Nottingham Trent University

Department Of Computer Science

COMP40751: Information & Comp Security 202425 Half Year 1

COMP40751 – Coursework 1

Karunakar Reddy Machupalli - N1334679

Abstract

An extensive cyber security case study of Azaak, an established international shipping company, is presented in this coursework. The study's main objectives are to examine Azaak's network and data architecture, find potential vulnerabilities and exploits, and carry out a comprehensive risk assessment. A ransomware attack recently exposed serious security flaws in the corporation, which runs internationally networked IT infrastructure with data centres spread across several locations. This paper offers comprehensive suggestions for improving Azaak's cyber security posture, encompassing managerial, procedural, legal, social, and technical methods. The suggested remedies seek to reduce risks, safeguard data assets, and guarantee Azaak's worldwide network infrastructure's resistance to upcoming cyberattacks. The conclusions and suggestions are backed up by well-considered hypotheses and more investigation, guaranteeing a strong and useful strategy for managing cyber security.

Table of Contents

Cyber Security Case Study Report

1.1 Introduction

Azaak, a leading global shipping and logistics company based in London, employs around 40,000 people across 75 countries and facilitates approximately 90% of global maritime trade. In June 2024, Azaak experienced a severe ransomware attack that crippled access to critical data, exposing significant IT infrastructure vulnerabilities. This incident underscored the urgent need for robust cybersecurity protocols to enhance data security and ensure operational continuity. The attack disrupted internal operations and jeopardised external partnerships and the supply chain. This report evaluates Azaak's network infrastructure, focusing on vulnerability identification, risk assessment, and targeted recommendations. It aims to enhance security by addressing IT weaknesses, evaluating potential risks, and proposing advanced security measures and employee training to safeguard critical logistics and shipping operations.

Table:1 Distribution of data centres

Continent	Country	Connection	City
North America	USA	Fiber Optic	New York
North America	USA	Fiber Optic	Seattle
Europe	UK	Fiber Optic	London
Europe	Germany	Fiber Optic	Frankfurt
Asia	Singapore	Fiber Optic	Singapore
Australia	Australia	Fiber Optic	Sydney

Based on the insights from the above table, the data centres are strategically distributed across the globe, with locations in North America, Europe, Asia, and Australia. This smart placement ensures that they are well-connected through high-speed fiber optic cables, facilitating rapid communication between them. The global presence of these data centres significantly reduces latency, providing a seamless and efficient experience. This setup not only enhances connectivity but also ensures robust and reliable data management across different regions, supporting Azaak's complex logistics and shipment operations effectively.

