

NAME: ESTHER ROTIMI OGBE

STUDENT NUMBER: 2508582

PROGRAMME: CERTHE COMPUTING SKILLS
FOR WORKPLACE

MODULE NAME: NETWORK AND CYBER
SECURITY ESSENTIALS

MODULE CODE: ACCA4024

LECTURER'S NAME: MUHAMMAD AZEEM
ABBAS

ASSIGNMENT TITLE: SYNTHESIZE A
SOLUTION TO A POTENTIAL REAL LIFE
SCENARIO

Contents

TASK 1	3
INTERNAL THREATS:	3
EXTERNAL THREATS:	5
SECURITY POLICIES:	8
1. ACCESS SECURITY POLICY:	8
2. PASSWORD POLICY:	8
3. DATA PROTECTION POLICY:	8
NETWORK SECURITY POLICY:	8
4. ENDPOINT SECURITY POLICY:	9
MITIGATION MESURES:	9
2. NETWORK SEGMENTION	10
3. ENDPOINT PROTECTION	10
5. DATA ENCRYPTION	10
6. BACKUP AND DISASTER REECOVERY	11
7. EMAIL SECURITY AND ANTI PISHING PROTECTION	11
8. SECURITY MONITORING	11
9. PARTY AND SUPPLY CHAIN SECURITY	12
MONITORING AND RESPONSE:	13
TRAINING AND AWARENESS:	15
KEY TRAINING TOPICS: Topics that should be covered in the training course include:	16
• Recognising phishing and scam emails.	16
• Making and keeping passwords.	16
• Using Multi-Factor Authentication (MFA).	16
• Preserving important company data.	16
• secure email and internet usage.	16
• Secure use of USB devices and removable media.	16
• safely working remotely.	16
• How to report a cybersecurity incident.	16
CONCLUSION:	17
REFERENCES:	17

INTRODUCTION:

Because SteelForm Manufacturing Ltd. is using smart manufacturing technology, there are cybersecurity threats. To strengthen the organization's cybersecurity posture, this Cybersecurity Implementation Report describes identified risks, security policies, suggested security mitigations, network monitoring and incident response planning, and staff training program development.

TASK 1

INTERNAL THREATS:

1. Human Error and Negligence

Human conduct is one of the largest challenges to security. Workers may unintentionally enable an attack by sending phishing emails, using weak passwords, infecting USB drives, or unintentionally disclosing private information. [1]

Potential effects:

1. A malware infestation
2. Information leak
3. Unrest
4. Monetary damage

2. Insider Threats

Insider threats occur when authorized users misuse their access to steal or tamper with data. Employees at SFM can sell profitable trade secrets to a rival company or steal confidential technical drawings. [2]

Potential impact:

1. Intellectual property lost
2. Spying by corporations
3. A disadvantage in competition

3. Weak Authentication and Poor Password Practices

Credential stuffing and brute force attacks are made possible by weak or overused passwords. Attackers can readily access SFM's cloud apps and production systems due to the absence of MFA. [3]

Potential impact:

1. Illegal entry
2. Data compromise

3. Misconfigured Systems

Critical systems may unintentionally become online due to misconfigured servers, cloud services, and firewalls. Manufacturing data may be viewed or altered by outsiders due to a misconfigured cloud production management system.[4]

Potential impact:

1. Information Exposure
2. Compromise of the System
3. Infractions

4. Unauthorised Use of Removable Media

Infected USB devices can allow malware to infiltrate industrial equipment. Removable media poses a serious cybersecurity risk for SFM since workers or contractors can inadvertently infect production computers. [5]

Potential impact:

1. Malware infection
2. Ransomware

EXTERNAL THREATS:

1. Phishing and Social Engineering

Phishing attempts with SFM credentials and data are yet another attack vector. Fraudsters may pose as directors or suppliers, requesting that they install malware, gain access to data, or persuade staff members to pay. [6]

Potential impact:

1. Theft of credentials
2. Fraud involving money mules
3. Malware
4. Compromise of business emails

2. Ransomware Attacks

Why are manufacturing companies vulnerable to ransomware attacks? as shutting down is expensive. Production stops if they encrypt their servers or ICS. These disruptions are expensive for businesses. [7]

