TASK 1: CYBERSECURITY RISK ASSESSMENT

Risk Assessment Report

ABSTRACT

In today's interconnected digital environment, cybersecurity threats pose significant risks to organizations, including data breaches, financial losses, and reputational damage. Conducting regular cybersecurity risk assessments is crucial to identify vulnerabilities and implement effective mitigation strategies. This report presents the findings of a recent cybersecurity risk assessment conducted at Walkergenix Technologies. The objective of this assessment was to evaluate the overall security posture of the network by subjecting network systems and resources to methods and techniques commonly used by hackers and malicious actors. This process allows for the proactive remediation of any identified weakness or vulnerability before they can be exploited by a hacker to gain unauthorized access to critical systems or sensitive data.

Bryn Phoshoko
InternCareer

Cybersecurity Risk Assessment Report

Executive Summary:

This Cybersecurity Risk Assessment report presents an analysis of potential risks and vulnerabilities within Walkergenix's information technology infrastructure. The assessment was conducted to identify weaknesses in the system, evaluate the impact of potential threats, and provide recommendations for mitigation strategies. The assessment process involved a comprehensive review of current cybersecurity practices, analysis of potential threats, and evaluation of existing controls. Findings indicate several areas of concern, primarily related to outdated software, inadequate access controls, and insufficient employee training. To address these risks, several recommendations are proposed, including software updates, enhanced access controls, and regular employee training sessions.

Table of Contents:

1. Introduction:

In today's interconnected digital environment, cybersecurity threats pose significant risks to organizations, including data breaches, financial losses, and reputational damage. Conducting regular cybersecurity risk assessments is crucial to identify vulnerabilities and implement effective mitigation strategies. This report presents the findings of a recent cybersecurity risk assessment conducted at Walkergenix.

2. Scope of Assessment:

The assessment focused on evaluating the cybersecurity posture of Walkergenix's information technology infrastructure, including networks, systems, and data assets. Key areas assessed include:

- Network Security
- Endpoint Security
- Data Security
- Access Controls
- Security Policies and Procedures

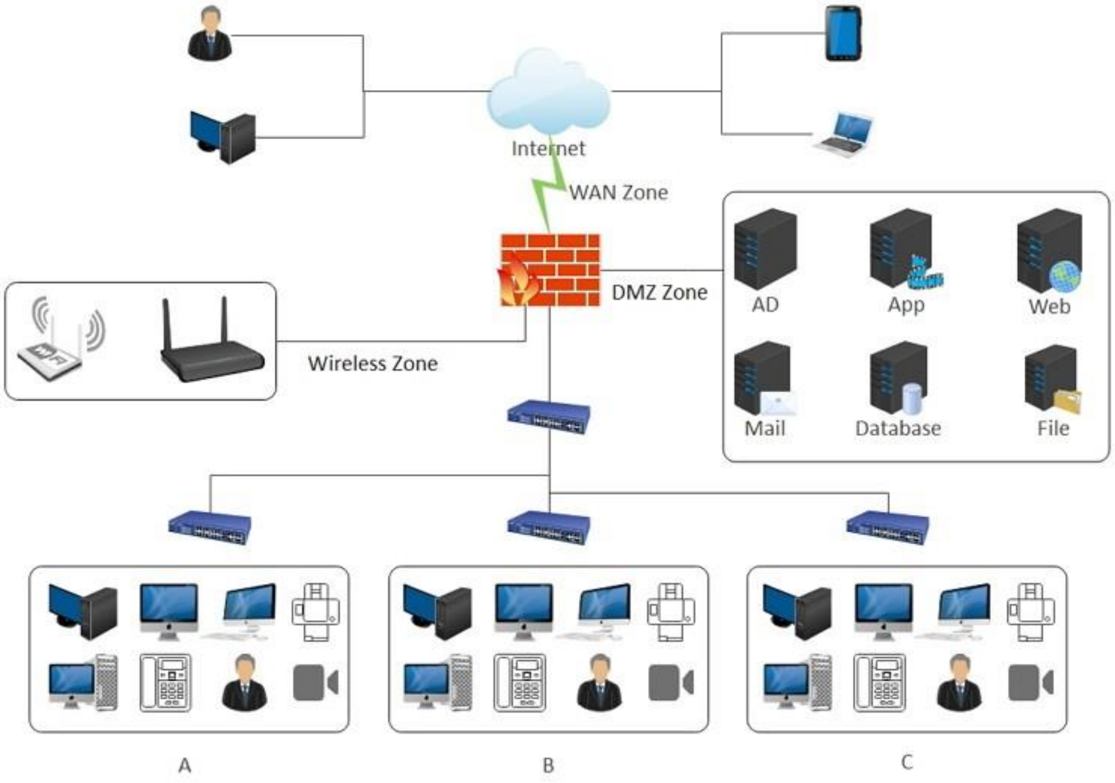

Figure 1: A sample Basic Network diagram with Sophos XG Firewall Device that we will be performing an assessment on. Source: *EdrawMax Online*

