBER SECURITY ESSENTIALS (ACCA4024)



2413014

Table of Contents

1. Introduction 2

2. Modern Cyber Threats.....2

 VTAM Threat Matrix.....2

3. Zero Trust Security Framework.....3

4. Security Policies 3

5. Technical Protection Measures 4

6. Monitoring and Incident Response 5

7. Recovery and Resilience 5

8. Training and Awareness 5

9. Business Benefits 5

 Business Impact Summary.....6

10. Conclusion 6

11. References 7

12. Appendix: Board Presentation Summary 8

1. Introduction

VTAM is a medium-sized financial company that manages important client information and assets. Because of this, strong cybersecurity is essential.

In the past, many companies used a 'castle-and-moat' security model. This approach put strong protection around the network, but often trusted users inside too much.

This model is no longer enough. Staff now work from various locations, use laptops and mobile devices, and access cloud services. As a result, the network boundary is no longer clear.

VTAM has already experienced targeted phishing attempts and nearly had a ransomware incident. These events show the company needs a stronger, more modern security plan.

This report recommends that VTAM adopt Zero Trust Architecture and the NIST Cybersecurity Framework 2.0. These frameworks help the company check access, lower risk, and recover more quickly if an attack occurs [1], [2].

2. Modern Cyber Threats

Cyber threats are getting more advanced and harder to spot. Attackers now use automation, social engineering, and trusted online services to hide what they are doing [3].

For VTAM, the main risks are ransomware, phishing, fake voice calls, supply chain attacks, and attackers using regular business tools to avoid being noticed.

These threats can compromise confidentiality, integrity, and availability. Confidentiality means keeping client data private. Integrity is making sure data remains accurate. Availability means systems are working when people need them. [3]

VTAM Threat Matrix

Threat	Simple Meaning	Possible Impact
Ransomware-as-a-Service	Criminal groups sell ransomware tools to other attackers. The attacker may lock data and demand money [3].	Systems may stop working and client data may be exposed.
AI phishing and vishing	Attackers use AI to write convincing emails or make fake voice calls [3].	Staff may be tricked into giving passwords or approving payments.
Supply chain attack	Attackers target a trusted supplier or software provider [3].	VTAM could be affected even if its own systems are protected.
Living off the Land	Attackers use normal tools already on the system to hide [3].	The attack may stay hidden for a long time.
Information manipulation	False or misleading information is used to influence people or markets [3].	Trust, investment decisions, and reputation may be damaged.

3. Zero Trust Security Framework

Zero Trust is a security approach where no one is trusted by default. It does not matter if the user is inside or outside the office network; every access request must be checked [2].

The main idea is 'never trust, always verify.' VTAM should check the user, device, location, and risk level before allowing access.

Zero Trust also follows the principle of least privilege. Staff only get access to the systems and data needed for their job. If an account is hacked, the attacker has limited access.

Micro-segmentation is also important. It divides key systems into smaller sections, making it harder for attackers to move through the network.

The relationships between the policy engine, policy administrator, and enforcement point are illustrated in Fig. 1 [7].