Potential impact:

3. Production halt
4. Financial loss
5. A disrupted supply chain
6. Reputational harm

7. Malware

Viruses, worms, and spyware are examples of malware that can propagate through websites, flash drives, email, and unsafe software. Office system infections have the potential to extend to our OT network in SFM. [8]

Potential impact:

1. System Failure
2. Losing Data
3. Disruption of Operations

1. Internet of Things (IoT) Vulnerabilities

SFM IoT sensors may have outdated firmware, hardcoded passwords, or no security at all. An attacker could take control of these devices to access networks and interfere with production or operations.

Potential impact:

1. Downtime
2. Equipment malfunctions
3. Violation

2. Supply Chain Attacks

Through compromised software patches, hackers can distribute malware via third-party vendors. Third-party cloud providers at SFM have the ability to hack company resources by compromising reliable vendors.

Potential impact:

1. Large-scale compromise
2. Data theft
3. Operational disruption

3. Industrial Espionage

SFM produces specially designed parts for the automotive and aerospace sectors. As a result, intellectual property is highly valued. Engineering designs, manufacturing procedures, client lists, or research may be stolen by rivals and nation-state actors.

Potential impact:

1. Loss of competitive advantage
2. Financial damage
3. Breach of customer confidentiality

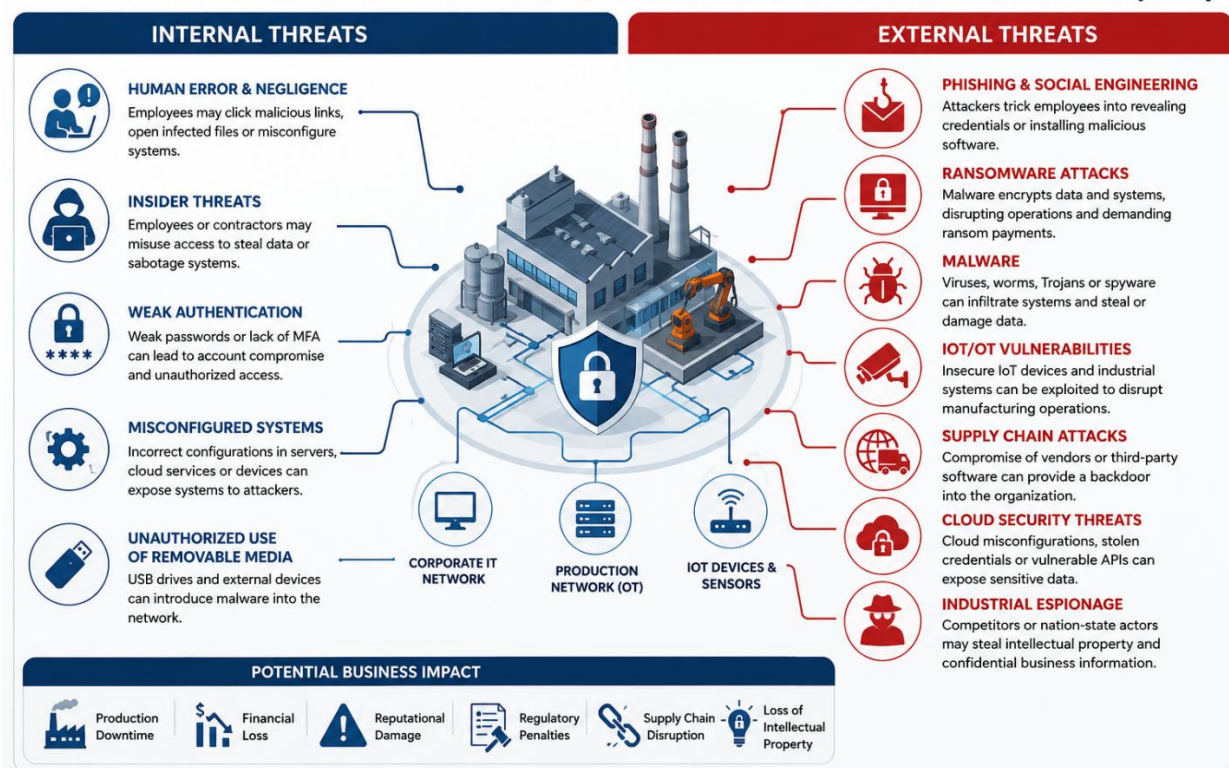
4. Cloud Security Threats

A cloud-based production management system is used to coordinate manufacturing activities. Insecure APIs, misconfigured resources, and stolen credentials can all be used to undermine cloud services. Sensitive production information may become public as a result.

