

NETWORKS AND CYBER SECURITY ESSENTIALS

ABDIRAHMAN MAHDI

2429936

1)INTRODUCTION

Cybersecurity is defined as the process of securing computer networks from cyberattacks by preventing unauthorized access and attacks by malicious software programs and hacking attempts that may cause data breaches. With the advent of Industry 4.0, there has been increasing use of new technologies such as the Internet of Things (IoT), automation, robotics, and cloud computing in order to increase the efficiency of manufacturing processes. But with an increase in connectivity, new risks have emerged, giving cybercriminals an opportunity to attack industrial systems and steal their information. Steel Form Manufacturing Ltd (SFM) is a mid-size manufacturing company that has embraced the technology of smart manufacturing which includes the use of IoT sensors, automation of machines, and cloud-based production systems. The aim of this report is to determine the cyber threats faced by SFM and implement mitigation strategies against those threats.

2) Identification of Threats

Internal Threats

Weak Passwords: Use of weak passwords by employees can give attackers an opportunity to hack into the systems and data of the company.

Employee Negligence: Employees can create cybersecurity problems when they unintentionally click on harmful links, share private information, and ignore the necessary cybersecurity protocol.

Insider Threats: The employees or contractors of the company who have authorized access can abuse their access to compromise company data.

Malware via USB: Malicious software can enter the company's system via infected USB drives.

Access Control Issues: Inadequate user permission management can make it possible for employees to use unauthorized access to company systems or data.

Unpatched Systems: The outdated systems and software in use in the company may be vulnerable to attacks from malicious individuals.

External Threats

Ransomware: The attackers will encrypt files and systems, blocking access to crucial data and potentially halting any manufacturing process until the company pays for the ransom.

Phishing: The cybercriminals may use false emails or messages to deceive the employees in giving away their login credentials or installing harmful software on their computers.

Malware: The harmful software can be used by the hackers for damaging systems, stealing data or spying on their activities, or gaining unauthorized access.

DDoS Attacks: The attackers will bombard systems or web services with heavy traffic and thus render the systems unusable or very slow.

Supply Chain Attacks: The attackers will use third-party software providers or service providers to attack the systems of SFM through them.

Industrial Espionage: Industrial competitors or other criminal groups can try to steal intellectual property, manufacturing processes, and engineering designs from the company.

Brute-Force Attacks: The attackers will try multiple password combinations to gain entry to the system or users' account.

Security Policy

Passwords that are too weak could facilitate access by malicious parties into the organization's systems via means such as brute force attack. Therefore, SFM should have in place measures such as the setting of strong password policies regarding length of the password, mixing of different types of characters, and frequent updating of the passwords. There should also be the implementation of multi-factor authentication, especially for critical systems. The employees should utilize password managers

Access Control Policy

It is recommended that SFM implements an access control policy that will ensure that the employees are only able to access those systems and information that they need to perform their duties. Role Based Access Control (RBAC) should be implemented and permissions are granted based on the roles of the individuals. Administrators rights should be reserved only to those IT personnel authorized for such. It should also be ensured that the rights for those employees that have left the organization are discontinued right away.

Network Security Policy

SFM must develop a network security policy to ensure that all its office, cloud and manufacturing networks are secure. For instance, firewalls must be installed in order to control traffic in the networks. The manufacturing network, which includes all the automated machines and other Internet of Things (IoT) devices, must be isolated from the normal office network. Any remote access into the company's network must be restricted to secure connections, and it must also include authentication of the user. It is important to monitor the network for any unusual behavior.

Data Protection Policy

SFM stores sensitive information such as engineering designs, customer details and manufacturing processes. There is thus need for a data protection policy that describes how the data will be stored, accessed and exchanged. The sensitive data must be encrypted while storing and transmitting it through network. Employees must only have access to confidential information when necessary to do their job. Sensitive data must also be backed up periodically to ensure that they can be retrieved in case of data loss or ransomware attack.

