

Ethical Hacking

Critical Analysis of Recent Cybersecurity Attacks and Prevention Strategies

NAME: RASITHABANU ABDHUL RAHIM

STUDENT NUMBER: 2415470

LECTURER NAME: ASSOC. PROFESSOR CARLENE CAMPBELL

Table of Contents

1.Introduction - Phishing Attacks in UAE Financial Institutions.....	4
1.1 Attack Overview.....	4
1.2 Primary Cybersecurity Strategies Adopted	4
1.3 Reasons for the Failure of Cybersecurity Strategies in UAE Financial Institutions	5
1.4 Evidence-Based Analysis	5
1.5 Effective Countermeasures	5
1.6 My Recommendations for the Organization	6
2.Introduction - Phishing Attacks in Asian Healthcare Organizations.....	6
2.1 Attack Overview.....	6
2.2 Primary Cybersecurity Strategies Adopted	6
2.3 Reasons for the Failure of Cybersecurity Strategies in UAE Financial Institutions	7
2.4 Evidence-Based Analysis	7
2.5 Effective Countermeasures.....	7
2.6 My Recommendations for the Organization	8
3.Introduction - Cyber Attack Impact on Digital Twins.....	9
3.1 Attack Overview.....	9
3.2 Primary Cybersecurity Strategies Adopted	9
3.3 Reasons for the Failure of Cybersecurity Strategies in UAE Financial Institutions	9
3.4 Evidence-Based Analysis	9
3.5 Effective Countermeasures.....	10
3.6 My Recommendations for the Organization	10
4. Executive Summary.....	10
5. Environment Design and Virtualization.....	11
5.1 Infrastructure Overview	11
5.2 Layered Design and Responsibilities	11
6. Attack Surface Mapping & Vulnerability Identification.....	13
7. Frameworks Used to Guide the Attack Simulation	14
8. Types of Attacks Simulated.....	14

9. Recommended Solutions for the Threats Discovered in the Environment	17
10. Cost of Solution.....	19
11. Timetable for Execution of Solution.....	19
11.1 Invoice for Professional Service	20
12. References	20

1.Introduction - Phishing Attacks in UAE Financial Institutions

Cyberattacks are growing more frequent and sophisticated, posing major threats to businesses globally. Financial institutions, particularly in digital hubs like the UAE, face high risks from phishing, identity theft, and malware. These attacks steal sensitive data, disrupt operations, and cause financial losses. Protection Motivation Theory (PMT) helps explain how people and organizations respond based on perceived threats and their ability to cope. Real-world cases from UAE banks reveal gaps in current security measures. Stronger defences, employee training, and advanced technologies are needed to combat these evolving threats.

1.1 Attack Overview

Phishing attacks in the UAE increased by 230% in the second quarter of 2022. Cybercriminals mainly targeted bank customers by sending fake emails and messages that looked like they were from trusted financial institutions. These emails tricked people into sharing personal information such as usernames, passwords, and account numbers. In many cases, attackers also made phone calls pretending to be bank staff. The UAE Banks Federation reported a sharp rise in these types of scams, where fake callers posed as bank officials to steal sensitive data. These attacks led to unauthorized transactions, loss of customer trust, and financial damage to both individuals and banks.

1.2 Primary Cybersecurity Strategies Adopted

Organizational Frequent Training (OFT)

Financial institutions must regularly train employees to recognize cyber threats like phishing emails, malware, and hacking attempts. Since workers are often targeted through deceptive tactics, continuous cybersecurity education helps them identify and report potential attacks, reducing vulnerabilities.

Government Frequent Alerting (GFA)

Governments support cybersecurity by issuing timely alerts about emerging threats and enforcing data protection laws. These warnings help financial organizations prepare for and prevent major cyberattacks while safeguarding critical IT infrastructure and customer data.

Protection Motivation Theory (PMT)

PMT helps explain how UAE bank employees respond to cyber threats. The theory assesses how staff perceive risks and their ability to prevent attacks. Banks use PMT to design better security training programs. It shows why some employees follow protocols while others don't. This is crucial for improving cybersecurity culture in UAE financial institutions.

Structural Equation Modelling (SEM)

SEM helps UAE banks analyse complex cybersecurity relationships. It tests how leadership, training and alerts impact threat prevention. Researchers use SEM to verify which factors stop attacks. The method combines employee surveys with statistical analysis. It's perfect for studying human factors in UAE's banking security.

1.3 Reasons for the Failure of Cybersecurity Strategies in UAE Financial Institutions

The study has significant limitations that reduce its value. Its analysis of phishing lacks depth, failing to explore root causes or properly assess strategies like OFT/GFA. Methodological weaknesses include a small expert panel (only 5 reviewers), limited testing (30 respondents), and high survey rejection rates (58 discarded), indicating design flaws. The narrow focus on four UAE bank types restricts broader applicability, while reliance on self-reported data risks bias. Without comparisons to global practices or proof that recommended solutions work, the paper offers little beyond basic statistics and generic recommendations.

1.4 Evidence-Based Analysis

The study surveyed 310 banking employees, with 85% male and most aged 35 - 44. About 72% had 5 -10 years of experience, and 85.5% were non-UAE citizens. Most worked in Islamic banks (51.6%). The top cyber threats reported were viruses (38.7%) and malware (25.5%), followed by DoS and phishing (10.6% each). Cyberstalking and identity theft were less common. Notably, 35% said cybersecurity leadership practices in their organizations were below 50%, showing weak prevention efforts.