1.2 Methodology

Diagram: 1 Methodology for the case study

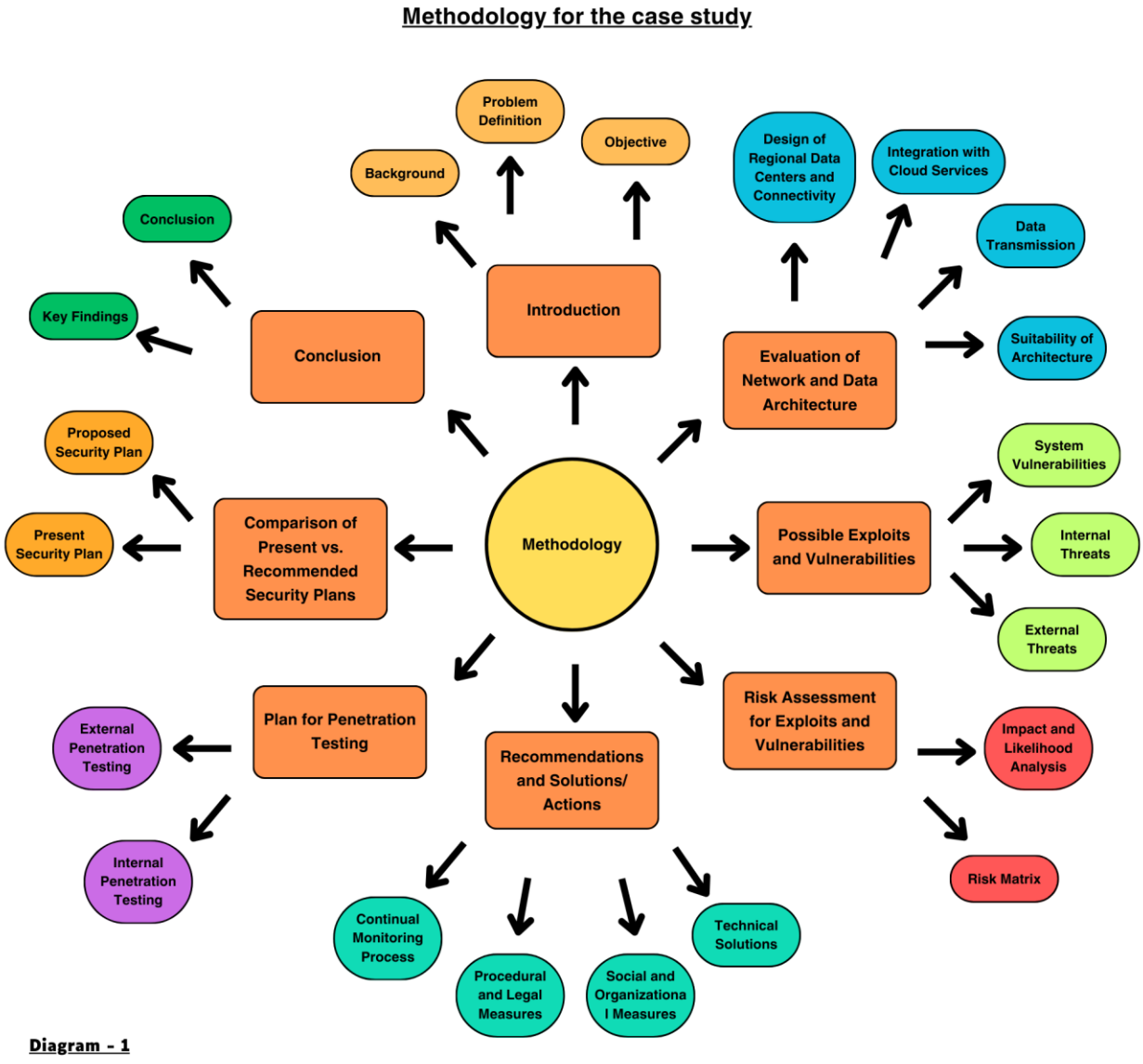
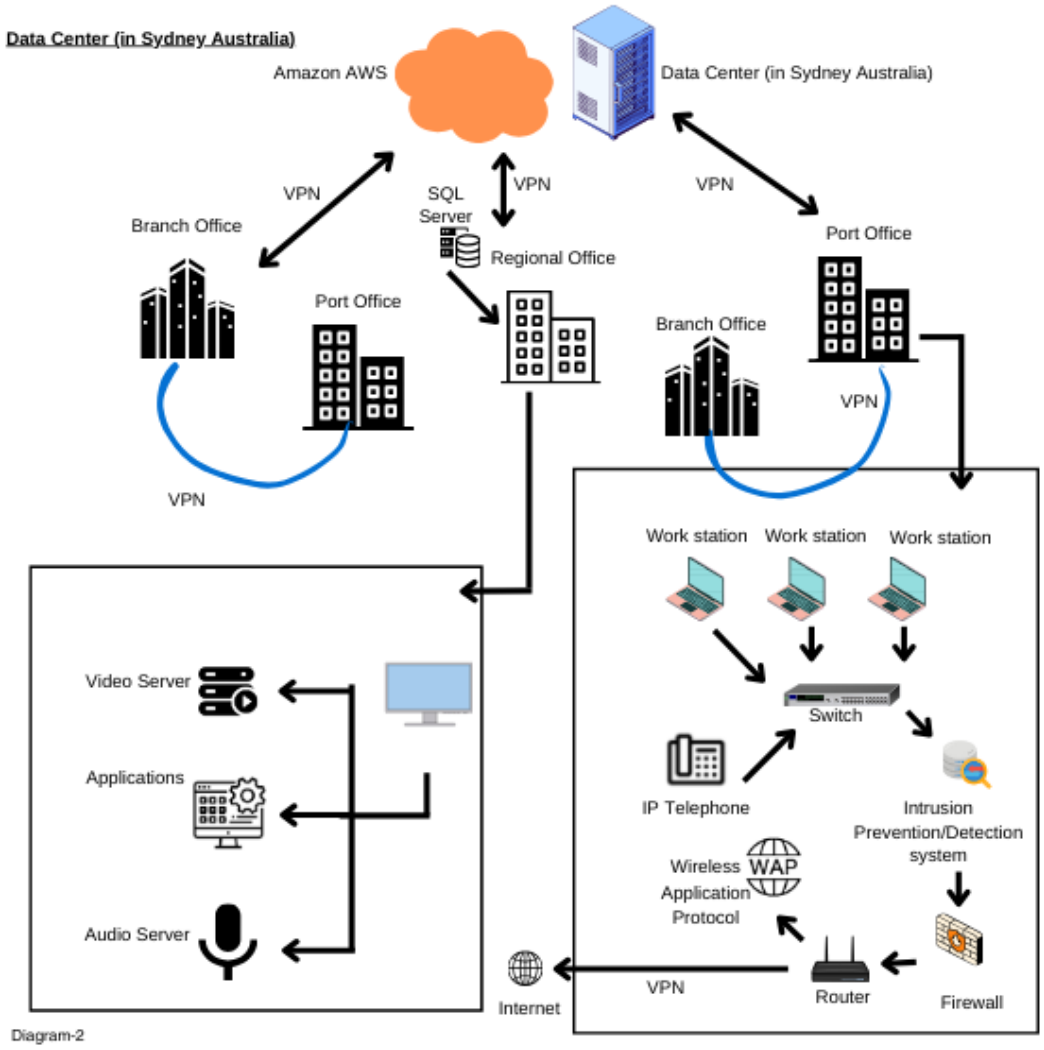