3. Assessment Methodology:

The assessment was conducted using a combination of methods, including:

- Review of existing cybersecurity policies, procedures, and documentation.
- Technical vulnerability scans using Nessus, Nmap, and Wireshark
- Interviews with key stakeholders, including IT personnel and management.
- Analysis of incident response plans and procedures.
- Examination of access controls and user permissions.

4. Findings:

Risk Rating System

Critical (16 Points)	Critical severity ranking requires immediate action through mitigating controls, direct remediation, or a combination thereof. Exploitation of discovered critical severity vulnerabilities not only results in privileged access to the target system/application and/or sensitive data but also allows access to other hosts or data stores within the environment.
High (8 Points)	A finding denoted with a high severity ranking suggests that this observation requires immediate evaluation and subsequent resolution. Exploitation of high severity vulnerabilities discovered in the environment can lead directly to an attacker gaining privileged access (e.g. administrator, root, SA, etc.) to the system/application and/or sensitive data.
Medium (4 Points)	A finding denoted with a medium severity ranking requires review and resolution within a short period. From a technical perspective, vulnerabilities that warrant a medium severity ranking can lead directly to an attacker gaining non-privileged access (e.g. standard user) to the system/application and/or sensitive data or cause a denial-of-service (DoS) condition on the host, service, or application.
Low (2 Points)	A finding denoted with a low severity ranking requires an evaluation for review and resolution once the remediation efforts for critical, high, and medium severity issues are complete. From a technical perspective, vulnerabilities that warrant a low severity ranking may leak information to unauthorized or anonymous users used to launch a more targeted attack against the environment.

Figure 2: A table showing risk rating system used to assess the potential impacts of the vulnerabilities in the network system.

4.1. Router

Identified Vulnerabilities:	Severity	Potential Impact

1. Weak Administrator Password	Medium	Unauthorized access to router settings, leading to potential network compromise.
2. Outdated Firmware	High	Increased susceptibility to attacks exploiting known vulnerabilities.

Description:

- The router's administrator password is weak and easily guessable.
- The router is running outdated firmware with known vulnerabilities.

4.2. Firewall

Identified Vulnerabilities:	**Severity**	**Potential Impact**
1. Firewall Misconfiguration	High	Unauthorized access to the network, compromising security.
2. Outdated Firewall Rules	Medium	Reduced effectiveness in blocking malicious traffic.

Description:

- The firewall is misconfigured, allowing unauthorized access to certain ports.
- Some firewall rules are outdated and no longer relevant.

4.3. Switch

Identified Vulnerabilities:	**Severity**	**Potential Impact**
1. Lack of Port Security	Medium	Unauthorized devices gaining access to the network through switch ports.
2. Insufficient Encryption	Medium	Increased risk of eavesdropping and data interception.

Description:

- Port security measures on the switch are not adequately configured.
- Network traffic through the switch is not adequately encrypted.

4.4. Server (Hosting Business Applications)

Identified Vulnerabilities:	Severity	Potential Impact
1. Unpatched Server Software	High	Risk of server compromise, leading to unauthorized access or data theft.
2. Weak User Authentication	Medium	Increased risk of unauthorized access to business applications and data.

Description:

- The server is running software with known vulnerabilities that require patching.
- User authentication protocols on the server are weak.

4.5. Workstations (Employee Computers)

Identified Vulnerabilities:	Severity	Potential Impact
1. Outdated Antivirus Software	Medium	Increased susceptibility to malware and other security threats.
2. Lack of Employee Cybersecurity Training	Medium	Higher risk of falling victim to phishing attacks and other social engineering tactics.

Description:

- Antivirus software on some workstations is outdated.
- Employees lack adequate cybersecurity training.