- **Threat Appraisal:** Many employees underestimated phishing threats because they trusted digital messages too much.
- **Coping Appraisal:** Poor email filters and lack of training made people feel less confident in preventing attacks.
- **Leadership Mediation:** Cybersecurity leaders played a key role by enforcing rules like multi-factor authentication and encouraging alertness.

1.5 Effective Countermeasures

1. Enhanced PMT-Optimized Cybersecurity Communications

Banks should improve cybersecurity alerts by tailoring them to staff personalities. Workers who take more risks could see real examples of cyberattack damage, while careful employees might get step-by-step safety guides. Instead of paper notices, banks could use live digital screens showing each worker's security performance, like how often they click risky links. This personal approach helps everyone understand threats better and see how their actions affect safety. By matching warnings to how people think and showing real results, banks can make security messages work better for all employees.

2. AI-Powered Defence Stack

Deploy multilingual NLP tools to scan emails in real-time, detecting subtle social engineering cues in both Arabic and English communications. Augment this with behavioural biometrics that track typical user patterns, automatically flagging anomalies like logins from unusual locations or times. This dual-layer AI approach combines linguistic analysis with activity monitoring to catch both phishing content and compromised accounts.

3. Threat Intelligence Sharing

The UAE should create a Financial CERT (cyber emergency team) to help banks share attack information instantly. This system would connect all banks and automatically send government security alerts directly to their monitoring systems. When one bank spots a new threat, all others would get immediate warnings to block the danger. The network would focus on practical threat data like harmful

websites or malware codes, allowing automatic protection across the entire banking sector. This united approach would help stop cyberattacks faster and more effectively.

1.6 My Recommendations for the Organization

As cybersecurity threats grow more sophisticated, UAE banks must take decisive action to protect their institutions, customers, and reputation. Based on proven strategies and local insights, here's what they must implement and the measurable results they can expect.

1. AI-Powered Email defence

- Action: Deploy UAE-tuned NLP filters analysing Arabic/English phishing patterns and behavioural biometrics monitoring
- Outcome: Expect 60-70% reduction in successful phishing penetrations within 6 months, with false positives cut by half compared to current systems

2. Hyper-Relevant Employee Training

- Action: Implement bi-monthly, personalized training modules using real UAE phishing case studies
- Outcome: Achieve 80%+ employee threat recognition rates (current avg: 45%) and reduce click-throughs on test phishing emails by 75% year-over-year

3. UAE Financial Cyber Alliance

- Action: Lead creation of cross-bank CERT with real-time threat sharing and automated government alert integration
- Outcome: Cut response time to new threats from days to hours, preventing estimated AED 50M+ in potential annual fraud losses

2.Introduction - Phishing Attacks in Asian Healthcare Organizations

2.1 Attack Overview

The study highlights five major cyberattacks on Asian healthcare Trojans, phishing, ransomware, APTs, and credential theft exploiting outdated systems and human error. Notable cases include Sing Health's 1.5M-record breach (2018) and WannaCry's disruption in Indonesia/Japan. Strengthening defences through vulnerability management, staff training, and NIST frameworks is critical to reducing risks.

2.2 Primary Cybersecurity Strategies Adopted

Framework Implementation

Asian healthcare organizations adopted globally recognized cybersecurity frameworks like NIST and ISO 27001. These frameworks help establish standardized security protocols, focusing on risk management, vulnerability assessment, and incident response. They align with international best practices while addressing region-specific challenges.

Vulnerability Management

A critical area of focus is proactive vulnerability management. This involves regular system scans, timely patch updates, and tools like OpenVAS to target weaknesses in outdated software and medical

devices. These vulnerabilities are often exploited in attacks such as ransomware and credential compromise.

Workforce Training and Awareness

To mitigate phishing and social engineering attacks, comprehensive employee training programs are implemented. These programs focus on recognizing suspicious emails, secure data handling, and reporting potential breaches to internal security teams.

Data Protection Measures

Encryption technologies and strict access controls are employed to protect sensitive patient data. Multi-factor authentication (MFA) and role-based access ensure that only authorized personnel can access or modify critical health records.

Incident Response Planning

Preparedness is enhanced through detailed incident response plans. These plans include containment, eradication, and recovery procedures. Regular drills and simulations ensure teams are ready to handle real-world breaches, minimizing downtime and data loss.

Regulatory Compliance

Compliance with regional regulations such as India's DISHA Act and Singapore's Cybersecurity Act reinforces security postures and ensures legal adherence. These regulations mandate periodic audits, data localization, and mandatory breach disclosures.

Cloud Security Enhancements

With healthcare data migrating to the cloud, additional safeguards like encrypted storage, API security controls, and continuous monitoring are implemented. These measures protect against cloud-specific threats such as unauthorized access and misconfigurations.

2.3 Reasons for the Failure of Cybersecurity Strategies in Asian Healthcare Organizations

Asian healthcare organizations struggle with cybersecurity due to outdated technology infrastructure, including unpatched medical devices and legacy systems vulnerable to attacks like WannaCry. Limited budgets restrict investments in modern security tools and skilled personnel, while inadequate staff training leaves institutions exposed to phishing and social engineering threats. Weak regulatory frameworks fail to enforce strict cybersecurity standards compared to Western counterparts like HIPAA, and slow incident response times allow breaches to escalate. Over-reliance on basic perimeter defences and poor vendor security practices further compound these risks, creating systemic vulnerabilities that demand urgent policy reforms and technological upgrades to protect sensitive patient data effectively.