Acceptable Use Policy

An acceptable use policy should explain how employees are permitted to use SFM's computers, networks and other technology. Employees should not install unauthorised software, share company passwords or connect unknown USB devices to company computers. Company equipment should primarily be used for authorised business

activities, and suspicious emails or unusual system behaviour should be reported to the IT security team immediately. This policy will help reduce risks caused by employee negligence, malware and infected USB devices.

Mitigation Measures

In order to mitigate the dangers associated with cyber threats, the following security controls are recommended for SteelForm Manufacturing Ltd (SFM). They will assist in safeguarding the company's manufacturing processes, cloud computing, IoT, and sensitive corporate data..

Endpoint Protection

The SFM should implement antivirus and Endpoint Detection and Response (EDR) software on company computers and other supported devices. These can help detect malicious software, monitor suspicious activity, and protect the organization against any malware propagation across the network. The antivirus should be centrally managed by the IT security team and updated frequently to ensure new threats are identified.

Data Encryption

Information that is sensitive in nature and includes things like engineering designs, customer information, and manufacturing data should always be encrypted both while storing and while transferring from one system to another. Information is rendered unreadable by using the correct key and, therefore, even if any data is stolen by an attacker, it will be harder for him/her to use it.

USB and Removable Device Controls

SFM needs to limit the use of USB drives and other kinds of removable storage devices since these devices can infect corporate computer systems with malware. The devices used in the office need to be approved by the IT department, and any unnecessary access to USB ports needs to be blocked on critical production computers.

Email Security

SFM should have an e-mail filter in place to screen for any suspicious e-mails containing attachments or links that pose security threats before reaching the employees. This is especially true as SFM has already been exposed to phishing attacks via e-mails targeted at their procurement department employees. Employees must also have an easy way to report suspicious e-mails to the IT security department.

Multi-Factor Authentication (MFA)

The SFM should put in place Multi-Factor Authentication (MFA) for both employees and administrators. In this case, the authentication process will involve more than one method, whereby users will authenticate their identity by use of a password plus another method, such as receiving an authentication code on a mobile phone.

Regular Software Updates

SFM must formulate an efficient patch management strategy where all operating systems, software programs, and IoT devices are updated on a regular basis. It is essential to implement security patches at the earliest possible moment in order to avoid exploitation by potential attackers.

Network Segmentation

The company's office network should be kept away from the company's production network through the use of firewalls and network segmentation. This would ensure that any cyber attack does not spread across the company's networks.

Regular Data Backups

SFM must undertake frequent data backups of all important data of the company. The backup data must be kept safely either offline or in a different cloud environment. It is important for SFM to test the backup data frequently in order to restore it easily when the need arises.