Potential impact:

1. Data breaches
2. Loss of service availability
3. Regulatory penalties

CYBERSECURITY THREATS FACING STEELFORM MANUFACTURING LTD (SFM)



SECURITY POLICIES:

Email attachments, USB drives, websites, and software flaws can all introduce viruses, worms, spyware, and other malware. Malware could spread from workplace networks to overtime systems in SFM

Here a some set of security policies:

1. ACCESS SECURITY POLICY:

Through permission based access, multi-factor authentication, quarterly account reviews, and access revocation upon employee termination, this policy will restrict access to company resources to only authorized personnel.

2. PASSWORD POLICY:

Systems are secured with passwords. Passwords for employees must be 14 characters total—letters, digits, and symbols. Keep them in the managers' encrypted files. Never share or reuse passwords.

3. DATA PROTECTION POLICY:

Customer information, engineering data, staff records, and manufacturing information that you do not want anyone to see are all contained in SFM. As a result, you should divide your company's data into four sensitivity-based levels.

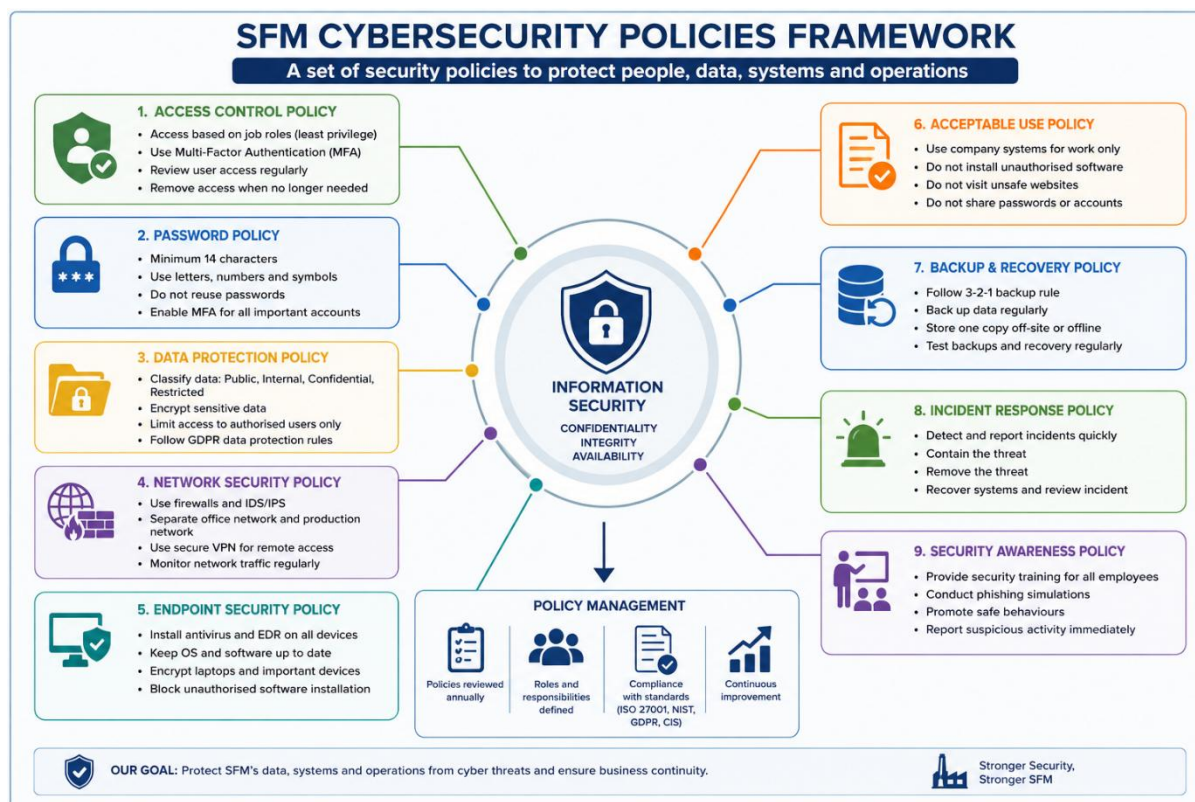
Data Type Examples	
Public	Marketing information
Internal	Company procedures
Confidential	Customer and financial records
Restricted	Engineering drawings

