



# **Cyber Security Framework for Vigilant Trust & Asset Management (VTAM)**

ACCA4024 Networks and  
Cyber Security Essentials

Tom Owen 2520277

# Why Cyber Security Matters to VTAM



Recent phishing and ransomware incidents show clear cyber risk



Financial services firms are attractive targets for attackers



A successful attack could cause financial loss and downtime



Sensitive customer and business data could be exposed



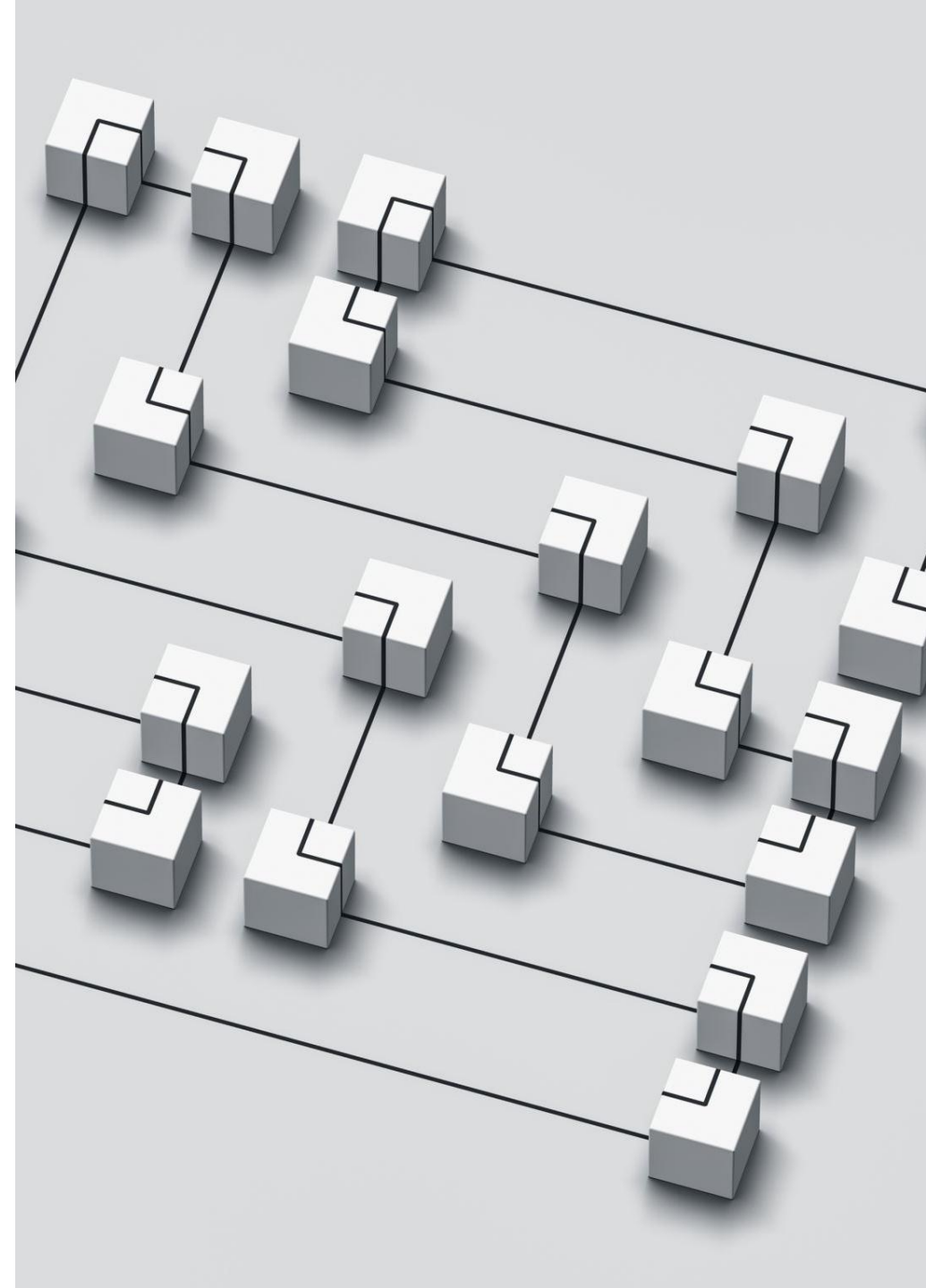
Reputational damage could reduce customer trust