Diagram – 1

1.3 Evaluation of Network and Data Architecture

1.3.1 Design of Regional Data Centers and Connectivity

Diagram:2 Data centre in Sydney Australia



The network diagram illustrates an IT system, with a Data Centre in Sydney, Australia, as the central hub linking regional, branch, and port offices. This Data Centre is connected to Amazon AWS via a secure VPN (Cisco RV340W VPN Router), providing access to cloud-based resources such as the SQL server. The Regional Office is directly connected to both the Data Centre and Amazon AWS through VPN, acting as an

intermediary for several branch and port offices. Each branch and port office has a secure VPN connection, either connecting directly to the Data Centre or routing through other offices, ensuring network flexibility.

The Port Office's internal network includes a video server, an audio server, and various applications for multimedia and operational support. For enhanced connectivity, a switch (Cisco SG350 Switch) and Router (Cisco RV Series Router) connects a Wireless Access Point (WAP) and IP phone system to multiple workstations. Firewalls filter incoming and outgoing traffic, while an Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) monitor and mitigate threats. A router connects the network to global networks, with VPNs ensuring secure access to other networks. Strong security protocols are implemented to protect data and maintain operational continuity across the networked offices.

1.3.2 Integration with Cloud Services

To address scaling requirements, Azaak incorporates public cloud platforms like Amazon AWS and Microsoft Azure alongside its regional data centres. These cloud services enable the expansion of applications critical to operations, such as container tracking and booking systems. While this hybrid model improves scalability, it also brings about new challenges, including the need to ensure secure data transmission between on-premises infrastructure and cloud environments.

1.3.3 Data Transmission

Secure data transmission between the Sydney Data Centre and networked offices is essential for operational efficiency. Virtual Private Network (VPN) connections, secured by **AES-256** encryption, ensure encrypted communication, prevent unauthorised access and safeguarding internal operations and cloud resource usage. Amazon AWS integration enhances remote data processing and storage, enabling real-time access across locations.

High-bandwidth fibre-optic Ethernet connections, supporting speeds of 1 GB and 10 GB, ensure reliable, low-latency data transfers, essential for handling large volumes of information efficiently. Transferring data from port offices to the AWS cloud further reduces risks of data loss or corruption by leveraging AWS's robust security, dependable storage, and disaster recovery capabilities.

The use of Virtual Local Area Networks (VLANs) improves network security by segmenting data traffic logically, ensuring that different types of traffic remain isolated. This configuration enhances overall system security and operational resilience.

1.3.4 Suitability of Architecture

This structure positions the Data Centre as a central hub for data access, security, and management. Integrating AWS cloud services enhances scalability and latency for data storage and applications. Despite its functionality, the architecture faces security challenges due to its complexity and multiple entry points. Direct VPN connections from branch and port offices increase the attack surface, heightening risk. Existing security measures, including a firewall, Intrusion Detection System (IDS), and Intrusion Prevention System (IPS), provide basic protection. However, advanced security upgrades would help mitigate the growing cybersecurity threats, further securing sensitive data and fortifying infrastructure resilience.