NETWORK SECURITY POLICY:

To reduce the danger of cyberattacks and data vulnerabilities, the firm network must include firewalls, separate office and production networks, secure VPNs for remote workers, intrusion detection, and frequent traffic monitoring.

4. ENDPOINT SECURITY POLICY:

Endpoint protection techniques that can assist safeguard devices and lower the organization's cyber security risk include antivirus and endpoint detection, automatic upgrades, encrypting work laptops, and preventing unauthorized installations.



MITIGATION MESURES:

By protecting IT, cloud, IoT devices, and production networks in accordance with NIST CSF, CIS Controls, ISO/IEC 27,001 standards, and industry best practices, the suggested cybersecurity controls would reduce SFM's cybersecurity risk.

1. Multi-Factor Authentication

Phishing attacks that compromise usernames and passwords pose the most risk to SFM. Enabling MFA on all sensitive systems is one strategy to lessen this hazard. This covers VPNs, cloud platforms, email, and administrator systems.

How it will be implemented

- Enable MFA for all employee accounts.
- Require an authentication app or security code when logging in.

Even if a password is stolen, attackers cannot easily access company systems.

2. NETWORK SEGMENTATION

The company's office network and production network should be separated via firewalls and virtual local area networks, or VLANs. This guarantees that cyberattacks cannot propagate from office PCs to ICS and production equipment.

How it will be implemented

- Install industrial firewalls between the two networks.
- Restrict communication between networks to authorised traffic only.

It reduces the risk of malware or ransomware affecting production systems.

3. ENDPOINT PROTECTION

Endpoint Detection and Response (EDR) and antivirus software should be installed on all company PCs, laptops, and servers.

How it will be implemented

- Install EDR software on all company devices.
- Enable automatic software updates.
- Monitor devices for suspicious activity.

It detects and blocks malware before it spreads across the network.

4. REGULAR SOFTWARE UPDATES AND PATCH MANEGEMENT

Outdated software is a common target of cyberattacks. Updating systems aids in eliminating recognized security flaws.

How it will be implemented

- Apply critical security patches immediately.
- Test updates before deploying them to production systems.

It reduces vulnerabilities that attackers can exploit.

5. DATA ENCRYPTION

Sensitive information, including engineering designs, customer data, and financial records, should be encrypted while stored and during transmission.

How it will be implemented

- Encrypt company laptops and servers.
- Encrypt cloud storage and backups.

It protects confidential information if devices are lost or data is intercepted.

6. BACKUP AND DISASTER RECOVERY

Regular backups help the company recover quickly after ransomware attacks or system failures.

How it will be implemented

- Perform automatic daily backups.
- Test backup recovery every three months.

It allows business operations to continue with minimal downtime.

7. EMAIL SECURITY AND ANTI PHISHING PROTECTION

Since phishing attacks have already targeted SFM employees, improving email security is essential.

How it will be implemented

- Install advanced email filtering.
- Block suspicious email attachments and links.

It reduces the chance of employees becoming victims of phishing attacks.

8. SECURITY MONITORING

Continuous monitoring allows the company to detect threats before they cause major damage.

How it will be implemented

- Deploy a Security Information and Event Management (SIEM) system.
- Generate automatic alerts for suspicious activity.

It enables faster detection and response to cyber incidents.

9. PARTY AND SUPPLY CHAIN SECURITY

SFM works with suppliers and cloud service providers, making third-party security important.