Stronger cyber security is a strategic investment in resilience

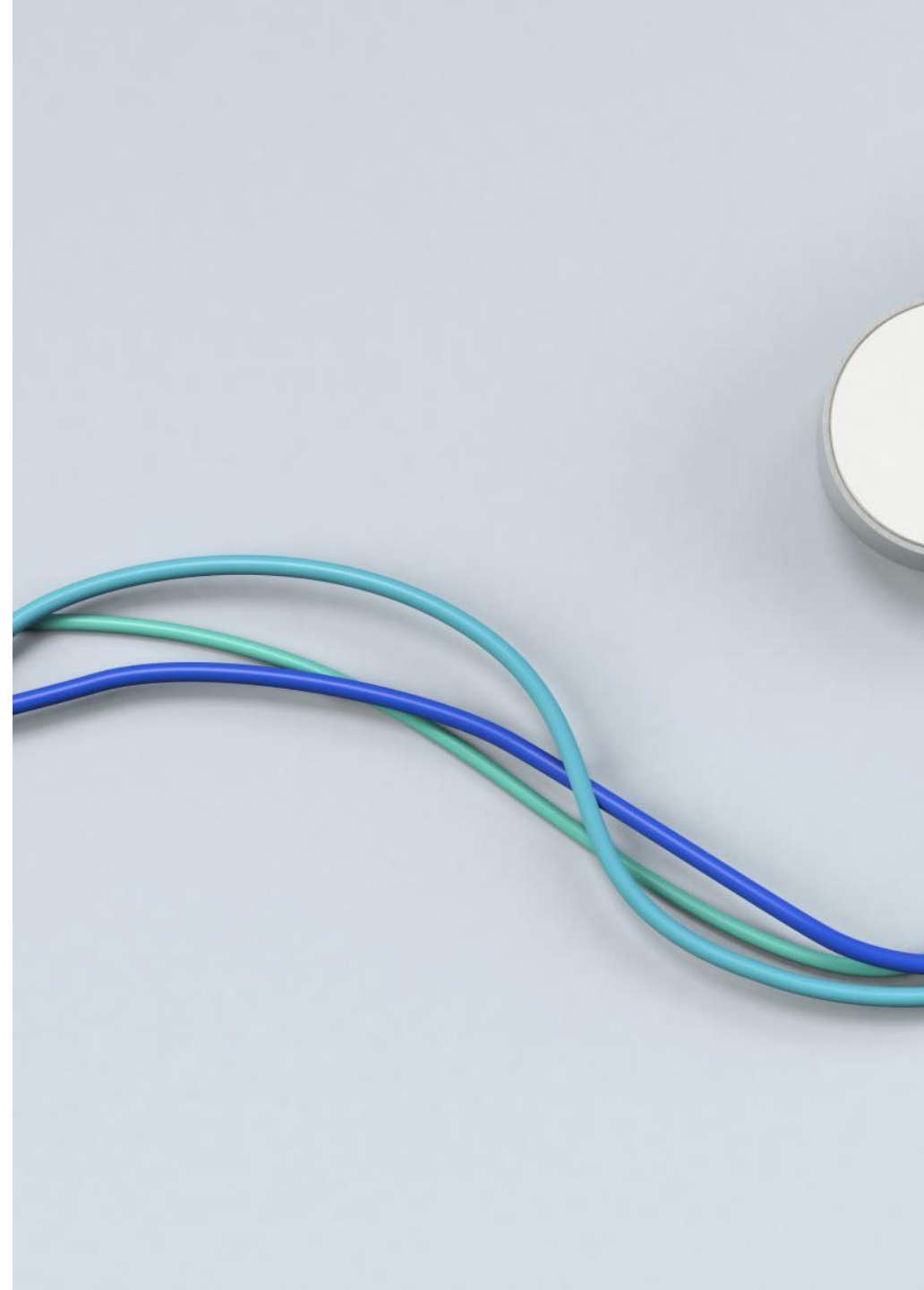
# Key Threats Facing VTAM

- Phishing and AI-powered vishing
- Ransomware-as-a-Service (RaaS)
- Supply chain compromise
- Cloud misconfiguration
- Hybrid working and remote access risks
- Insider threats



# Zero Trust as the Recommended Approach

- No user, device, or system should be trusted automatically
- Access should only be given after verification
- Least privilege should be applied to all staff accounts
- MFA should be used for remote and cloud access
- Device compliance should be checked before access is allowed
- This reduces the risk of unauthorised access and lateral movement