Employee Cybersecurity Training

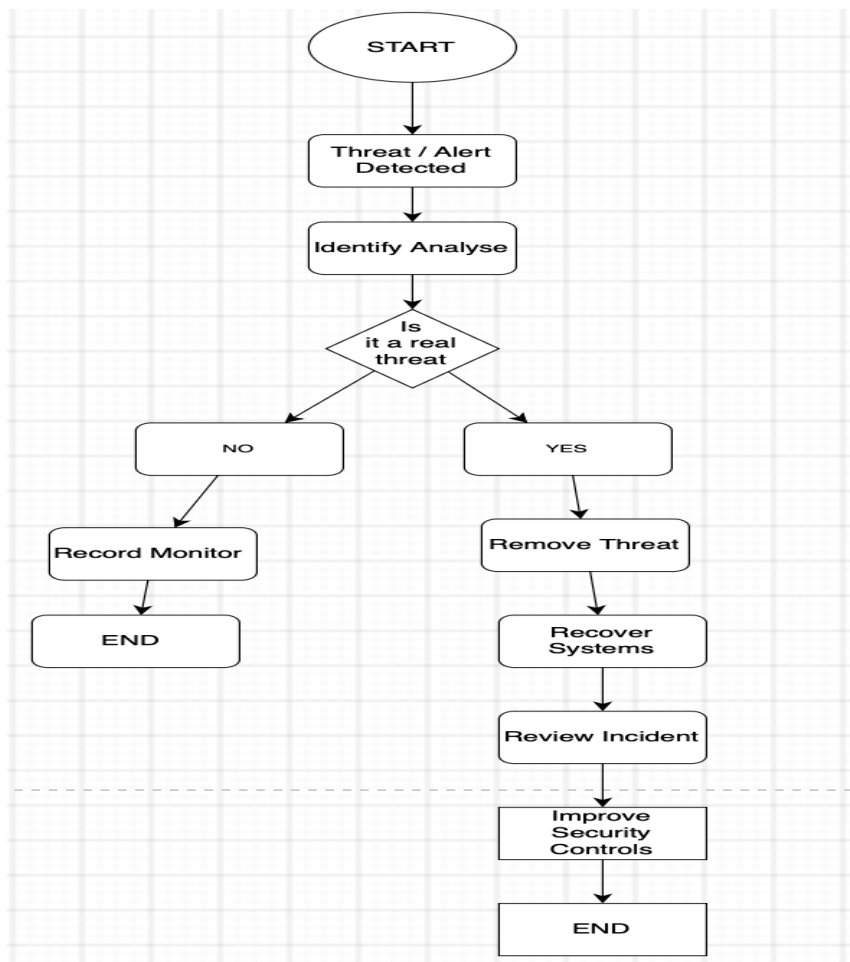
Training for employees about cybersecurity is very important as it will ensure that they understand how to spot phishing emails, how to create secure passwords, how to use USBs properly, and how to detect any suspicious behavior.

Monitoring and Response

SteelForm Manufacturing Ltd (SFM) needs to ensure that their network is regularly monitored for any suspicious behavior with the use of firewalls, Intrusion Detection Systems (IDS), and Security Information and Event Management (SIEM). In the event that an incident takes place, the firm will need to act on the basis of an incident response plan that entails identifying the threat, isolating affected systems, eliminating the threat, restoring data/services from secure backups where necessary, and reviewing the incident itself.

The IT security department at SFM needs to review all security alarms periodically and investigate any suspicious activities, which may include multiple attempts to log in or any other unauthorized access to the systems. These incidents need to be documented for the date of incident, systems involved, and actions taken. This will help SFM identify recurring security issues and safeguard itself from future incidents.

Flowchart---



Training and Awareness

SFM should organize regular cyber security training sessions to ensure that all employees are aware of the security policies of the company. Topics covered in such training programs should include detecting phishing e-mails, developing secure passwords, safe use of USB drives, securing data, and suspicious activity. Induction training for new hires should always include cyber security training. Annual refresher training should be organized for existing employees.

In order to make sure that the training is effective, SFM must also conduct phishing simulations on a regular basis during the year. Such a procedure can be used to check how employees respond to suspicious emails without compromising the safety of company systems. Additional training should be provided for those employees who have problems with such tests. Information about new threats must also be shared by the IT security team in a brief manner. It is important to keep records of the training completion.

Conclusion

To sum up, the utilization of more advanced Industry 4.0 technology has helped SFM get numerous advantages but has exposed it to various cyberattacks as well. The internal threats, including insecure passwords, negligence of the employees and poor access control, as well as the external threats such as ransomware, phishing and industrial espionage, may significantly impact the company. However, the adoption of proper security policies, multi-factor authentication, network segregation, system updating, backup, and employee training can help the company decrease these risks. Network monitoring and a proper incident response procedure will assist SFM to promptly react to possible attacks.

References

National Cyber Security Centre (NCSC) (2026) *Cyber Essentials overview and requirements*. Available at: NCSC Cyber Essentials website (Accessed: 13 August 2026).

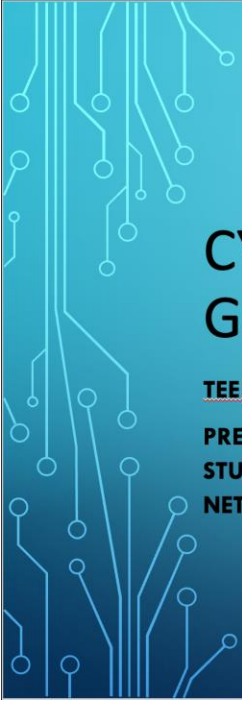
National Cyber Security Centre (NCSC) (2026) *Small organisations guide to cyber security*. Available at: NCSC website (Accessed: 13 August 2026).