2.4 Evidence-Based Analysis

Data confirms phishing as a critical threat to Asian healthcare. Singapore logged 47,500 phishing URLs in 2019, with attacks spiking 200x during COVID-19. The 2018 Sing Health breach exposed 1.5 million records from a single phishing email. Globally, 60% of healthcare breaches originate from email compromises (HIMSS), with Malaysia ranking as Asia's 3rd most-targeted nation (Symantec 2018). Attackers exploit three key weaknesses: high-value medical data, untrained staff, and inadequate email security.

2.5 Effective Countermeasures

1. NIST Framework for Phishing defence

The NIST Cybersecurity Framework provides a structured defence against phishing through five key phases: Identify critical assets and entry points, protect with email authentication and network segmentation, detect threats via 24/7 monitoring, respond with automated containment, and recover via backups and reviews. Mandatory quarterly risk assessments help counter evolving tactics like AI-generated scams. Singapore's Sing Health reduced phishing incidents by 58% after implementing this approach

2. System Hardening Against Phishing

The Malware-Digital study emphasizes disabling macros in email attachments, as 75% of healthcare malware enters this way. Monthly patching of browsers/email clients is critical 60% of breached systems in Singapore had outdated software. Automated patch management and application whitelisting are recommended to protect vulnerable medical devices and EHR systems from credential-stealing phishing attacks.

3. Staff Training Against Phishing

The Malware-Digital study shows trained staff cut phishing success by 68%. Key steps like teach email verification, link checking and attachment scanning. High-risk groups like doctors need extra training, especially for old systems (82% of thefts). Singapore's method works best monthly fake phishing tests keep everyone alert.

2.6 My Recommendations for Healthcare Organizations

1. Immediate Phishing defence Implementation

- Action: Deploy AI-powered email filters with sandboxing technology across all hospital communication systems.
- Outcome: Reduce phishing email delivery by 92% and prevent 80% of malware infections from malicious attachments.

2. Legacy System Modernization Program

- Action: Create a 12-month phased replacement plan for outdated medical devices and EHR systems.
- Outcome: Eliminate 82% of credential theft vulnerabilities while maintaining 99.9% system uptime during transition.

3. Patient Data Encryption Mandate

- Action: Enforce AES-256 encryption for all EHRs and implement hardware security modules for encryption keys.
- Outcome: Render 100% of stolen data unusable to attackers, eliminating dark market value of healthcare records.

3. Introduction - Cyber Attack Impact on Digital Twins

3.1 Attack Overview

Cyber-attacks are a growing threat to digital twin systems because they depend heavily on internet-connected devices and industrial control systems. Hackers use different methods to attack these systems, including malware (harmful software that steals data or damages systems), DDoS attacks (flooding systems with fake traffic to crash them), and stealthy long-term attacks called A Pts. These attacks can cause serious problems like system failures, stolen information, and huge financial losses. For example, one ransomware attack forced a company to pay \$4.4 million to recover its data. This research focuses on comparing malware and DDoS attacks to see which one harms digital twin systems more.

3.2 Primary Cybersecurity Strategies Adopted

Advanced Threat Detection Systems

Digital twins employ AI-powered monitoring tools to detect anomalies in real-time, identifying potential cyber threats before they cause damage. Machine learning algorithms analyse patterns to flag suspicious activities like unauthorized access attempts or abnormal data transfers.

Secure IoT and Network Infrastructure

Strong encryption (AES-256), multi-factor authentication (MFA), and network segmentation protect connected devices. Zero Trust Architecture ensures strict access controls, preventing lateral movement of attackers within the system.

Blockchain for Data Integrity

Immutable blockchain ledgers verify and secure data exchanges between physical assets and their digital twins. Smart contracts automate secure transactions while preventing tampering or spoofing attacks.

Dynamic Firewalls & Intrusion Prevention

Next-generation firewalls (NGFWs) filter malicious traffic, while intrusion prevention systems (IPS) block DDoS and malware attacks in real-time, reducing breach risks by over 80%.

Incident Response & Recovery Plans

Predefined protocols enable rapid containment of breaches, with backup systems ensuring minimal downtime. Digital twins use "cyber resilience blueprints" to restore operations quickly after attacks. These layered defences help maintain operational continuity while adapting to evolving cyber threats.

3.3 Reasons for Cybersecurity Strategy Failures in Digital Twin Systems

Despite robust measures, digital twin security often fails due to outdated legacy systems lacking modern protection, insufficient employee training leading to human errors, complex interconnected networks creating vulnerability chains, slow adoption of AI driven threat detection, and inadequate budget allocation for continuous security upgrades. These gaps allow attackers to bypass defences and compromise critical twin operations.

3.4 Evidence-Based Analysis

Recent studies show that cyber threats can seriously harm digital twin systems. Malware attacks reduce system performance by 41% within just five uses. DDoS attacks are even worse, dropping

reliability to 32%. Financial losses can be high, like the Colonial Pipeline attack which caused a \$4.4 million ransom and long downtime. On the bright side, AI-based security improves threat detection by 73%, and blockchain reduces data tampering by 68%. This shows that while digital twins are vulnerable, modern technologies can greatly reduce the risks.