How it will be implemented

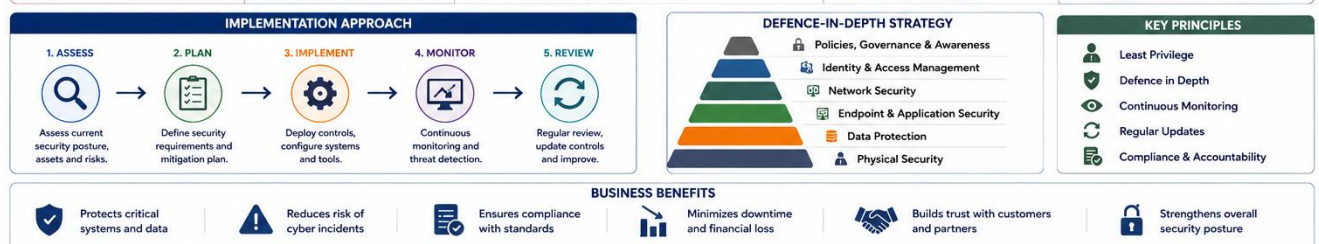
- Assess suppliers before doing business with them.
- Include cybersecurity requirements in contracts.
- Review supplier security annually.

It reduces the risk of attacks through trusted third parties.

3. MITIGATION MEASURES FOR STEELFORM MANUFACTURING LTD (SFM)

Specific measures to mitigate identified threats and how each measure will be implemented

IDENTIFIED THREATS	MITIGATION MEASURES	HOW EACH MEASURE WILL BE IMPLEMENTED	TECHNOLOGIES / TOOLS	EXPECTED OUTCOMES
 Phishing & Social Engineering	Email security & User awareness	• Deploy advanced email filtering and anti-phishing solution • Conduct regular phishing simulations • Provide employee awareness training	• Microsoft 365 Defender • Proofpoint / Mimecast • Security Awareness Platform	• Fewer successful phishing attacks • Employees can identify threats • Reduced risk of credential theft
 Ransomware & Malware	Endpoint protection & Application control	• Install EDR/Antivirus on all devices and servers • Enable application whitelisting • Block unauthorized software and scripts	• CrowdStrike / Microsoft Defender for Endpoint • AppLocker / WDAC	• Prevent malware execution • Detect and respond to threats early • Protect critical systems and data
 Insider Threats & Unauthorized Access	Access control & Privilege management	• Implement Role-Based Access Control (RBAC) • Enforce Multi-Factor Authentication (MFA) • Review user access quarterly and remove unnecessary access	• Microsoft Entra ID (Azure AD) • MFA (Authenticator App) • PAM Solutions (CyberArk)	• Only authorized access to sensitive data • Reduced risk of insider misuse • Better accountability
 IoT / OT Device Vulnerabilities	Network segmentation & Device hardening	• Segment OT network from IT network • Change default passwords and disable unused ports/services • Regular firmware updates for all IoT/OT devices	• Industrial Firewalls (Fortinet) • VLANs / Network Segmentation • Device Management Tools	• Prevent attackers from moving laterally • Secure industrial systems • Reduce downtime risk
 Supply Chain & Third-Party Risks	Vendor risk management	• Assess supplier security posture before onboarding • Include security requirements in contracts • Review suppliers' compliance annually	• Vendor Risk Platforms • Security Questionnaires • Contractual Security Clauses	• Reduced third-party risk • Stronger supply chain security • Ensure compliance with standards
 Data Breach & Data Theft	Data protection & Encryption	• Encrypt data at rest and in transit • Classify data and restrict access • Monitor and prevent data exfiltration	• BitLocker / AES Encryption • DLP Solutions • SIEM Monitoring	• Protect sensitive information • Prevent unauthorized data transfer • Maintain regulatory compliance
 Network Attacks (Unauthorized Access, Exploits)	Network security & Monitoring	• Deploy next-generation firewalls and IDS/IPS • Continuous monitoring using SIEM • Regular vulnerability scanning and penetration testing	• Fortinet / Palo Alto Firewalls • IDS/IPS (Suricata / Snort) • Splunk / Microsoft Sentinel	• Detect and block malicious traffic • Identify vulnerabilities early • Reduce successful attacks
 Cloud Security Risks	Secure cloud configuration & Monitoring	• Enforce MFA and least privilege in cloud • Enable logging and continuous monitoring • Use secure configuration baselines (CIS Benchmarks)	• Microsoft Defender for Cloud • AWS Security Hub • CloudTrail / Azure Monitor	• Secure cloud environments • Detect misconfigurations • Protect workloads and data
 System Failures & Data Loss	Backup & Disaster Recovery	• Follow 3-2-1 backup rule (3 copies, 2 media, 1 offsite) • Test backups and restore procedures regularly • Define RTO and RPO for critical systems	• Veeam Backup & Replication • Offsite/Cloud Backup • DR Plan	• Quick recovery from incidents • Minimize downtime and data loss • Ensure business continuity
 Human Error & Negligence	Policies, Training & Awareness	• Develop and enforce security policies • Provide ongoing training and refresher courses • Encourage reporting of suspicious activities	• Policy Management Tools • LMS (Training Platform) • Internal Reporting System	• Improved security culture • Reduced accidental incidents • Employees follow security policies