National Cyber Security Centre (NCSC) (2026) *Phishing scams: how to spot and report them*. Available at: NCSC website (Accessed: 13 August 2026).

National Cyber Security Centre (NCSC) (2026) *Keeping devices and software up to date*. Available at: NCSC website (Accessed: 13 August 2026).

National Institute of Standards and Technology (NIST) (2024) *The NIST Cybersecurity Framework (CSF) 2.0*. Gaithersburg, MD: National Institute of Standards and Technology.

National Institute of Standards and Technology (NIST) (2025) *Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile (SP 800-61 Rev. 3)*. Gaithersburg, MD: National Institute of Standards and Technology.



CYBERSECURITY AND DATA GOVERNANCE POLICY

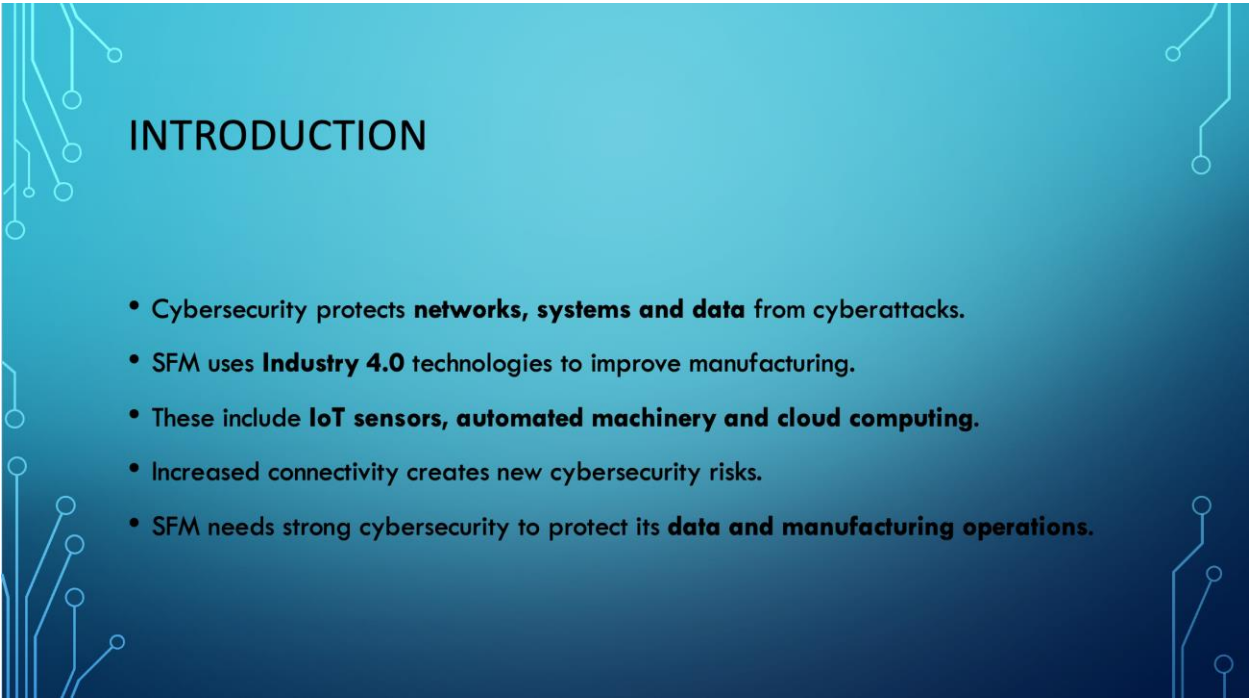
TEELFORM MANUFACTURING LTD (SFM)

