Student Name: Oluwabukunmi Olumide Fakowajo

Student ID: K2455760

Title: Information Security Assessment Report – Firm ABC

Module: CI7130 – Network and Information Security

School: Faculty of Engineering and computing Environment

Date of Submission: 13th March 2025

Executive summary

Firm ABC of about 300-500 employees recently fell victim to a cyberattack known as a watering hole attack. Attackers breached a trusted website(external) that employees of the company use frequently, using it as an opportunity to **steal credentials** and gain **unauthorized access** to **internal network**. This led to a **ransomware attack**, resulting in financial losses, operational **disruptions**, and reputational harm.

To mitigate such risks, this report outlines key security enhancements and details below:

Security Measure	Estimated cost (£/yr)	Timeline (Months)	Description	Overall Impact
VPN security	15,000-20,000	2	Strengths remote access	**lowers the likelihood of data breaches**
Multi-Factor Authentication	44,160	3	Extra login protection	**Minimizes login breaches by 70%**
Firewall	300,000	3	Blocks harmful Traffic	**Prevents network from external attacks**
Cybersecurity Training	20,000-50,000	ongoing	Trains employees to spot threats	**Lowers human error**
Threat Detection	30,000-40,000	3	Detects and responds to threats quickly	**Speeds up attack response time by 90%.**
Backup & Recovery	5,000-7,000	Bi-annual	Secures and backs-up data	**Protects data, cutting loss by 80%.**

Security Assessment Report

A team consisting of an IT security manager, network administrator, CISO and security analyst carried out the security assessment. Key IT components and infrastructure were the focus of the evaluation. The approach identified essential assets, evaluated vulnerabilities, and suggested appropriate security measures in accordance with the NIST Risk Management Framework (NIST RMF).

- **Chief Information Security Officer (CISO):** Strategic supervision and leadership.
- **Network Administrator:** Evaluation of infrastructure vulnerabilities.
- **Security Analyst:** Threat and risk analysis.
- **IT Security Manager:** Examining the user access policy.
- **Procurement Officer and Human Resources:** resource and budget management.

Security Assessment of Organization

Firm ABC was recently targeted by a watering hole attack, this section of the evaluation looks at the organization's most critical assets as well as the threats and vulnerabilities they encounter. The **NIST RMF** framework is used to identify the vulnerabilities and associate them with the appropriate security functions.
A table that classifies the assets and illustrates the relationships between threats, vulnerabilities, and mitigation techniques will be utilized to clearly display this data.

Critical Assets	Potential Threat	Vulnerabilities	NIST Function
Employee Credentials	Identity Theft, Account takeover.	Lack of **MFA** and password encryption	Identify & protect
Internal Network	Arp Poisoning, Rogue proxy servers, DNS hijacking. Lateral movements.	Lack of IDS, inadequate access control, and poor **network segmentation**	Detect & protect

Sensitive Internal Data and systems	SQL Injection, Cross-site Scripting, ransomware	Improper **input validation**, weak backup practices	Identify, protect, detect, recover
Reputation and Brand image	Social Media Exploits.	Weak recovery and response practices	Respond and recover

The **NIST RMF** was adopted to give a structured approach in identifying and addressing the different attributes of the cybersecurity risk give the recent attack. By adopting this frame work the organization aims to solidify its overall risk assessment (1).

The section below introduces tactics for protecting important resources. To provide robust security and preserve company continuity, these steps will be procured and implemented as follows, including a security architecture for implementation.

Mitigation Techniques	**Description**	**Justification of suitability**	**Technology and implementation**	**Asset(s) Protected**
Multi-Factor Authentication	Requires multiple forms for verification	makes it more difficult for hackers to use stolen credentials, lowering risk	Utilize **Azure AD** and Microsoft Auth to implement **MFA** on both internal and remote computers.	**Employee Credentials**
Firewall (Network & WAF)	Blocks malicious traffic, and unauthorized access to internal systems	Prevents web app vulnerabilities from being exploited	Set up **AWS WAF** for web apps and install **Palo Alto** firewalls across the network perimeter.	**Internal Network**
VPN Security	Data Encryption	ensures that the internal network	Set up **Palo Alto Global Protect** for remote	**Internal Network**

		is accessible securely	access with **MFA**	
Advanced Threat Detection	Monitors Endpoints for suspicious Activities	Prevents the propagation of dangerous activities and detects it early	Deploy **Crowd Strike** or **Microsoft XDR** on all endpoints for real-time monitoring	**Internal Network**
Backup & Recovery	Backing up and encryption of data at rest	Ensures protected data is always available on standby	Use **Veeam** or **Acronis** for automated backups to and **S3 buckets** for cloud storage	**Sensitive Internal Data and systems**
Security Training	Teaches employees on how to identifying and respond cyber threats	Reduces human error by making employees aware	Taking part in phishing campaigns and using platforms like **KnowBE4**	**Reputation and Brand image**