1.4 Possible Exploits and Vulnerabilities

1.4.1 System Vulnerabilities

Azaak's reliance on outdated software and hardware exposes its IT infrastructure to a wide array of system vulnerabilities. All employee devices operate on Microsoft Windows 7, an operating system that reached its end-of-life (EOL) on January 14, 2020, with no access to Extended Security Updates (ESU). This makes the company susceptible to recently discovered high-risk exploits, such as CVE-2021-40465, CVE-2021-40441, CVE-2022-41128 and CVE-2022-41125, which allow attackers to use Windows Text Shaping Remote Code Execution Vulnerability, CVE-2021-40441 vulnerability allows attackers to elevate privileges on the affected systems. Network devices, including the Cisco SG350 Series Managed Switches and Cisco RV Series Small Business Routers. Specifically, the models RV016, RV042, RV042G, and RV082 have been identified with critical vulnerabilities such as CVE-2023-20025 and CVE-2023-20026, operate with outdated firmware and lack proper security configurations, making them vulnerable to exploitation. These gaps highlight the pressing need to update and secure system software and firmware to prevent attackers from exploiting unpatched vulnerabilities.

Table:2 Possible Exploits

Vulnerabilities	Description
CVE-2021-40465	Windows Text Shaping Remote Code Execution Vulnerability
CVE-2021-40441	Windows Media Center Elevation of Privilege Vulnerability
CVE-2022-41128	Windows Scripting Languages Remote Code Execution Vulnerability
CVE-2022-41125	Windows CNG Key Isolation Service Elevation of Privilege Vulnerability

CVE-2023-20025	Vulnerability in the web-based management interface of Cisco Business RV Series Routers
CVE-2023-20026	Attacker could exploit this vulnerability by sending a crafted request to the web-based management interface

1.4.2 Internal Threats

Inadequate devices and network security procedures increase internal vulnerabilities, putting the company at risk from careless or malicious insider threats. For example, CVE-2023-20025 allows for remote code execution due to improper user input validation on the web-based administration tool RV016, which could be used by insiders with bad intentions. Another major risk is malware infections, which can replicate and spread throughout the company network, disrupting operations and compromising sensitive data. These infections are often caused by employees visiting compromised websites or unintentionally downloading malicious attachments. Phishing emails and whaling are examples of social engineering attacks that target employees by taking advantage of their ignorance to obtain sensitive data or get around authentication measures. These internal threats are made worse by improperly configured firewalls, which give hackers access to confidential information or systems.

Table:3 Possible Internal Threats

Possible Internal Threats
Misconfigurations In Role Management
Weak Passwords
Outdated Systems
Malicious Insiders

1.4.3 External Threats

External threats to Azaak's IT infrastructure primarily stem from vulnerabilities in network hardware, misconfigurations, and exposure to sophisticated cyberattacks. The outdated Cisco RV340W VPN router is particularly concerning, as it could allow remote code execution and privilege escalation, such as CVE-2023-20025 and CVE-2023-20026, enabling attackers to compromise the web-based management interface and execute arbitrary commands. The absence of logical segmentation within the network, coupled with misconfigured firewalls, increases exposure to external attack vectors, facilitating unauthorized access to

sensitive resources. Cybercriminals targeting widely used software platforms, such as Windows 7, compound the risks by using known vulnerabilities to conduct advanced persistent threats (APTs) or ransomware attacks. The June 2024 ransomware incident underscores the dire consequences of external threats, emphasising the need for robust defence mechanisms, such as advanced and up-to-date intrusion detection and prevention systems (IDS/IPS), encryption protocols, and network segmentation, to safeguard against future external attacks.

Table:4 Possible External Threats

Possible External Attacks
Cybercriminals
Distributed Denial of Service
Hacktivists
Third-Party Attacks

1.5 Risk Assessment for Exploits and Vulnerabilities

1.5.1 Impact and Likelihood Analysis

Windows 7 End-of-Life (EOL) Vulnerability

- **Likelihood**: High
- **Impact**: Severe
- **Description**: All employee devices at Azaak operate on Microsoft Windows 7, an operating system that reached its end of life on 14 January 2020, with no access to Extended Security Updates (ESU). This exposes the company to high-risk exploits such as CVE-2021-40465, CVE-2021-40441, CVE-2022-41128, and CVE-2022-41125, which allow attackers to execute remote code and elevate privileges on affected systems.

Unpatched Cisco SG350 Series Managed Switches

- **Likelihood**: Medium
- **Impact**: High
- **Description**: These switches, operating with outdated firmware, are vulnerable to critical exploits. Attackers can leverage these vulnerabilities to disrupt network operations and gain unauthorized access to sensitive data.