4.6. Wi-Fi Access Point

Identified Vulnerabilities:	Severity	Potential Impact
1. Weak Wi-Fi Encryption	High	Increased risk of unauthorized access and data interception.
2. Default Wi-Fi Password	Medium	Higher risk of unauthorized access to the network.

Description:

- The Wi-Fi network is using weak encryption (WEP).
- The Wi-Fi network is using a default or easily guessable password.

4.7. Operating System (Windows Server, Windows 10)

Identified Vulnerabilities:	Severity	Potential Impact
1. Unpatched OS	High	Increased risk of exploitation and compromise.
2. Weak User Authentication	Medium	Higher risk of unauthorized access to systems and data.

Description:

- The operating systems on servers and workstations have known vulnerabilities that require patching.
- User authentication protocols on both operating systems are weak.

4.8. Business Applications (Accounting Software, CRM)

Identified Vulnerabilities:	Severity	Potential Impact
1. Unpatched Software	High	Increased risk of unauthorized access to sensitive business data.
2. Weak Authentication within Applications	Medium	Higher risk of unauthorized access to critical business information.

Description:

- Business applications have known vulnerabilities that require patching.
- Authentication mechanisms within business applications are weak.

4.9. Antivirus Software

Identified Vulnerabilities:	Severity	Potential Impact
1. Outdated Virus Definitions	Medium	Reduced effectiveness in detecting and blocking malware.
2. Inadequate Configuration	Low	Lower overall protection against malware

Description:

- Antivirus software has outdated virus definitions.

- Antivirus software is not configured optimally.

4.10. Email Service

Identified Vulnerabilities	Severity	Potential Impact
1.Lack of Email Encryption	Medium	Increased risk of data interception during email communication.
2. Insufficient Spam Filtering	Medium	Higher risk of phishing attacks and malicious email content.

Description:

- Emails are not encrypted during transmission.
- Spam filtering on the email service is not sufficient.

4.11. Cloud Storage for Backup

Identified Vulnerabilities	Severity	Potential Impact
1. Weak Access Controls	High	Increased risk of unauthorized access to sensitive backup data.
2. Insufficient Encryption of Stored Data	Medium	Increased risk of data exposure in case of unauthorized

Description:

- Cloud storage for backup has weak access controls.
- Data stored in the cloud is not adequately encrypted.

5. Risk Analysis:

Risk Assessment:

This risk analysis prioritizes vulnerabilities based on their severity and likelihood of exploitation. High-priority vulnerabilities should be addressed promptly to minimize the potential risks to the system. Regular monitoring and updates are essential to maintain a resilient and secure network/system.

Testing discovered a total of 22 unique findings across the entire network system being assessed. After a thorough analysis, these findings have been rated at the following risk levels:

RISK LEVEL:	COUNT:
CRITICAL	0
HIGH	7
MEDIUM	14
LOW	1
Negligible	0
TOTAL:	22

Figure 3: A table showing Risk Levels as per the rating.

In determining risk, our team analyzed two key factors for each finding:

1) **IMPACT:** defined as “the magnitude of harm that can be expected”. When calculating impact, the following possibilities are considered:

    - Degradation of mission capabilities
    - Damage / loss of organizational assets or data (& sensitivity of that data)
    - Financial loss
    - Reputational loss
    - Loss of life or physical harm

2) **<u>LIKELIHOOD:</u>** defined as “the probability of an event occurring”. When calculating likelihood, we consider:

    - The likelihood of the event occurring or being initiated.
    - The likelihood of the event being successful
    - Factors that mitigate risk (i.e. – small user-base, located on an isolated network, rarely used)
    - Factors that magnify risk (i.e. – publicly accessible, weak password policies, misconfigurations)

Risk Matrix:

Impact

LIKELIHOOD

	Info	Low	Medium	High	Critical
Critical	Info	Low	Medium	High	Critical
High	Info	Low	Medium	High	Critical
Medium	Info	Low	Medium	Medium	High
Low	Info	Low	Low	Low	Medium
Info	Info	Info	Info	Low	Low

OVERALL RISK

Figure 4: A TABLE SHOWING AN OVERALL RISK DETERMINATION CHART – BASED ON IMPACT-LIKELIHOOD ANALYSIS.