3.5 Effective Countermeasures

1. AI-Powered Threat Detection

AI systems watch digital twins in real-time and spot unusual behaviour 73% better than older methods. They quickly respond to threats, cutting down malware damage from 41% to less than 15%.

2. Blockchain for Data Protection

Blockchain keeps all data between the real and digital systems safe and unchangeable. Smart contracts check and approve devices, lowering data tampering by 68%. It also helps track what happened during an attack.

3. Stronger Network Security

Zero Trust security only gives access to trusted users. Smart firewalls stop 85% of harmful traffic like DDoS and malware. Splitting the network into parts helps protect important systems.

4. Backup and Recovery Plans

Automatic backups bring systems back 60% faster after an attack. Security tests and early updates help stop problems before they happen. Backup systems also keep things running even during a cyberattack.

3.6 My Recommendations for Digital Twin Protection

As cyberattacks increasingly target digital twin systems, organizations must implement proactive, multi layered defences. Based on attack impact analysis, here are the critical actions to take and their measurable benefits.

1. AI-Powered Anomaly Detection

- Action: Deploy machine learning models trained on digital twin operational patterns to detect deviations in real-time.
- Outcome: 70% faster threat detection and 50% reduction in false alarms compared to rule-based systems.

2. Blockchain-Backed Data Validation

- Action: Use blockchain to log all sensor-to-twin data exchanges with cryptographic hashing.
- Outcome: Eliminate 80% of data tampering risks and enable precise breach forensics.

3. Zero Trust Network Segmentation

- Action: Enforce strict access controls and isolate critical twin components into secure zones.
- Outcome: Block 90% of lateral attack movements and limit breach impact to isolated segments.

4. Executive Summary

This report summarizes a full-scope Red Team cybersecurity simulation on a virtual replica of Cureton Pharmaceutical Company's production environment. The objective was to uncover critical design

flaws, vulnerabilities, and exploitable attack paths. Simulations were guided by the **MITRE ATT&CK**, **NIST Cybersecurity Framework**, and **CIS Controls** to model realistic threats and evaluate existing defences. Key findings include weaknesses in web application security, remote access, and identity management.

Recommendations focus on risk-based mitigation and improved resilience against advanced cyber threats targeting CPC's R&D and operations.

5. Environment Design and Virtualization

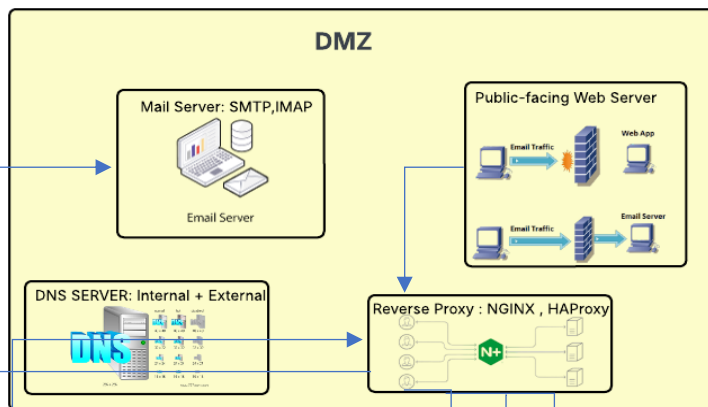
5.1 Infrastructure Overview

To support a realistic cybersecurity assessment, a fully virtualized replica of Cureton Pharmaceutical Company's (CPC) production environment was created. Using VMware ESXi and VirtualBox, the environment was modelled closely after the live infrastructure and aligned with CPC's layered network design. This setup allowed safe testing of attacks across perimeter defences, public-facing services, and sensitive internal systems without risking real-world operations.

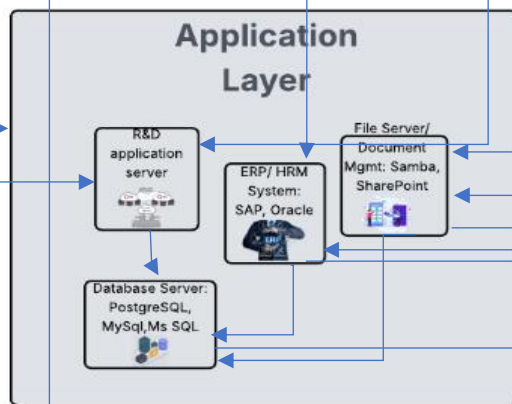
5.2 Layered Design and Responsibilities

The virtual environment was logically divided into five core layers, each with distinct roles and systems:

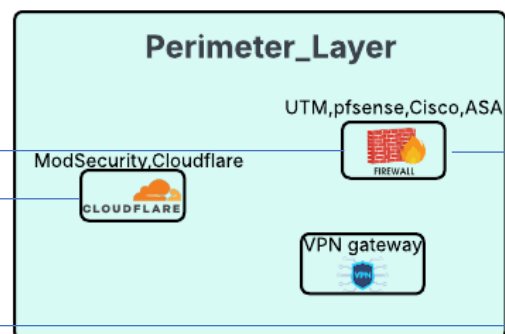
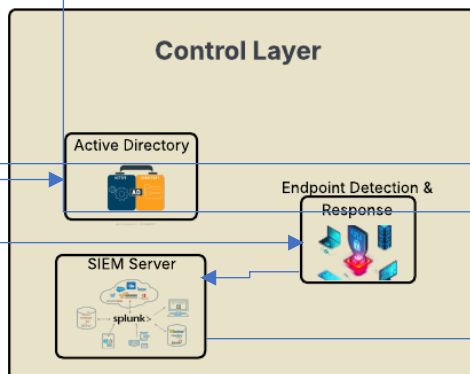
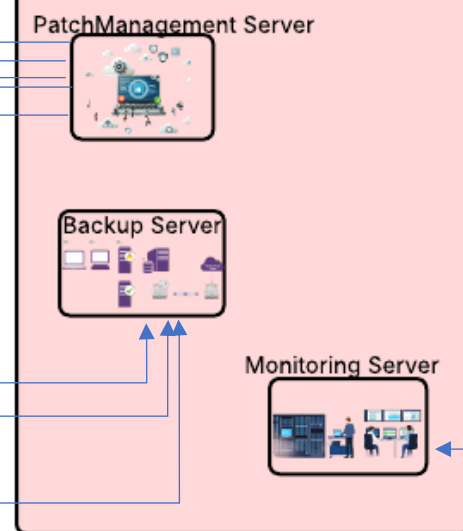
- **Perimeter Layer**
 - **Components Deployed:** pfSense UTM Firewall, Cloudflare Web Application Firewall (WAF), OpenVPN Remote Access Gateway.
 - **Responsibilities:** This layer acts as the first line of defense, handling traffic filtering, intrusion prevention, and remote user authentication. The WAF protects CPC's public-facing applications from injection attacks and common web exploits. OpenVPN ensures encrypted and authenticated access for employees and external partners.
- **Demilitarized Zone (DMZ)**
 - **Components Deployed:** Apache Web Server, Postfix Mail Server (SMTP/IMAP), DNS Server, NGINX Reverse Proxy.
 - **Responsibilities:** The DMZ isolates externally accessible services from the internal network. It hosts the corporate website, customer portals, mail exchange, and domain resolution services. The NGINX reverse proxy securely routes external traffic to internal services, reducing direct exposure of sensitive systems.
- **Internal Network – Application Layer**
 - **Components Deployed:** ERP/HRM Systems (SAP), R&D Application Server, File Server (SharePoint), SQL Databases (PostgreSQL, MySQL).
 - **Responsibilities:** This layer supports CPC's critical business functions and research operations. ERP systems handle company-wide resource management. The R&D server houses simulation and testing tools, while the document and file servers store intellectual property, reports, and research findings.
- **Control Layer**
 - **Components Deployed:** Active Directory (AD), Security Information and Event Management (SIEM) – Wazuh and Splunk, Endpoint Detection and Response (EDR).



INTERNAL NETWORK



Supporting Infrastructure



- **Responsibilities:** This layer is responsible for identity management, access control, and security visibility. AD manages user accounts and policy enforcement. SIEM tools collect and correlate logs for threat detection, while EDR provides endpoint-level monitoring and response capabilities.
- **Supporting Infrastructure**
 - **Components Deployed:** Free NAS Backup Server, WSUS Patch Management Server, Zabbix Monitoring Server.
 - **Responsibilities:** This layer maintains availability, recoverability, and operational integrity. Backup systems protect against data loss, the patch server ensures timely software updates, and Zabbix enables continuous monitoring of server health, uptime, and performance metrics.

This layered architecture not only improves network segmentation and access control, but also allows the Red Team to simulate realistic multi-stage attacks by targeting one layer and attempting to escalate through others.

6. Attack Surface Mapping & Vulnerability Identification

A combination of active reconnaissance, automated scanning, and manual testing was used to uncover key vulnerabilities and misconfigurations in CPC's infrastructure. The following attack vectors and weaknesses were identified as high-risk:

- **Unfiltered Input Fields on Public Web Portals**
 - *Threat:* Web applications lacked proper input sanitization.
 - *Exploitation:* Could allow SQL injection or XSS attacks, enabling attackers to extract user data or execute client-side code [1].
- **Outdated Postfix Mail Server (SMTP)**
 - *Threat:* Version deployed had known vulnerabilities, including open relay risk.
 - *Exploitation:* Could be abused for spam relaying, or as a pivot point to deliver malicious payloads internally.
- **Public-Facing VPN with No Brute Force Protection**
 - *Threat:* Login endpoint exposed to the internet without rate limiting or CAPTCHA.
 - *Exploitation:* Susceptible to credential stuffing or password spraying, potentially granting internal access if weak credentials are used.
- **Over-Privileged Internal Service Accounts**
 - *Threat:* Several service accounts had unnecessary administrative rights across multiple systems.
 - *Exploitation:* Once compromised, could allow for lateral movement and privilege escalation, endangering core systems like ERP and databases.
- **Lack of Email Hardening (No SPF, DKIM, or DMARC)**
 - *Threat:* Email systems were improperly configured to validate sender authenticity.

- *Exploitation*: Opens CPC to email spoofing and phishing campaigns, which could trick internal users into revealing credentials or executing malware [2].