PREPARED BY: ABDIRAHMAN MAHDI

STUDENT NUMBER: 2429936

NETWORKS AND CYBER SECURITY ESSENTIALS

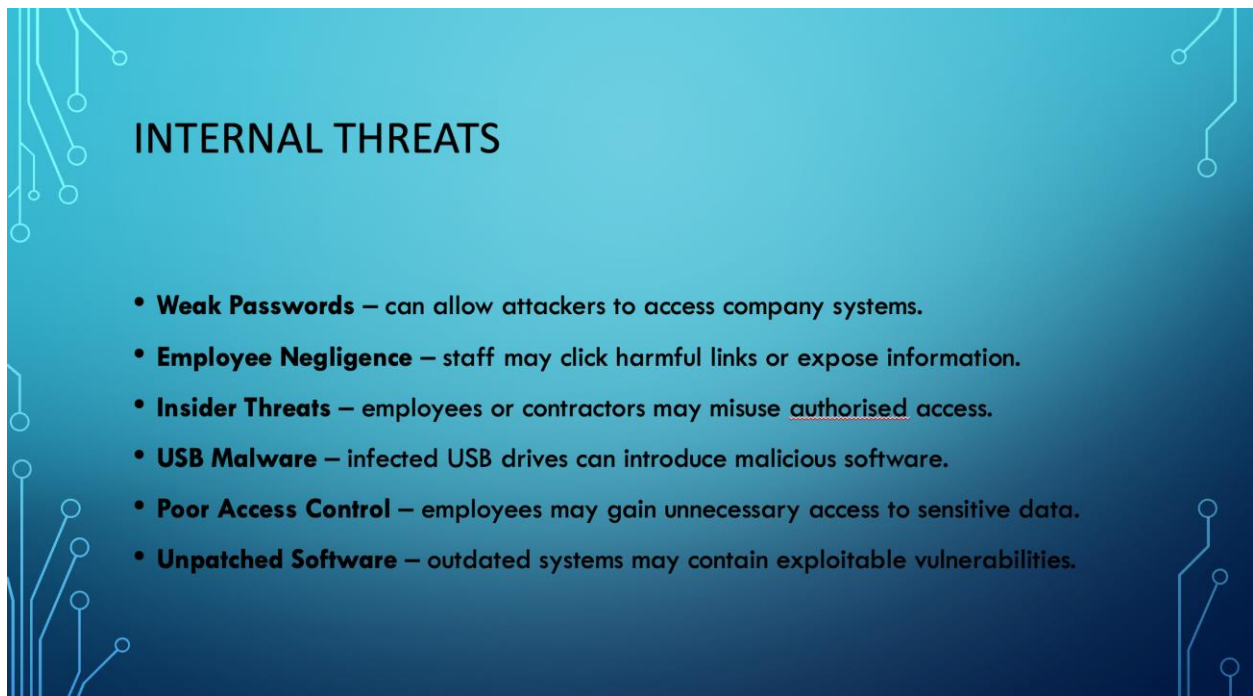
Slide 2



INTRODUCTION

- Cybersecurity protects **networks, systems and data** from cyberattacks.
- SFM uses **Industry 4.0** technologies to improve manufacturing.
- These include **IoT sensors, automated machinery and cloud computing**.
- Increased connectivity creates new cybersecurity risks.
- SFM needs strong cybersecurity to protect its **data and manufacturing operations**.