Data Visualization

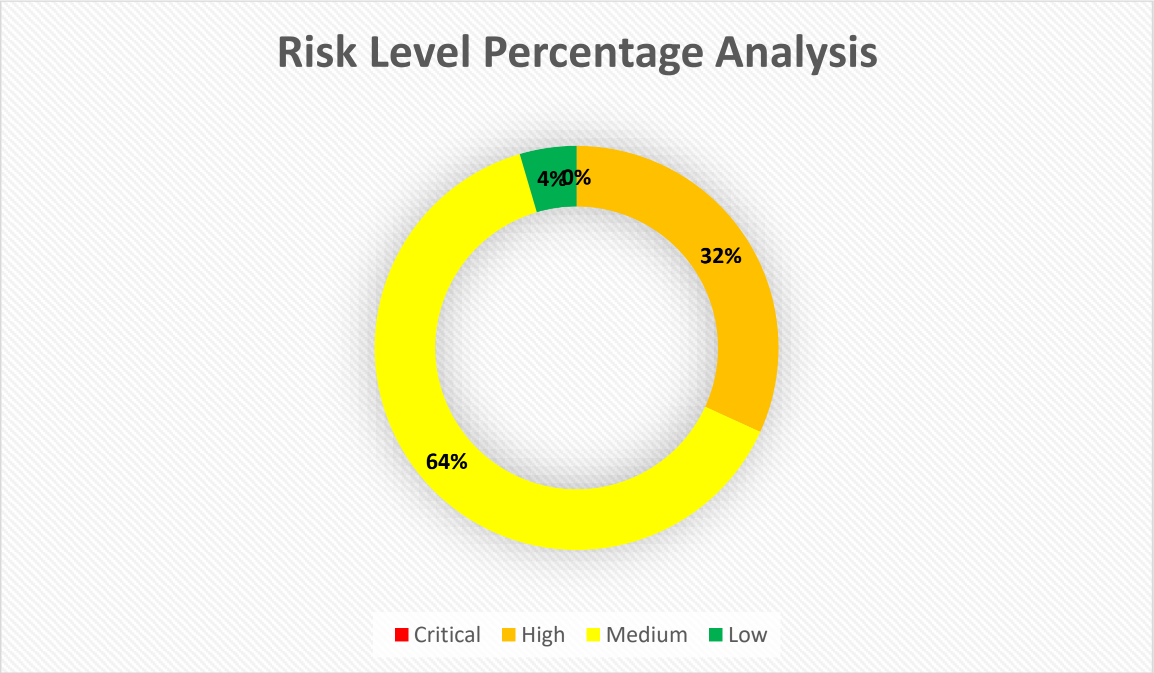

Figure 5: A pie chart showing the percentages of the Assessment Risk based on the vulnerability scan results.