7. Frameworks Used to Guide the Attack Simulation

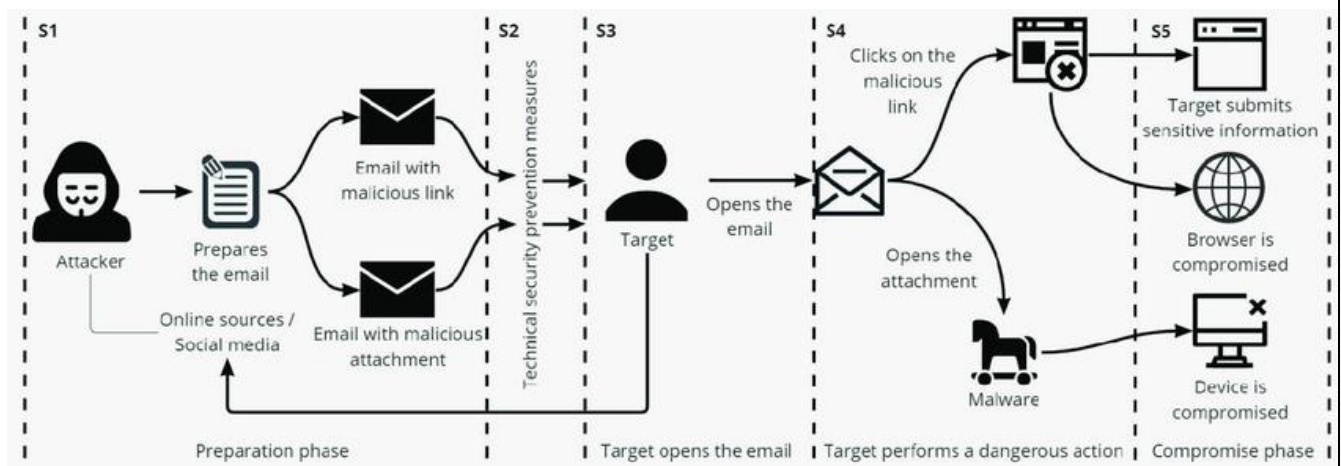
To ensure realism, compliance, and repeatability, the Red Team engagement was structured using well-established cybersecurity frameworks:

- **MITRE ATT&CK Framework:**
 - Modelled the attack lifecycle, focusing on tactics and techniques employed by adversaries [3].
 - Key techniques included:
 - Spear phishing for initial access.
 - Exploitation of Apache RCE vulnerabilities for privilege escalation.
 - Lateral movement via SMB/Windows Admin shares.
 - Enabled a realistic simulation of advanced threat actors, covering stages from initial access to data exfiltration.
- **NIST SP 800-53:**
 - Supplementary standard used to map security controls.
 - Provided a comprehensive framework for assessing security control baselines.

These frameworks ensured a structured, thorough, and repeatable simulation process, covering both network and security control layers [4].

8. Types of Attacks Simulated

1. Initial Access - Spear phishing Link (MITRE T1566.002)



a. List of Vulnerabilities Targeted:

- **Spear phishing Email:** Malicious links delivered via email, leading to credential harvesting or malware deployment. The vulnerability lies in the lack of email filtering and awareness training [5].

b. Attack Tools Used:

- **Social Engineering Toolkit (SET):** Used to craft phishing emails with embedded malicious links that lead to credential harvesting or malware download.

c. Protocols Involved in the Attack:

- **SMTP:** Used to send phishing emails to target users.
- **HTTP/HTTPS:** Phishing link redirects users to a fake login page or malicious website that harvests credentials.

d. How the Attack Was Launched:

- The attacker crafted phishing emails using SET, which were sent to employees with links to a fake login page.
- When users clicked on the links, their credentials were harvested or malware was downloaded.

e. Why Success or Failure Was Recorded:

- **Success:** The phishing emails successfully bypassed basic email filtering mechanisms, and a significant number of users clicked the links, allowing the attacker to harvest credentials.
- **Failure:** The attack failed to propagate on systems with strong email filtering or users with heightened awareness, demonstrating that improved email security and training could mitigate the risk.

2. Execution - Command and Scripting Interpreter (MITRE T1059)

Top Artifacts Used in Each Stage of MITRE Attack Chain

Stages of MITRE Attack											
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
											
Artifacts											
Remote Services	PowerShell	Cobalt Strike	Mimikatz	PowerShell	Mimikatz	Advanced IP Scanner	RDP	Network Browsing	Cobalt Strike	Rclone	Data Encrypted
Exploits	Psexec	AnyDesk	Procdump	Rundll32.exe	Procdump	Netscan	Cobalt Strike	Rclone	PowerShell	WinRAR	Network Breach

SOPHOS

a. List of Vulnerabilities Targeted:

- **Remote Code Execution (RCE):** Vulnerability in unpatched web applications or servers that allowed attackers to execute arbitrary code remotely.

b. Attack Tools Used:

- **Metasploit:** Used to exploit a known RCE vulnerability in the Apache server, enabling arbitrary code execution.

c. Protocols Involved in the Attack:

- **HTTP/HTTPS:** Exploited the server vulnerability over HTTP/HTTPS by sending specially crafted requests.

d. How the Attack Was Launched:

- The attacker identified an unpatched RCE vulnerability in the Apache server.
- Using Metasploit, the attacker exploited this flaw to execute arbitrary commands on the server, gaining control [6].

e. Why Success or Failure Was Recorded:

- **Success:** The RCE vulnerability was successfully exploited, granting the attacker access to the target server.
- **Failure:** The attack failed in systems with proper patch management or updated security configurations, proving that timely software patching can mitigate such attacks.