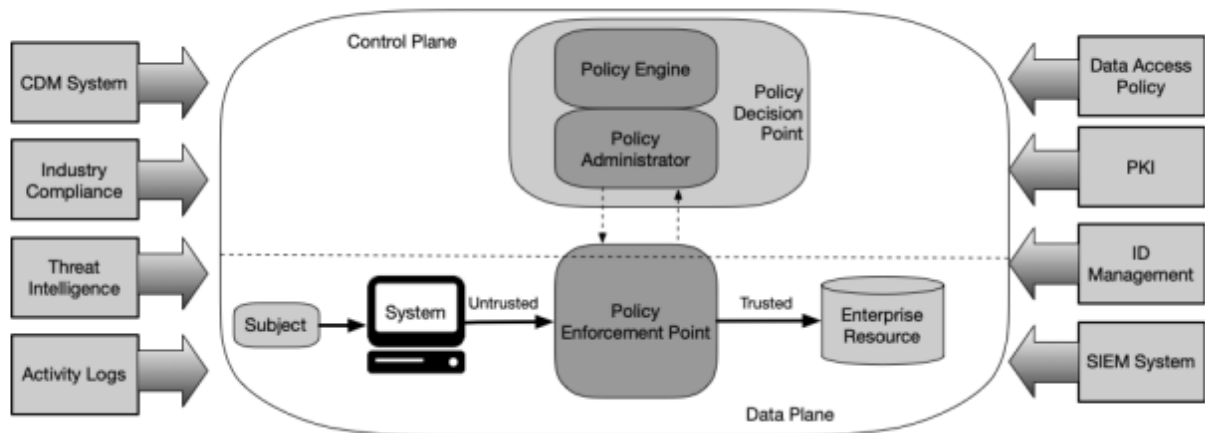


Figure 1 - Core Zero Trust Logical Components (adapted from NIST SP 800-207, Fig. 2) [7].

4. Security Policies

Strong cybersecurity needs clear rules. The NIST Cybersecurity Framework 2.0 includes a GOVERN function, which means leaders must understand and manage cyber risk [1].

The CSF 2.0 functions are shown in Fig. 2 [8].



Figure 2- NIST Cybersecurity Framework 2.0 Core Functions (from NIST CSWP 29, Fig. 2) [8].

VTAM should create an Identity and Access Management policy. This policy should require strong multi-factor authentication, especially phishing-resistant methods such as FIDO2 security keys [2], [3].

VTAM should also set up a cloud governance policy. This helps the company identify weak settings or errors in cloud systems before attackers can exploit them.

Finally, VTAM should use risk-based vulnerability management. This means fixing the most serious weaknesses first, especially those listed in the CISA Known Exploited Vulnerabilities catalogue [4], [6].

5. Technical Protection Measures

The protect function in the NIST Cybersecurity Framework focuses on safeguards that lower the risk of a successful attack [1].

VTAM should use hardware security keys or other phishing-resistant MFA. This makes it much harder for attackers to steal access, even if they trick a user.

The company should use Endpoint Detection and Response or Extended Detection and Response tools. These tools can detect suspicious behaviour, such as unusual PowerShell commands or odd login activity.

VTAM should encrypt important data. Data stored in systems should use strong encryption like AES-256, and data sent over networks should use secure communication such as TLS 1.3.

Patch management needs to be well organized. VTAM should check the CISA KEV catalogue often, scan its own systems, and quickly fix vulnerabilities that are being actively exploited [4].

6. Monitoring and Incident Response

VTAM should plan for the possibility of an attack. The detect and respond functions help the company spot problems early and act fast [1].

A Security Operations Centre can monitor logs from cloud systems, laptops, servers, and network devices. These logs can be collected in a Security Information and Event Management system.

Security Orchestration, Automation, and Response can help take quick action. For example, if ransomware is detected, the system can isolate the device and disable the account while the response team investigates.

VTAM should also follow a clear incident response process. This should cover preparation, detection, containment, eradication, recovery, and learning from incidents.

7. Recovery and Resilience

Recovery matters because no security system is perfect. If an attack happens, VTAM needs to keep the business running and restore key systems quickly [1].

VTAM should keep immutable backups, so attackers cannot easily delete or encrypt backup copies.

The company should test recovery plans every quarter. Testing ensures backups work and staff know what to do during a real incident.

VTAM should also prepare communication plans. If client data is affected, the company may need to inform clients and regulators as required by law.

8. Training and Awareness

Technology alone cannot stop every attack. Staff need to understand how attackers try to trick them.

VTAM should go beyond a single yearly training video. Instead, it should offer regular short training sessions and realistic phishing simulations.

Training should cover fake phishing emails, fake voice call examples, password safety, reporting procedures, and payment approval checks.

The company could also appoint security champions in each department. These staff members can help others follow good security practices.

9. Business Benefits

Zero Trust is not only a technical improvement. It also protects the business.

Better cybersecurity can lower the risk of financial losses, downtime, fines, and reputational damage.

For a financial company like VTAM, trust is crucial. Clients want to know that their information and assets are safe. A strong Zero Trust plan helps VTAM show it takes security seriously.