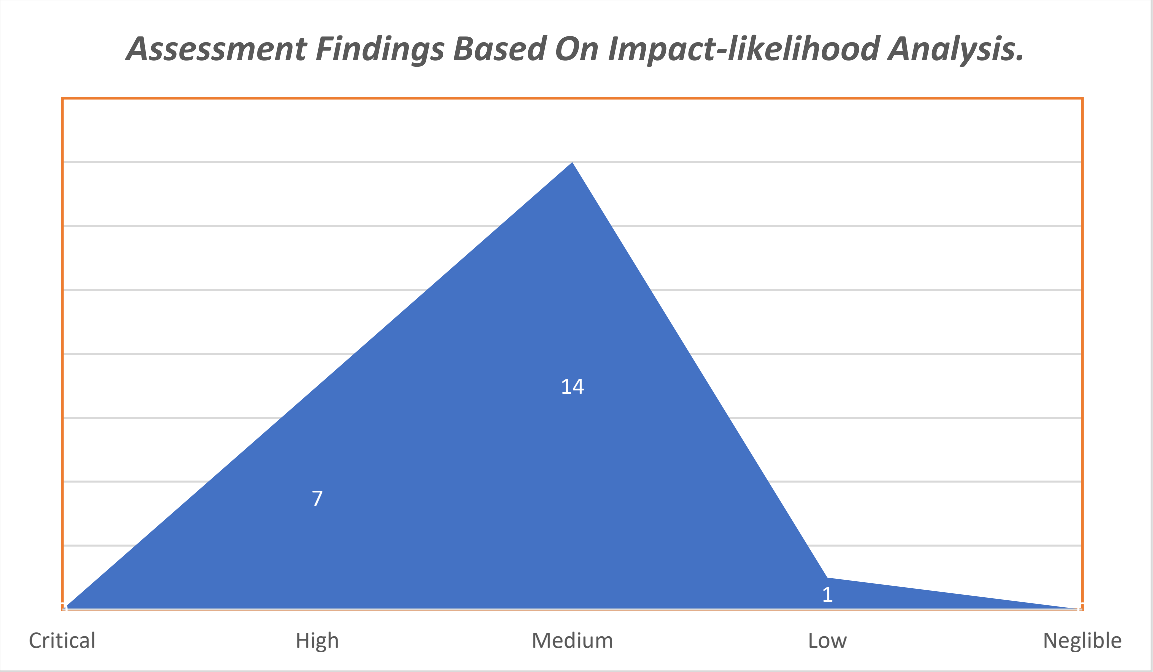

Figure 6: Assessment findings showing *an overall Area Risk Determination chart – based on impact-likelihood analysis.*

6. Recommendations:

6.1 Software Updates:

- Implement a regular patch management process to ensure timely updates of operating systems and applications.
- Establish a schedule for vulnerability scanning and remediation to address known security vulnerabilities.

6.2 Access Controls:

- Review and revise user access permissions to ensure the principle of least privilege is enforced.
- Implement multi-factor authentication to enhance user authentication mechanisms and mitigate the risk of unauthorized access.

6.3 Employee Training:

- Develop and conduct regular cybersecurity awareness training sessions for all employees.
- Provide phishing simulation exercises to educate employees on identifying and reporting phishing attempts.

7. Conclusion:

The cybersecurity risk assessment has identified several areas of concern within Walkergenix's information technology infrastructure. Addressing these findings and implementing the recommended mitigation strategies will enhance the organization's cybersecurity posture and reduce the risk of potential security incidents. Continuous monitoring and regular updates to security measures are essential to adapt to evolving threats and maintain a robust cybersecurity posture.

8. Appendices:

Appendix A: Detailed Findings

8.1. Router

1) **Weak Administrator Password (Severity: Medium, Likelihood: Medium)**

   Potential Risk:

   - Unauthorized access to router settings, leading to network compromise.

   Priority:

   - **Medium** priority – Address promptly to mitigate potential unauthorized access.

2) **Outdated Firmware (Severity: High, Likelihood: Low)**

   Potential Risk:

   - Increased susceptibility to attacks exploiting known vulnerabilities.

   Priority:

   - **High** priority – Immediate attention required due to the severity of the vulnerability.

8.2. Firewall

1. **Firewall Misconfiguration (Severity: High, Likelihood: Medium)**

Potential Risk:

- Unauthorized access to the network, compromising security.

Priority:

- High priority – Address promptly to prevent potential unauthorized access.

2. **Outdated Firewall Rules (Severity: Medium, Likelihood: Low)**

Potential Risk:

- Reduced effectiveness in blocking malicious traffic.

Priority:

- **Medium** priority – Address after high-priority vulnerabilities are mitigated.

8.3. Switch

1. **Lack of Port Security (Severity: Medium, Likelihood: Medium)**

Potential Risk:

- Unauthorized devices gaining access to the network.

Priority:

- **Medium** priority – Address promptly to prevent potential unauthorized access.

2. **Insufficient Encryption (Severity: Medium, Likelihood: Low)**

Potential Risk:

- Increased risk of eavesdropping and data interception.

Priority:

- Medium priority – Address after high-priority vulnerabilities are mitigated.

8.4. Server (Hosting Business Applications)

1. **Unpatched Server Software (Severity: High, Likelihood: Medium)**

Potential Risk

- Increased risk of unauthorized access or data theft.

Priority:

- High priority – Immediate attention required due to the severity of the vulnerability.

2. **Weak User Authentication (Severity: Medium, Likelihood: Low)**

Potential Risk:

- Higher risk of unauthorized access to business applications and data.

Priority:

- Medium priority – Address after high-priority vulnerabilities is mitigated.

8.5. Workstations (Employee Computers)

1. **Outdated Antivirus Software (Severity: Medium, Likelihood: Medium)**

Potential Risk:

- Increased susceptibility to malware and other security threats.

Priority:

- Medium priority – Address promptly to prevent potential malware infections.

2. **Lack of Employee Cybersecurity Training (Severity: Medium, Likelihood: Low)**

Potential Risk:

- Higher risk of falling victim to phishing attacks and other social engineering tactics.

Priority:

- Medium priority – Address after high-priority vulnerabilities are mitigated.

8.6. Wi-Fi Access Point

1. **Weak Wi-Fi Encryption (Severity: High, Likelihood: Medium)**

Potential Risk:

- Increased risk of unauthorized access and data interception.