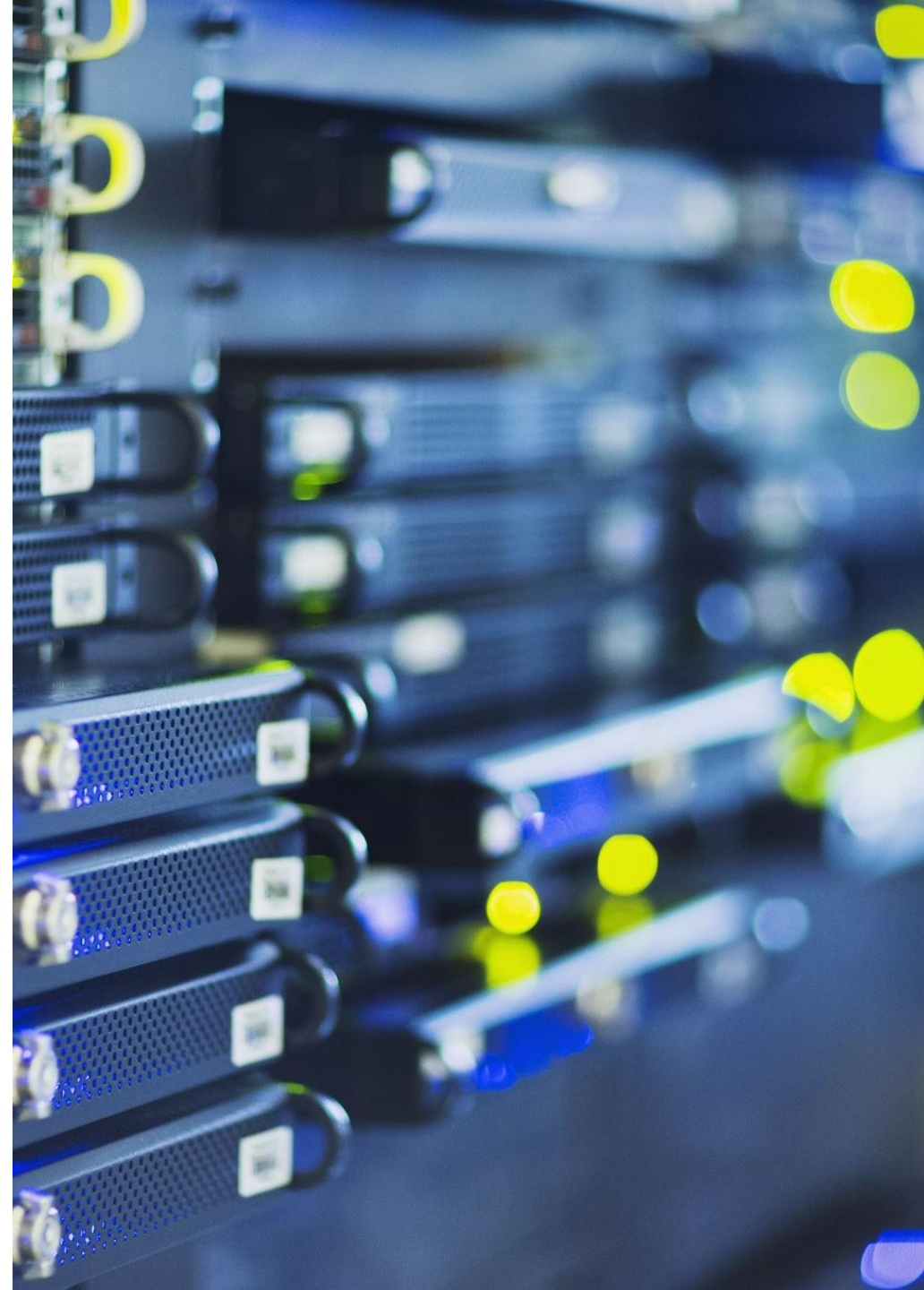
# Technical Mitigation Measures

- MFA to reduce unauthorised access
- Email filtering to reduce phishing risk
- Endpoint protection to detect malware and ransomware
- Network segmentation to contain breaches
- Patch management to reduce exploitable weaknesses
- Secure backups to support recovery after an attack



# Monitoring and Incident Response

- Continuous monitoring of systems and network activity
- SIEM to collect and analyse logs in one central place
- SOAR to support faster and more consistent responses
- Clear incident response process for serious threats
- Isolate affected systems quickly to stop the spread
- Use backups and recovery plans to restore services