Business Impact Summary

Risk Area	Business Problem	Benefit of Zero Trust
Financial	Ransom payments, recovery costs, and lost business.	Lower risk and better control of security spending.
Reputation	Clients may lose trust after a data breach.	Shows clients that VTAM protects their data.
Regulation	Possible fines and investigations.	Helps prove that VTAM follows recognised security standards.

10. Conclusion

VTAM needs to update its cybersecurity, as the old 'castle-and-moat' model is no longer sufficient. Hybrid working, cloud services, phishing, ransomware, and AI-based attacks have all raised the risk.

Zero Trust gives VTAM a stronger, clearer approach. By checking every access request, using least privilege, monitoring systems, training staff, and preparing recovery plans, VTAM can protect client data and keep the business running.

Using the NIST Cybersecurity Framework 2.0 and NIST Zero Trust guidance provides VTAM with a recognised framework for improving security in a practical way [1], [2].

11. References

- [1] NIST, “The NIST Cybersecurity Framework (CSF) 2.0,” NIST Cybersecurity White Paper (CSWP) 29, Feb. 2024. [Online]. Available: <https://doi.org/10.6028/NIST.CSWP.29>

- [2] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, “Zero Trust Architecture,” NIST Special Publication 800-207, Aug. 2020. [Online]. Available: <https://doi.org/10.6028/NIST.SP.800-207>

- [3] ENISA, “ENISA Threat Landscape 2024,” European Union Agency for Cybersecurity, Oct. 2024. [Online]. Available: <https://www.enisa.europa.eu/topics/cyber-threats/threat-landscape>

- [4] CISA, “Known Exploited Vulnerabilities (KEV) Catalog,” Cybersecurity & Infrastructure Security Agency, 2024. [Online]. Available: <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>

- [5] ISO/IEC, “ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems,” 2022.

- [6] CISA, “Binding Operational Directive 22-01: Reducing the Significant Risk of Known Exploited Vulnerabilities,” Nov. 2021.

- [7] Zero Trust Architecture diagram (SP 800-207 Fig. 2)

- [8] NIST CSF 2.0 diagram (CSF 2.0 Fig. 2)

12. Appendix: Board Presentation Summary

Cyber Risk & Zero Trust Board Pack

Threats translated into business risk, controls and board decisions [1],



1. Why cyber risk is a board-level issue

VTAM has already faced advanced phishing and attempted ransomware, so the business question is resilience

What is at stake

Client and staff data, asset-management records, payments, privileged accounts and confidence in VTAM.

Why now

Hybrid work, mobile devices, SaaS and suppliers mean the old office perimeter no longer defines the attack surface [2], [3].

Board accountability

Cyber decisions affect risk appetite, service continuity, legal exposure and investment priorities [1], [7].

Typical incident path

1. Staff member receives convincing phishing or vishing contact [5], [6]
2. Credentials or MFA approval are captured [2]
3. Attacker accesses cloud files or finance workflow [1]
4. Ransomware or data theft creates disruption [6]

Business consequence

- Interrupted client service
- Recovery cost and overtime
- Possible data protection investigation
- Reputational damage
- Urgent disclosure or ransom pressure

Meaning: the framework should be judged by risk reduction, not by how many tools are purchased [1].

2. Modern threat picture for VTAM

Threats are easier to buy, more convincing and more likely to enter through identity, suppliers or cloud services.

RaaS

Ransomware kits and affiliate models lower the skill needed to attack a medium-sized firm [5], [6].
Business impact: outage and recovery cost

AI social engineering

AI-assisted phishing and vishing make fake requests sound more believable [5], [6].
Business impact: fraud and account takeover

Supply chain

A compromised IT, SaaS or payment supplier can become an indirect route into VTAM [5].
Business impact: data exposure and payment diversion

Cloud/hybrid

Stolen passwords, unmanaged devices and risky sharing bypass the office perimeter [2], [3].
Business impact: data leakage and privilege abuse



Human contact



Identity access



Cloud



Business data



Disruption

3

3. Risk priorities: the 4 risks to explain first

What could happen, why it matters, and the first control to fund.