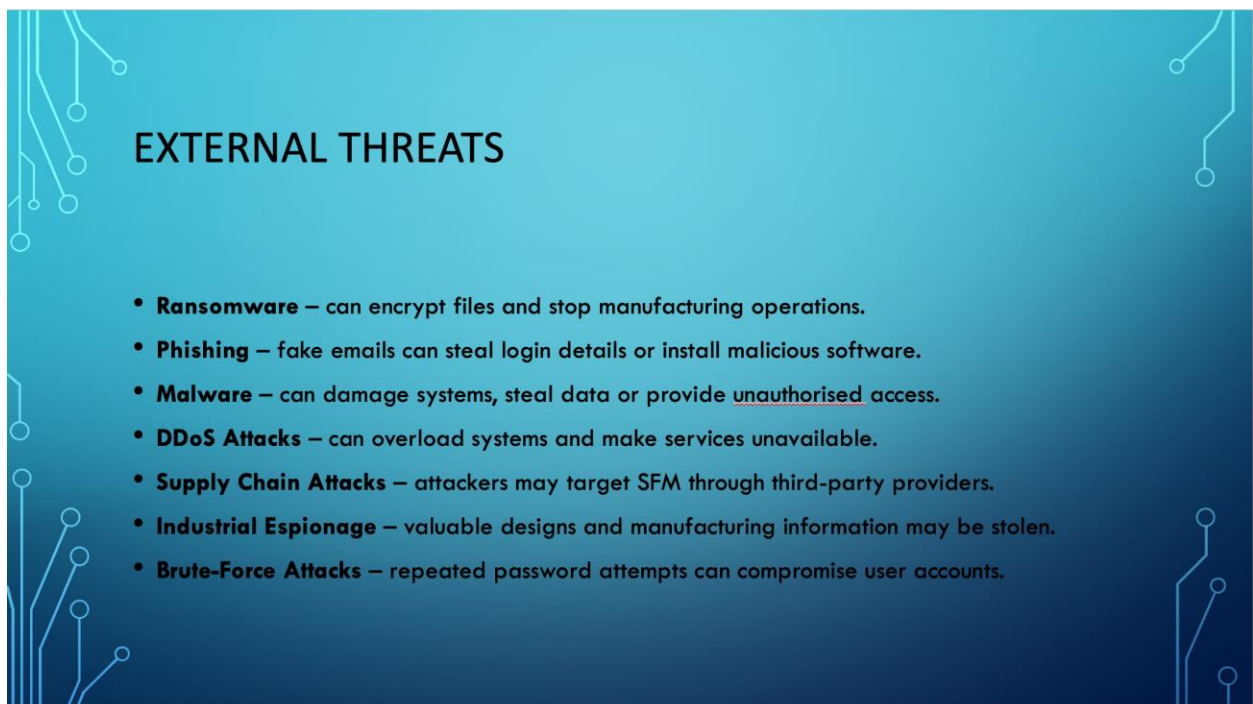
Slide 3



INTERNAL THREATS

- **Weak Passwords** – can allow attackers to access company systems.
- **Employee Negligence** – staff may click harmful links or expose information.
- **Insider Threats** – employees or contractors may misuse authorised access.
- **USB Malware** – infected USB drives can introduce malicious software.
- **Poor Access Control** – employees may gain unnecessary access to sensitive data.
- **Unpatched Software** – outdated systems may contain exploitable vulnerabilities.