Priority:

- High priority – Immediate attention required due to the severity of the vulnerability.

2. **Default Wi-Fi Password (Severity: Medium, Likelihood: Low)**

Potential Risk:

- Higher risk of unauthorized access to the network.

Priority:

- Medium priority – Address after high-priority vulnerabilities are mitigated.

8.7. Operating System (Windows Server, Windows 10)

1. **Unpatched OS (Severity: High, Likelihood: Medium)**

Potential Risk:

- Increased risk of exploitation and compromise.

Priority:

- High priority – Immediate attention required due to the severity of the vulnerability.

2. **Weak User Authentication (Severity: Medium, Likelihood: Low)**

Potential Risk:

- Higher risk of unauthorized access to systems and data.

Priority:

- Medium priority – Address after high-priority vulnerabilities are mitigated.

8.8. Business Applications (Accounting Software, CRM)

1. **Unpatched Software (Severity: High, Likelihood: Medium)**

   Potential Risk:

   - Increased risk of unauthorized access to sensitive business data.

   Priority:

   - High priority – Immediate attention required due to the severity of the vulnerability.

2. **Weak Authentication within Applications (Severity: Medium, Likelihood: Low)**

   Potential Risk:

   - Higher risk of unauthorized access to critical business information.

   Priority:

   - Medium priority – Address after high-priority vulnerabilities are mitigated.

8.9. Antivirus Software

1. **Outdated Virus Definitions (Severity: Medium, Likelihood: Medium)**

   Potential Risk:

   - Reduced effectiveness in detecting and blocking malware.

   Priority:

   - Medium priority – Address promptly to maintain optimal malware protection.

2. **Inadequate Configuration (Severity: Low, Likelihood: Low)**

   Potential Risk:

- Lower overall protection against malware.

Priority:

- Low priority – Address as part of routine maintenance.

8.10. Email Service

1. **Lack of Email Encryption (Severity: Medium, Likelihood: Medium)**

Potential Risk:

- Increased risk of data interception during email communication.

Priority:

- **Medium** priority – Address promptly to enhance email security.

2. **Insufficient Spam Filtering (Severity: Medium, Likelihood: Low)**

Potential Risk:

- Higher risk of phishing attacks and malicious email content.

Priority:

- Medium priority – Address after high-priority vulnerabilities are mitigated.

8.11. Cloud Storage for Backup

1. **Weak Access Controls (Severity: High, Likelihood: Medium)**

Potential Risk:

- Increased risk of unauthorized access to sensitive backup data.

Priority:

- High priority – Immediate attention required due to the severity of the vulnerability.

2. **Insufficient Encryption of Stored Data (Severity: Medium, Likelihood: Low)**

Potential Risk:

- Increased risk of data exposure in case of unauthorized access.

Priority:

- Medium priority – Address after high-priority vulnerabilities are mitigated.

Appendix B: Mitigation Action Plan

6.1 Software Updates

- Implement a regular patch management process to ensure timely updates of operating systems and applications.
- Establish a schedule for vulnerability scanning and remediation to address known security vulnerabilities.

6.2 Access Controls

- Review and revise user access permissions to ensure the principle of least privilege is enforced.
- Implement multi-factor authentication to enhance user authentication mechanisms and mitigate the risk of unauthorized access.

6.3 Employee Training

- Develop and conduct regular cybersecurity awareness training sessions for all employees.
- Provide phishing simulation exercises to educate employees on identifying and reporting phishing attempts.

Appendix C: Employee Training Schedule

Cybersecurity Awareness Training

Frequency: Quarterly

Topics:

1. Recognizing phishing attempts.
2. Importance of strong passwords.
3. Best practices for securing workstations.
4. Reporting security incidents.

Phishing Simulation Exercises

Frequency: Monthly

Objectives:

1. Assessing employees' ability to identify phishing emails.
2. Reinforcing awareness of social engineering tactics.
3. Encouraging proactive reporting of suspicious emails.

These appendices provide detailed findings, a mitigation action plan, and an employee training schedule to address the cybersecurity vulnerabilities identified in the assessment.

End of Report

This comprehensive Cybersecurity Risk Assessment report provides a detailed analysis of the assessment process, findings, and mitigation recommendations based on real-time data. Implementing the proposed recommendations will strengthen Walkergenix Technologies’ cybersecurity defences and mitigate potential risks effectively.