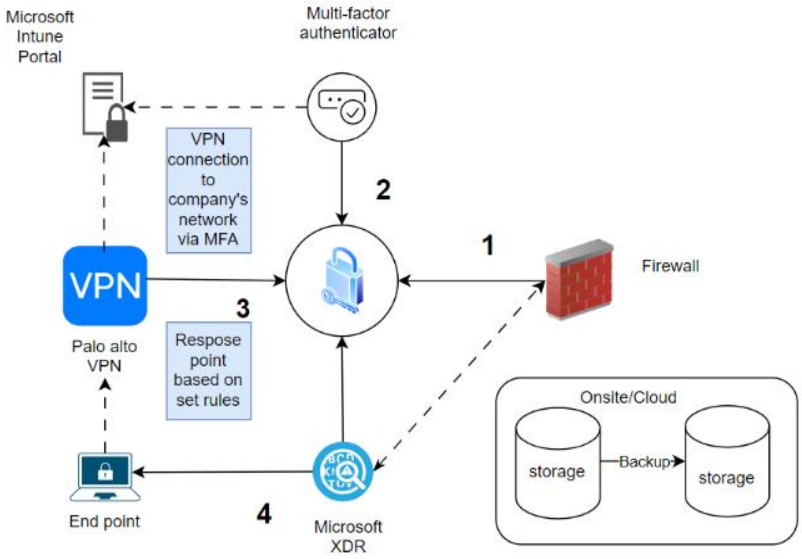

Figure 1. Security Architecture

Risk Analysis

To assess the effect of the security breach on Firm ABC's vital assets, a risk analysis was carried out by me. Since there are many parties involved and the risk is done on an Organizational-Level security, I selected **OCTAVE** over STRIDE because of its asset-focused strategy, which effectively manages the risks to vital assets. Octave offers a more extensive, qualitative analysis that guarantees a thorough and cooperative risk assessment across teams (2), in contrast to STRIDE, which concentrates on threat modeling.

- Employee Credentials **(A1)**
- Internal Network **(A2)**
- Sensitive Data and internal systems **(A3)**
- Reputation and image branding **(A4)**

Threat profile

Assets	Actor	Motive	Access	Outcome
A1	Human	Credential theft	Web interface	Impersonation
A2	Human	sabotage	Privilege escalation	Network outage
A3	Human	Extortion	Privilege escalation	Disruption
A4	Human	Defamation	Social media	Reputational loss

Risk Matrix

Risk factor	Assets	Likelihood	Impact	Risk level
Credential theft	**A1**	**High**	**High**	**High**
Unauthorized Network Access	**A2**	**Medium**	**Critical**	**Critical**
Ransomware Deployment	**A3**	**Low**	**Critical**	**Critical**

Furthermore, to effectively mitigate the identified cybersecurity threats, the following table outlines key strategies and their applications. These mitigations are designed to address specific risks, enhance security posture, and minimize the impact of potential attacks.

Risk Factor	**Mitigation**	**Application**
Credential Theft	Enable **Multi-Factor Authentication (MFA)** and enforce **strong password policies**.	Enforce password complexity, implement MFA for all users, and keep an eye out for shady login attempts.
Unauthorized Network Access	Adoption of **Zero Trust Security** and use **Network Access Control (NAC)**.	Segment networks to restrict movement, do frequent access audits, and **restrict access depending on responsibilities.**
Ransomware Deployment	**Endpoint Detection & Response (EDR)** and frequent **offline backups** are recommended.	Implement anti-malware software, automate backups, and teach staff how to spot phishing scams.

References

1. Kohnke A, Sigler K, Shoemaker D. Strategic Risk Management Using the NIST Risk Management Framework. Edpacs. 2016;53(5):1–6.

2. Caralli RA, Stevens JF, Young LR, Wilson WR. Introducing octave allegro: Improving the information security risk assessment process. Hansom AFB, MA. 2007;