Risk	Why it matters to VTAM	First action
1. Ransomware outage [6]	Can stop teaching systems, assessments, payroll, and file access.	Test backups, strengthen patching, and deploy endpoint detection [1], [4].
2. Cloud account compromise [2], [6]	A stolen password can expose learner data and shared files quickly.	Use MFA, device checks, and tighter sharing permissions [2], [3].
3. Supplier compromise [5]	A trusted provider can become the route into VTAM or its data.	Review supplier access, due diligence, and incident reporting terms [1], [5].
4. AI vishing / payment fraud [5], [6]	Staff may be tricked into approving a payment or resetting an account.	Use call-back verification and regular phishing/vishing practice [5], [6].

Board takeaway: prioritise controls that reduce disruption first - backups, MFA, supplier assurance, and staff verification [1], [2], [5].

4

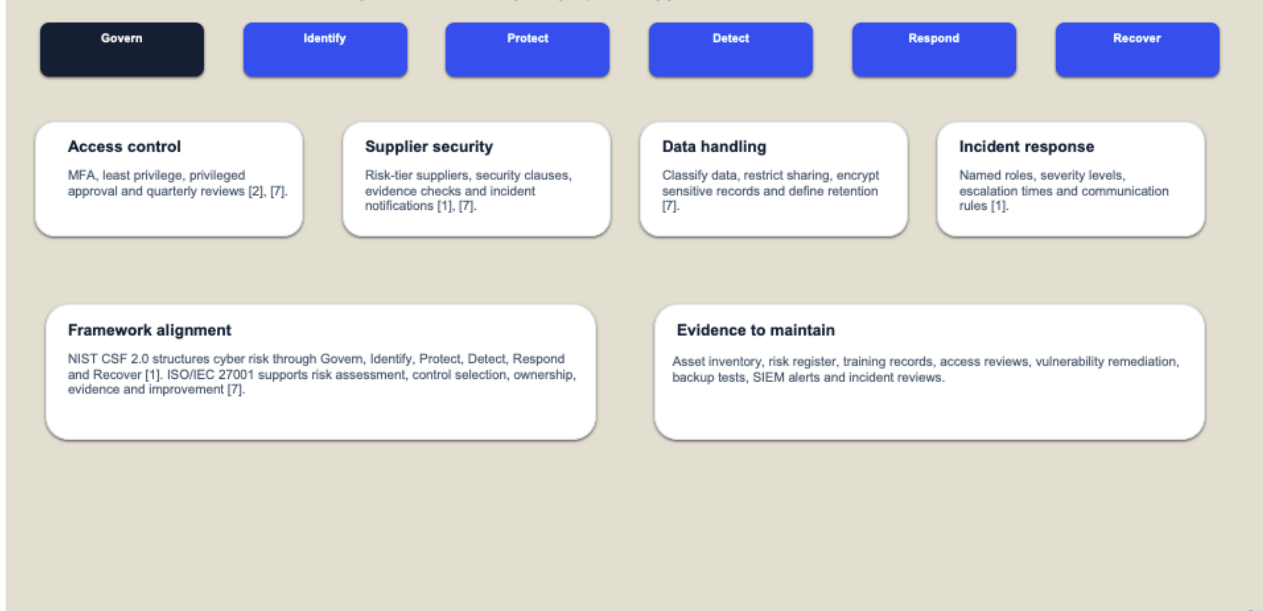
4. Zero Trust operating model

Zero Trust replaces location-based trust with evidence-based access decisions [2], [3].



5. Policy framework aligned to NIST CSF and ISO 27001

Policies should be short, owned and auditable. They turn Zero Trust into day-to-day expectations [1].



6. Layered controls and implementation detail

Prevention, detection, response and recovery must work together [1].

MFA + conditional access

Require MFA for all users; step-up verification for risky logins; block legacy authentication [2], [3].

EDR on endpoints

Deploy to staff devices; isolate suspicious laptops; investigate ransomware indicators [1], [6].

SIEM logging

Collect M365, VPN, firewall, EDR and admin logs; create high-value alert rules [1].

CSPM / cloud reviews

Scan cloud settings for public sharing, weak permissions and insecure storage [1], [3].

CISA KEV patching

Prioritise vulnerabilities known to be exploited, not only CVSS scores [4].

Immutable backups

Keep offline/immutable backups; test restore time and data integrity quarterly [1], [6].