Unpatched Cisco RV Series Small Business Routers

- **Likelihood**: Medium
- **Impact**: High
- **Description**: Models such as RV016, RV042, RV042G, and RV082 have been identified with critical vulnerabilities, including CVE-2023-20025, which allows for remote code execution due to improper user input validation on the web-based administration tool.

Outdated Cisco RV340W VPN Router

- **Likelihood**: Medium
- **Impact**: High
- **Description**: This router is particularly concerning due to vulnerabilities like CVE-2023-20025 and CVE-2023-20026, which allow remote code execution and privilege escalation, posing significant risks to network integrity.

Internal Threats

- **Likelihood**: High
- **Impact**: Medium to High
- **Description**: Inadequate security procedures and improperly configured firewalls increase the risk of malware infections and phishing attacks. These threats can disrupt operations and compromise sensitive data.

External Threats

- **Likelihood**: High
- **Impact**: Severe
- **Description**: Azaak's IT infrastructure faces risks from outdated hardware, misconfigurations, and advanced cyberattacks. Vulnerabilities in the Cisco RV340W VPN router and Windows 7 systems, such as CVE-2023-20025 and CVE-2023-20026, allow remote code execution and privilege escalation. The June 2024 ransomware attack underscores the need for updated security measures.

1.5.2 Risk Matrix

Table:5 Risk Matrix

Vulnerability	Likelihood	Impact	Risk Level
Windows 7 EOL	High	Severe	Critical
Unpatched Cisco SG350 Switches	Medium	High	High

Unpatched Cisco RV Series Routers	Medium	High	High
Outdated Cisco RV340W VPN Router	Medium	High	High
Internal Threats (Malware, Phishing)	High	Medium	High
External Threats	High	Severe	Critical

1.6 Recommendations and Solutions/Actions

1.6.1 Technical Solutions

Upgrading systems from Windows 7 to Windows 10 or 11 is essential for Azaak's cybersecurity. Windows 7 lacks security updates, making systems vulnerable. Windows 10 or 11 offers advanced security features and regular updates, mitigating these risks.

Network segmentation is also crucial. Dividing the network into smaller, isolated segments with dedicated security controls restricts data access and contains threats within specific segments, minimising breach impacts.

Regular firmware updates and hardware replacements are vital. Replacing outdated devices like the Cisco RV Series and Cisco SG350 with modern alternatives such as the Cisco Catalyst 9000 series and ISR 4000 routers addresses known vulnerabilities, safeguarding network devices against emerging threats and enhancing overall security.

Table:6 Solutions and Objectives

Solutions	Objectives
Replacing End of Support hardware & software	To enhance security and efficiency
Employee Training	Enhance employee skills and knowledge
Implementing network segmentation	Enhance security and performance
Implementing SOC and SIEM	Enhance detection and response capabilities
Regular Penetration Testing	Identify and address security vulnerabilities
Regular Audits	Ensure compliance and identify improvements

1.6.2 Social and Organizational Measure

Regular security training sessions for employees are essential to increase awareness of phishing and social engineering risks. These sessions should educate staff on recognising suspicious emails and links, thereby enhancing their ability to respond to potential threats. Implementing strict access control policies is also crucial. Role-based access ensures employees only access necessary data and systems, reducing the risk of unauthorised access. Additionally, mandatory multi-factor authentication (MFA) for remote access adds an extra layer of security, making it more difficult for attackers to gain access even if login credentials are compromised.

1.6.3 Procedural and Legal Measures

Enforcing regular audits and cybersecurity assessments is crucial for maintaining compliance with regulations and proactively addressing risks. These audits ensure adherence to legal requirements and industry standards, identifying potential vulnerabilities before they can be exploited. Additionally, developing a formal incident response plan with clearly defined roles and protocols is essential for rapid recovery following any attack or breach. This plan should outline specific actions to be taken by designated personnel, ensuring a coordinated and efficient response to minimise downtime and damage. These measures collectively enhance the organisation's resilience against cyber threats.

1.6.4 Continual Monitoring Process

Introducing Security Information and Event Management (SIEM) systems is essential for continuous monitoring, alerting, and logging. SIEM systems provide real-time analysis of security alerts generated by applications and network hardware, enabling the organisation to detect and respond to security incidents promptly. Additionally, regular vulnerability scanning and penetration testing are crucial for proactively identifying and resolving emerging risks. These practices help uncover potential security weaknesses before they can be exploited by attackers, ensuring that the organisation's defences remain robust and up to date. Together, these measures significantly enhance the organisation's ability to monitor and protect its network infrastructure.