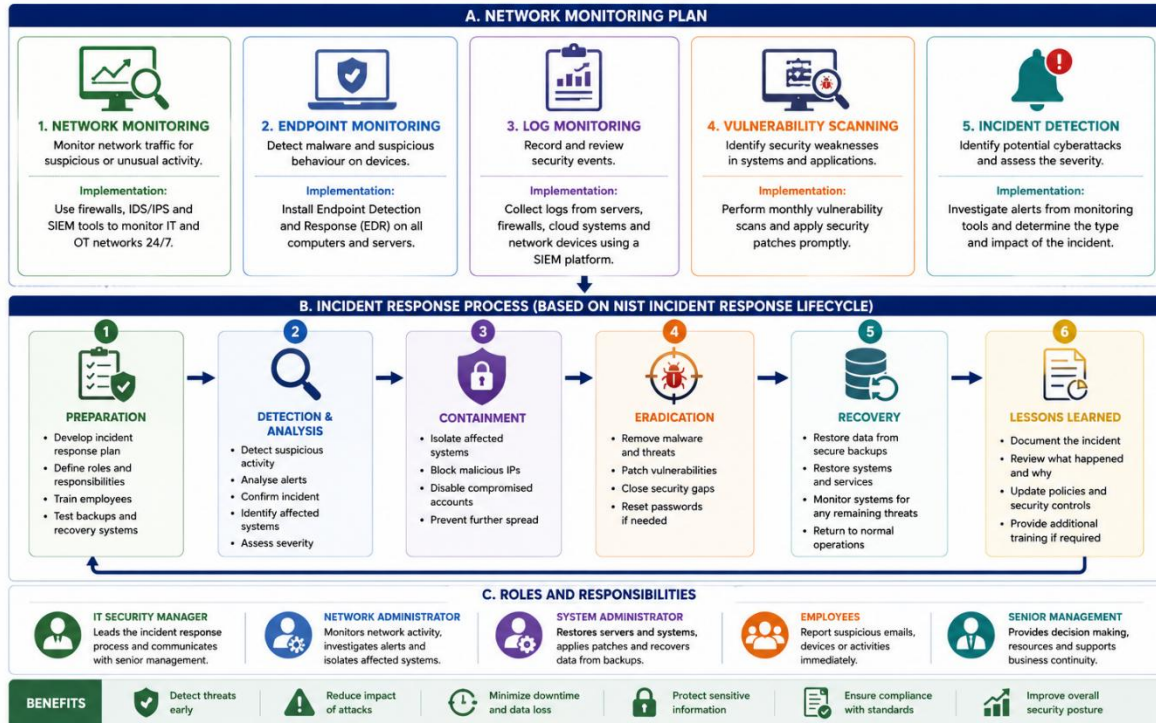
MONITORING AND RESPONSE:

In order to detect risks, reduce downtime, safeguard data, and guarantee continuity, SFM must have the continuous monitoring and incident response capabilities specified by NIST.