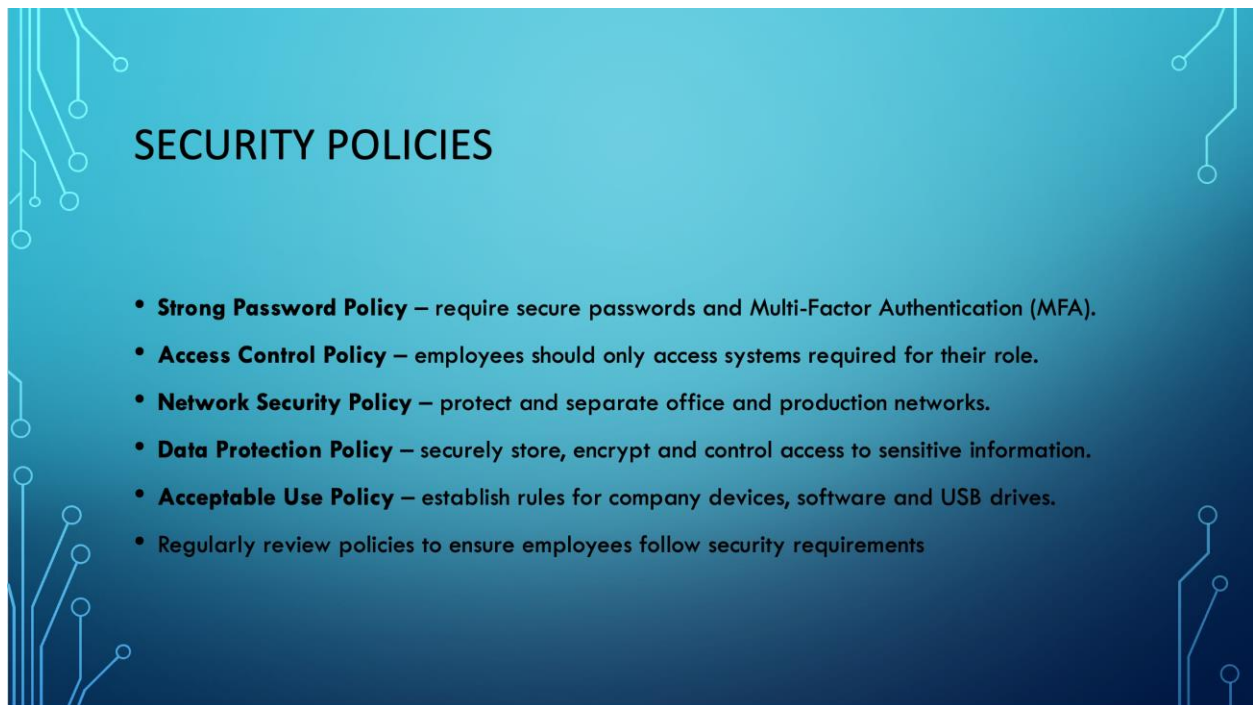
Slide 4



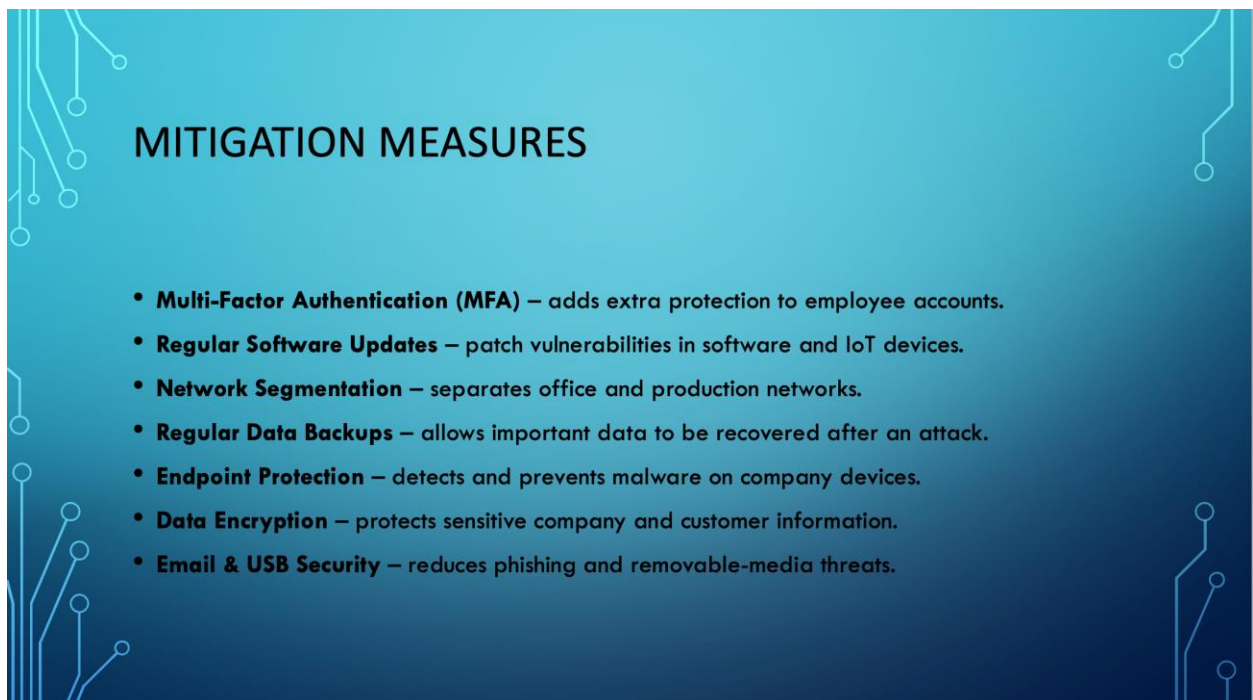
EXTERNAL THREATS

- **Ransomware** – can encrypt files and stop manufacturing operations.
- **Phishing** – fake emails can steal login details or install malicious software.
- **Malware** – can damage systems, steal data or provide unauthorised access.