1.7 Plan for Penetration Testing

1.7.1 Internal Penetration Testing

An exhaustive methodology for evaluating internal systems is essential. This involves conducting vulnerability scans on employee devices to identify security weaknesses, including operating systems, applications, and network configurations. Additionally, it is crucial to test access control mechanisms, ensuring role-based access controls are correctly implemented and multi-factor authentication (MFA) is enforced for sensitive systems and data. Monitoring insider threats by tracking unusual or suspicious activities is also essential. Furthermore, social engineering simulations, such as phishing exercises, should be conducted to assess employee resilience against real-world attacks. These simulations help identify areas needing further training. By integrating technical vulnerability assessments with social engineering tests, organisations can comprehensively understand and enhance their internal security posture.

1.7.2 External Penetration Testing

Executing external penetration testing is essential for evaluating the security of publicly accessible applications and branch offices. These tests should mimic an external attacker attempting to exploit known vulnerabilities in web applications, network services, and other publicly accessible systems. Additionally, social engineering tactics, such as phishing or pretexting, should be used to evaluate the susceptibility of branch office staff to manipulation.

Post-testing reviews are crucial. They involve documenting all findings, including discovered vulnerabilities and exploitation methods. Based on these findings, a detailed plan should be developed to implement fixes and mitigate identified risks. This process ensures vulnerabilities are promptly addressed, continuously improving the organisation's security posture.

1.8 Comparison of Present vs. Recommended Security Plans

1.8.1 Present Security Plan

The existing security protocols at Azaak demonstrate both advantages and deficiencies. One notable strength is the requirement for Virtual Private Network (VPN) connections, which ensures secure communication between regional offices and data centers. This measure helps protect data in transit from interception and eavesdropping. Additionally, the implementation of regional firewalls provides a layer of

defence by controlling incoming and outgoing network traffic based on predetermined security rules, thereby reducing the risk of external attacks.

Nonetheless, substantial deficiencies exist in the current security plan. The reliance on outdated systems, such as Windows 7, poses substantial vulnerabilities due to the lack of security updates and support from Microsoft. This leaves the systems susceptible to new threats and exploits. Furthermore, the current network architecture lacks adequate segmentation, increasing the risk of widespread compromise in the event of a breach. The absence of regular firmware updates for network devices, such as Cisco routers and switches, also exposes the infrastructure to known vulnerabilities that could be exploited by attackers.

1.8.2 Proposed Security Plan

The suggested security plan employs important measures to close important gaps. System upgrades from Windows 7 to Windows 10 or 11 guarantee the latest security patches and features, lowering the possibility of exploitation. By reducing the risk of unauthorised access, role-based access and mandatory multi-factor authentication (MFA) for remote access guarantee that only authorised personnel can access sensitive data.

Network segmentation improves overall security by limiting attackers to smaller segments. Awareness of social engineering and phishing is raised by employee security training.

Cisco ISR 4000 series routers and Cisco Catalyst 9000 series switches will be used to replace the network's antiquated hardware. Patching and updating firmware regularly will fix known vulnerabilities. Emerging risks are recognised and addressed with the introduction of Security Information and Event Management (SIEM) systems for ongoing monitoring, alerting, and routine vulnerability scanning and penetration testing.

1.9 Report and Conclusion

1.9.1 Key Findings

Table:7 Key Findings

Key Findings

System Vulnerabilities
Outdated Network Hardware
Lack of ISO Guidelines
Internal Threats
External Threats

1.9.2 Conclusion

In summary, the implementation of the proposed security measures will markedly enhance Azaak's capacity to prevent, detect, and respond to cyber threats. By systematically addressing the identified vulnerabilities and adopting a comprehensive suite of technical, social, organisational, procedural, and monitoring solutions, Azaak will significantly bolster its cybersecurity resilience. These measures will ensure the protection of critical assets and fortify the organisation against future cyber-attacks.

References

1. https://www.cve.org/CVERecord?id=CVE-2021-40465

2. https://www.cve.org/CVERecord?id=CVE-2021-40441

3.https://www.cve.org/CVERecord?id=CVE-2022-41128

4. https://www.cve.org/CVERecord?id=CVE-2022-41125

5. https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2021-40441

6. https://www.cve.org/CVERecord?id=CVE-2023-20025

7. https://www.cve.org/CVERecord?id=CVE-2023-20026

8. https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sbr042-multi-vuln-ej76Pke5

9. https://www.microsoft.com/en-us/security/business/security-101/what-is-siem