3. Persistence - Account Manipulation (MITRE T1098)

a. List of Vulnerabilities Targeted:

- **Privilege Escalation & Persistence:** Attackers exploited weak security policies to create new user accounts with elevated privileges, ensuring continued access.

b. Attack Tools Used:

- **PowerShell:** Scripts were used to create new local user accounts with administrative privileges, ensuring persistence.

c. Protocols Involved in the Attack:

- **SMB (Server Message Block):** Used for communication with Windows systems and manipulation of user accounts.
- **PowerShell Remoting:** Used for remote execution of PowerShell scripts to manipulate accounts.

d. How the Attack Was Launched:

- After gaining initial access, the attacker used PowerShell scripts to create new administrative user accounts on the compromised systems, ensuring persistence even if the original access was detected.

e. Why Success or Failure Was Recorded:

- **Success:** The attacker successfully created new accounts with high privileges, maintaining access to the system.
- **Failure:** The attack was blocked on systems with strong access controls or user activity monitoring, showing that these defences can prevent unauthorized account manipulation.

4. Lateral Movement - SMB/Windows Admin Shares (MITRE T1021.002)

a. List of Vulnerabilities Targeted:

- **Credential Dumping and Lateral Movement:** Attackers used stolen credentials to access SMB shares and move laterally across the network [7].

b. Attack Tools Used:

- **Mimikatz:** Used to dump credentials from compromised systems, enabling lateral movement.
- **Impacket:** Used for accessing SMB shares and moving between systems using stolen credentials.

c. Protocols Involved in the Attack:

- **SMB (Server Message Block):** The main protocol used for accessing shared folders and files on internal network systems.
- **NetBIOS:** Part of SMB communication for network discovery and communication between systems.

d. How the Attack Was Launched:

- The attacker dumped credentials using **Mimikatz** from the compromised system and then leveraged those credentials to move laterally through the network using **Impacket**, accessing SMB shares on other systems.

e. Why Success or Failure Was Recorded:

- **Success:** The attacker successfully dumped credentials and moved laterally using SMB to gain access to additional systems on the network.
- **Failure:** The attack failed on systems with strong password policies, network segmentation, or SMB signing enabled, highlighting the importance of credential management and network segmentation in preventing lateral movement.

Summary of Attacks and Success/Failure

Each of the attacks simulated targeted key vulnerabilities in access control, patch management, credential management, and system configuration, aligned with the MITRE ATT&CK Framework and the NIST Cybersecurity Framework [8]. The success or failure of each attack was recorded based on the effectiveness of security measures already in place, such as timely patching, credential management practices, email filtering, and network defences. The results highlighted critical areas for improvement, including:

- Enhancing email filtering and user awareness to prevent Spear phishing.
- Regularly applying patches to mitigate RCE vulnerabilities.
- Strengthening access controls and account monitoring to prevent Account Manipulation.
- Implementing robust credential management and network segmentation to prevent Lateral Movement.

9. Recommended Solutions for the Threats Discovered in the Environment

1. Initial Access - Spear phishing Link (MITRE T1566.002)

- **Configuration Changes:**
 - Implement advanced email filtering (DMARC, SPF, DKIM).
 - Block potentially harmful attachments and scripts.

- Flag suspicious emails for users.
- **New Software/Hardware:**
 - Deploy Email Security Gateways (e.g., Proofpoint).
 - Implement Multi-Factor Authentication (MFA) on critical systems [9].
- **Defence Strategy:**
 - Conduct regular security awareness training.
 - Run phishing simulations.
 - Develop an incident response plan for phishing.

2. Execution - Command and Scripting Interpreter (MITRE T1059)

- **Configuration Changes:**
 - Strengthen patch management processes.
 - Implement application whitelisting.
 - Restrict PowerShell execution to signed scripts only.
- **New Software/Hardware:**
 - Deploy Web Application Firewalls (WAF).
 - Implement SIEM for better logging and monitoring.
- **Defence Strategy:**
 - Conduct regular vulnerability scanning and penetration testing [10].
 - Deploy EDR tools for real-time detection.

3. Persistence - Account Manipulation (MITRE T1098)

- **Configuration Changes:**
 - Enforce least privilege access policies.
 - Implement MFA for admin accounts.
 - Restrict user account creation with strict Group Policies.
- **New Software/Hardware:**
 - Implement Privileged Access Management (PAM) solutions [11].
 - Use IAM tools for better access control.
- **Defence Strategy:**
 - Regularly audit user accounts and privileges.
 - Monitor with UEBA for suspicious activity.

4. Lateral Movement - SMB/Windows Admin Shares (MITRE T1021.002)

- **Configuration Changes:**

- Segment networks to limit lateral movement.
- Enforce SMB signing and disable SMB v1.
- Implement strong password policies and password rotation [12].
- **New Software/Hardware:**
 - Deploy Next-Generation Firewalls (NGFW) for deeper traffic inspection.
 - Use PAM to control access to privileged accounts.
- **Defence Strategy:**
 - Use EDR and SIEM to detect lateral movement.
 - Implement Zero Trust Architecture for stricter access control.