Implementation principle: start with controls that reduce several risks quickly, prove they work, then automate where the process is stable [1].

Prevent

Detect

Respond

Recover

7

7. 24/7 monitoring and incident response flow

A repeatable process reduces confusion during ransomware, account takeover and supplier incidents [1], [6].

1. Alert

SIEM, EDR, user report or supplier warning [1]

2. Triage

Confirm scope, severity and affected assets [1]

3. Contain

Disable accounts, isolate devices, block indicators [1]

4. Eradicate

Remove malware, revoke tokens, close exploited route [1]

5. Recover

Restore systems and data from clean backups [1], [6]

6. Learn

Post-incident review; update controls and training [1]

Monitoring model

Alerts feed into a central SIEM [1]. SOAR playbooks automate repeatable steps such as disabling an account or opening an incident ticket, with human approval for major actions [1].

Ransomware trigger

If encryption, ransom note, mass file changes or suspicious admin activity appears, isolate devices, preserve evidence, check backups and start communications [6].

Success measures

Mean time to detect, mean time to contain, high-severity alerts, tested recovery time and post-incident action closure.

8

8. Ransomware playbook: before, during and after

Ransomware resilience requires rehearsed actions, tested backups and clear ownership [1], [6].

Before an incident

- MFA and least privilege for admin access [2]
- Patch internet-facing systems using CISA KEV [4]
- EDR on endpoints and servers [1]
- Immutable/offline backups [6]
- Restore tests with target recovery time [1]
- Supplier, legal and communications contacts [1]
- Tabletop exercise at least annually [1]

During first hours

- Declare severity and open incident log [1]
- Isolate infected devices; preserve evidence [1]
- Disable suspicious accounts and revoke tokens [2]
- Identify patient zero and lateral movement [1]
- Check whether data was exfiltrated [6]
- Start communication plan [1]
- Recover only from clean backups [1]

After recovery

- Root-cause analysis [1]
- Lessons learned and board report [1]
- Update alert rules and blocked indicators [1]
- Close policy or training gaps [1]
- Validate backup and patch improvements [1], [4]
- Check regulatory notification requirements [7]
- Track actions to completion [1]

Meaning: backups matter, but clean restoration, containment and evidence handling are what protect business continuity [1], [6].

9

9. Continuous training and security culture

Training should build safe behaviour under pressure, not only tick an annual compliance box [5], [6].

Induction baseline

Password safety, MFA prompts, reporting routes, data handling and safe cloud sharing [2], [7].

Monthly micro-learning

Five-minute topics: phishing, vishing, invoice fraud and supplier warnings [5], [6].

Simulated attacks

Regular phishing and vishing simulations with supportive coaching, not blame [5], [6].

Role-specific practice

Finance, HR, IT admins and managers rehearse realistic decisions [1].

Report

Verify

Escalate

Learn

Behaviour targets

Staff pause before unusual requests, verify through trusted channels and report quickly even if they clicked [5], [6].

KPIs

Report rate, repeat click rate, training completion, time to report and manager tabletop participation [1].

10

11. IEEE Reference List

- [1] National Institute of Standards and Technology, The Cybersecurity Framework (CSF) 2.0, NIST CSWP 29. Gaithersburg, MD, USA: NIST, 2024.
- [2] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, Zero Trust Architecture, NIST Special Publication 800-207. Gaithersburg, MD, USA: NIST, 2020.
- [3] Cybersecurity and Infrastructure Security Agency, Zero Trust Maturity Model, Version 2.0. Washington, DC, USA: CISA, 2023.
- [4] Cybersecurity and Infrastructure Security Agency, Known Exploited Vulnerabilities Catalog. Washington, DC, USA: CISA.
- [5] European Union Agency for Cybersecurity, ENISA Threat Landscape 2025. Heraklion, Greece: ENISA, 2025.
- [6] Verizon Business, 2025 Data Breach Investigations Report. New York, NY, USA: Verizon, 2025.
- [7] International Organization for Standardization, ISO/IEC 27001:2022: Information Security, Cybersecurity and Privacy Protection — Information Security Management Systems — Requirements. Geneva, Switzerland: ISO, 2022.