# Staff Awareness and Training



Ongoing training improves staff awareness of modern attacks



Simulated phishing and vishing exercises build practical recognition skills



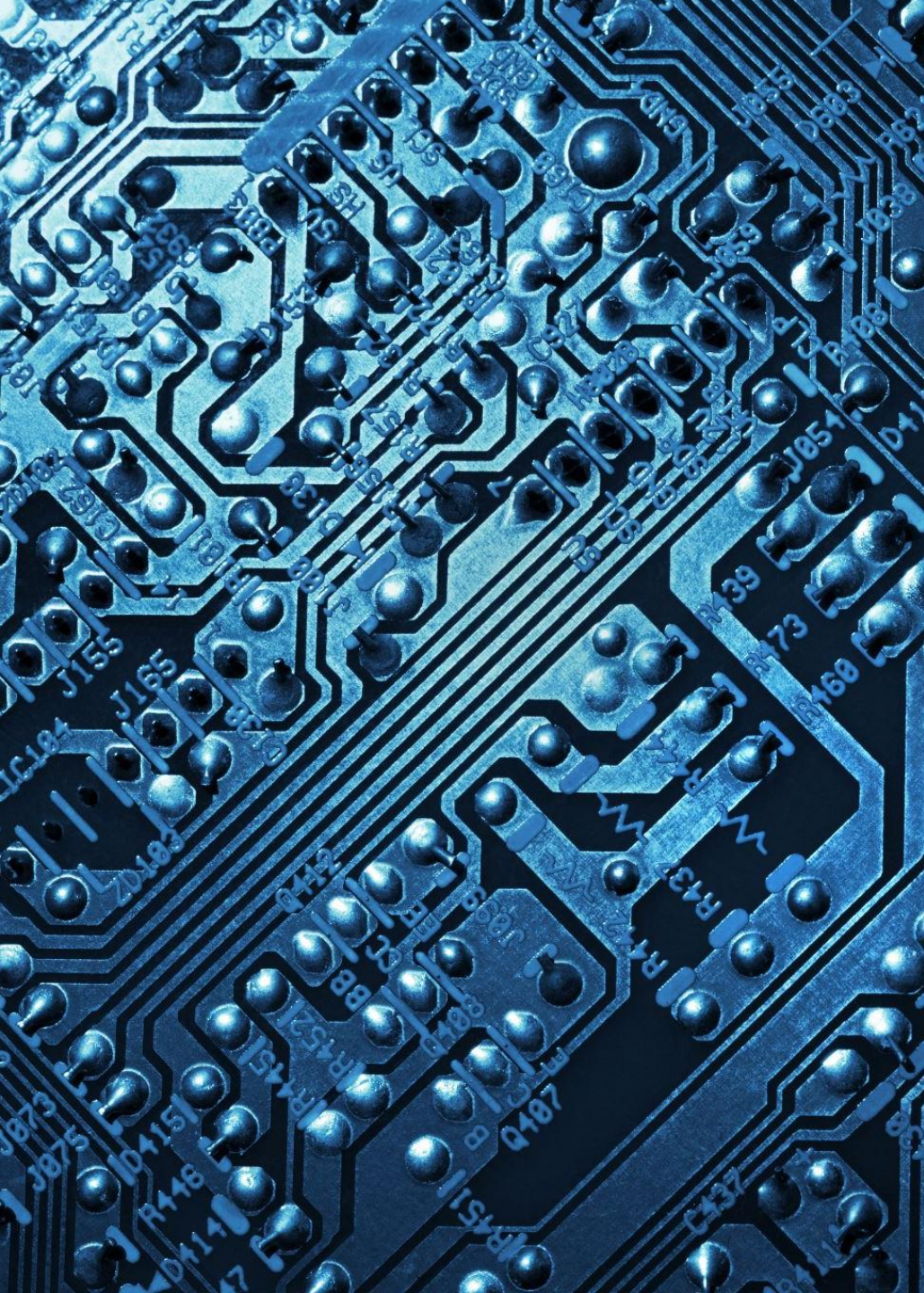
Fast reporting helps the organisation respond sooner



Better awareness reduces the chance of successful social engineering



Stronger staff awareness supports overall business resilience



# Conclusion and Recommendation

- VTAM is exposed to evolving cyber threats that could disrupt services and damage trust
- A Zero Trust framework is the most suitable response to these risks
- Security policies, technical controls, monitoring, and training should work together
- These measures would reduce the likelihood and impact of successful attacks
- Investing in cyber resilience is a business priority, not just a technical one

# References

- [1] S. Rose *et al.*, *Zero Trust Architecture*, NIST SP 800-207, 2020.
- [2] NIST, *Cybersecurity Framework (CSF) 2.0*, 2024.
- [3] CISA, *Zero Trust Maturity Model Version 2.0*, 2023.
- [4] CISA, *StopRansomware Guide*, 2025.
- [6] ENISA, *Threat Landscape: Finance Sector*, 2025.
- [7] NIST, *Computer Security Incident Response Recommendations and Considerations for Cyber Risk Management*, 2025.
- [8] CISA, *Recognize and Report Phishing*.