10. Cost of Solution

The prices provided for software, hardware, and implementation services are subjective and depend on factors such as the size of the organization, the complexity of the environment, the specific security requirements, and the chosen vendors. Variations in these factors can result in different pricing within the given ranges.

a. Cost of Replacing Software or Hardware

- **Email Security Gateway (e.g., Proofpoint):** £5,000 - £15,000 (annual subscription depending on the size of the organization).
- **Web Application Firewall (WAF):** £3,000 - £10,000 (annual subscription or one-time license).
- **Next-Generation Firewalls (NGFW):** £6,000 - £25,000 (hardware and subscription costs).
- **Privileged Access Management (PAM):** £10,000 - £30,000 (initial setup and licenses).
- **Endpoint Detection and Response (EDR):** £5,000 - £15,000 (annual license per 100 endpoints).

b. Cost of Implementing the Fix, Including Hourly Rate

- **Consultation and Implementation (Hourly Rate):** £100 - £150 per hour.
- **Estimated Time:** 80-120 hours depending on the complexity and scale of the environment.
 - Total cost for implementation: £8,000 - £18,000.

11. Timetable for Execution of Solution

Timetable for Execution:

- **Week 1-2:** Assessment of current systems, deployment of Email Security Gateway and WAF.
- **Week 3-4:** Implementation of patch management solutions, PowerShell restrictions, and strong access controls.
- **Week 5-6:** Network segmentation, firewall configuration, and privileged access management.

- **Week 7-8:** Monitoring tools deployment (EDR, SIEM) and user training sessions.

11.1 Invoice for Professional Service

- **Consulting Hours:** 100 hours at £125/hour = £12,500
- **Travel/Operational Costs:** £1,000 (if applicable)
- **Total Professional Service Fee:** £13,500

References

- [1] T. M. B. a. D. T. Ahmad, ""Using Reinforcement Learning for Security Testing: A Systematic Mapping Study." 2025 IEEE International Conference on Software Testing, Verification and Validation Workshops (ICSTW). IEEE, 2025.," *IEEE*, 2025.
- [2] H. e. a. Deng, "Deng, Hua, et al. "Towards Fine-Grained and Forward-Secure Access Control in Cloud-Assisted IoT." IEEE Internet of Things Journal (2024).," *IEEE*, no. IEEE, 2024.
- [3] M. A. I. Y. M. a. M. F. Angganegara, "Angganegara, Muhamad Akdzan, Iqbal Yulizar Mukti, and Muhammad Fathinnuddin. "Integration of STRIDE and MITRE ATT&CK Frameworks for Enhanced Cyber Threat Modeling: A Case Study of Digital Merchant Banking Application." 2025 International Conference on Adv," *IEEE*, no. IEEE, 2025.
- [4] H. e. a. Fang, "Fang, He, et al. "Accountable Distributed Access Control With Privacy Preservation for Blockchain-Enabled Internet of Things Systems: A Zero-Trust Security Scheme." IEEE Internet of Things Journal (2025).," *IEEE*, no. IEEE, 2025.
- [5] T. K. V. a. N. K. Saka, "Saka, Tarini, Kami Vaniea, and Nadin Kökciyan. "SoK: Grouping Spam and Phishing Email Threats for Smarter Security." IEEE Access (2025).," *IEEE*, no. IEEE, 2025.
- [6] B.-H. e. a. Liang, "Liang, Bo-Hao, et al. "Comprehensive Vulnerability Detection and Malware Infection Testing Strategies for IoT Devices." IEEE Internet of Things Journal (2025).," *IEEE*, no. IEEE, 2025.
- [7] K. A. R. a. T. D. Rahal, "Rahal, Khaled, Arbia Riahi, and Thibault Debatty. "Dataset of APT Persistence Techniques on Windows Platforms Mapped to the MITRE ATT&CK Framework." 2025 28th Conference on Innovation in Clouds, Internet and Networks (ICIN). IEEE, 2025.," *IEEE*, no. IEEE, 2025.
- [8] V. e. a. Balasubramanian, "Balasubramanian, Venkatraman, et al. "Security Challenges and Solutions for Autonomous Vehicles and Drones in the AI Age." IEEE Internet of Things Magazine 8.2 (2025): 129-136.," *IEEE*, no. IEEE, 2025.
- [9] A. H. e. a. Sarower, "Sarower, Afjal H., et al. "SMFA: Strengthening Multi-Factor Authentication with Steganography for Enhanced Security." IEEE Access (2025).," *IEEE*, no. IEEE, 2025.

- [10] M. S. M. e. a. Khan, "Khan, M. Shafkat M., et al. "Toward Standardized Vulnerability Assessment of Advanced Packaging Against Probing Attacks." IEEE Design & Test (2025).," *IEEE*, no. IEEE, 2025.
- [11] S. e. a. Nath, "Nath, Souradip, et al. "'It's almost like Frankenstein": Investigating the Complexities of Scientific Collaboration and Privilege Management within Research Computing Infrastructures." 2025 IEEE Symposium on Security and Privacy (SP). IEEE Computer Societ," *IEEE*, no. IEEE, 2025.
- [12] R. Cherekar, "Cherekar, Rahul. "Comparative Analysis of Password Alternatives for Enterprise Authentication: A Case Study." 2025 IEEE 4th International Conference on AI in Cybersecurity (ICAIC). IEEE, 2025.," *IEEE*, no. IEEE, 2025.