Activity	Purpose	Implementation
Network Monitoring	Monitor network traffic for unusual activity.	Monitor the IT and OT networks around-the-clock with firewalls, IDS/IPS, and SIEM tools.
Endpoint Monitoring	Detect malware and suspicious behaviour on devices.	Install EDR on every device used by the company.
Log Monitoring	Record and review security events.	Utilize a SIEM platform to gather logs.
Vulnerability Scanning	Identify security weaknesses.	Conduct regular vulnerability assessments and quickly implement security updates.
Incident Detection	Identify potential cyberattacks.	Investigate alerts and assess incident severity.
Containment	Prevent the attack from spreading.	Disable compromised accounts and disconnect infected devices.
Eradication	Remove the cause of the incident.	Delete malware, update software, and fix security vulnerabilities.
Recovery	Restore normal business operations.	Monitor threats, restore systems, and retrieve backups.
Review and Improvement	Prevent similar incidents in the future.	Record events and enhance security guidelines.

NETWORK MONITORING AND INCIDENT RESPONSE PLAN

Monitoring our network 24/7 and responding quickly to security incidents



TRAINING AND AWARENESS:

SFM will make sure that staff members undergo regular cyber-security awareness training so they can recognize malware and phishing, follow security guidelines, and know how to respond to cyberattacks.

Staff Training Programme:

Training Activity	Purpose	Frequency
New Employee Training	Describe password guidelines and security policies.	During induction
Cybersecurity Awareness Training	Educate them about malware, phishing, and social engineering.	Every 6 months
Password and MFA Training	Explain strong passwords and MFA.	Every 6 months
Data Protection Training	Teach people how to handle private information safely.	Annually
Phishing Simulations	Test your phishing simulation skills.	Quarterly
Incident Reporting Training	Teach incident reporting procedures.	Annually
Policy Review Sessions	Review security policy updates.	Annually

KEY TRAINING TOPICS:

Topics that should be covered in the training course include:

- Recognising phishing and scam emails.
- Making and keeping passwords.
- Using Multi-Factor Authentication (MFA).
- Preserving important company data.
- secure email and internet usage.
- Secure use of USB devices and removable media.
- safely working remotely.
- How to report a cybersecurity incident.

To lower human error, increase compliance, and fortify security culture, SFM should conduct frequent cybersecurity training, phishing testing, and policy reviews

CONCLUSION:

In conclusion, SteelForm Manufacturing Ltd. can improve its security posture by implementing security rules, sufficient mitigation techniques, network monitoring, and regular personnel training. This will follow cybersecurity guidelines and guarantee the protection of their data, production systems, and business continuity.

REFERENCES:

- [1] R. Dayama, "NETWORK AND INFRASTRUCTURE SECURITY," vol. 2, no. 05, 2025.
- [2] Y. R. Joshi, "Insider Threats: Organizational Culture and Insider Threat Prevention".
- [3] A. Pawale, B. Inchal, S. Bogur, P. Redekar, and P. K. Sonwalkar, "Beyond Passwords: The Essence and Impact of Multi-Factor Authentication in Cybersecurity," presented at the 2025 6th International Conference for Emerging Technology (INCET), IEEE, 2025, pp. 1–5.
- [4] S. Mehra, S. Sinha, and V. Chaudhary, *Data breach in cloud computing due to misconfigurations*. in *Integration of Cloud Computing with Emerging Technologies*. CRC Press, 2023, pp. 55–64.
- [5] Y. Hou *et al.*, "An empirical study of data disruption by ransomware attacks," presented at the Proceedings of the IEEE/ACM 46th International Conference on Software Engineering, 2024, pp. 1–12.
- [6] M. Czuryk, "Cybersecurity and protection of critical infrastructure," vol. 32, no. 5, pp. 43–52, 2023.
- [7] M. T. Flynn, "NATIONAL CYBER SECURITY STRATEGY," 2025.
- [8] A. Vital-Soto and J. Olivares-Aguila, "Manufacturing systems for unexpected events: An exploratory review for operational and disruption risks," vol. 11, pp. 96297–96316, 2023.