- **DDoS Attacks** – can overload systems and make services unavailable.
- **Supply Chain Attacks** – attackers may target SFM through third-party providers.
- **Industrial Espionage** – valuable designs and manufacturing information may be stolen.
- **Brute-Force Attacks** – repeated password attempts can compromise user accounts.

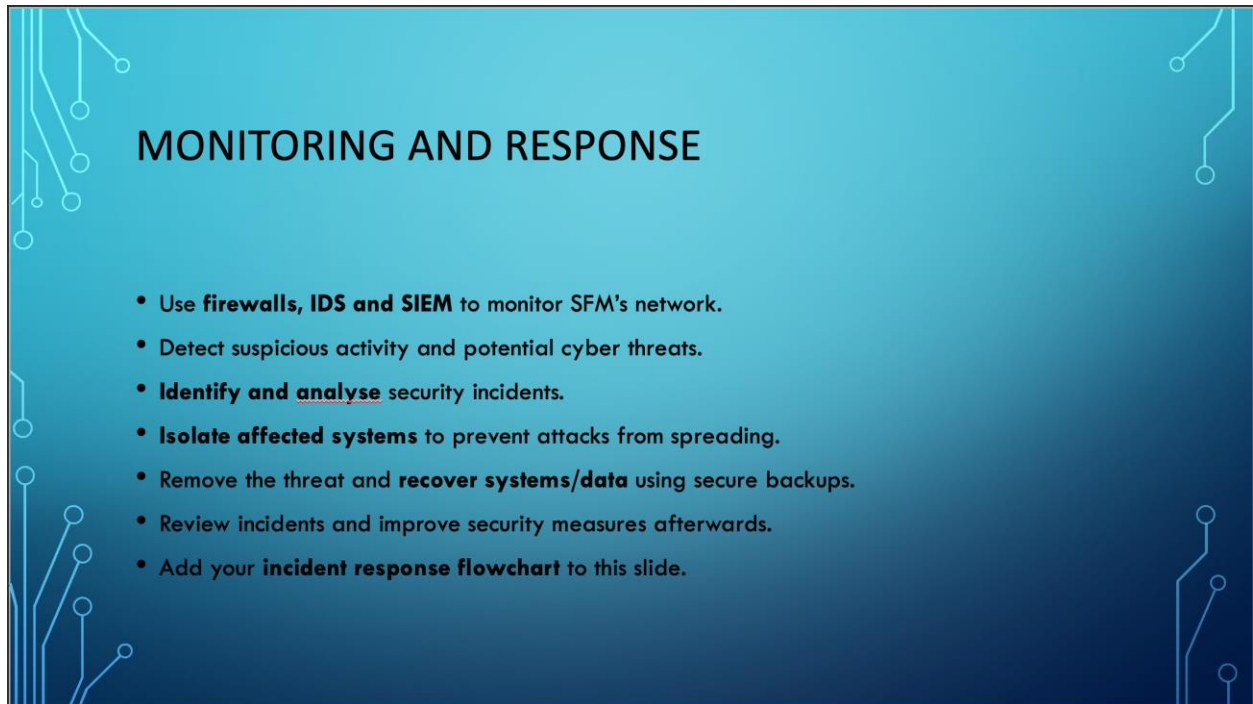
Slide 5



Slide 6



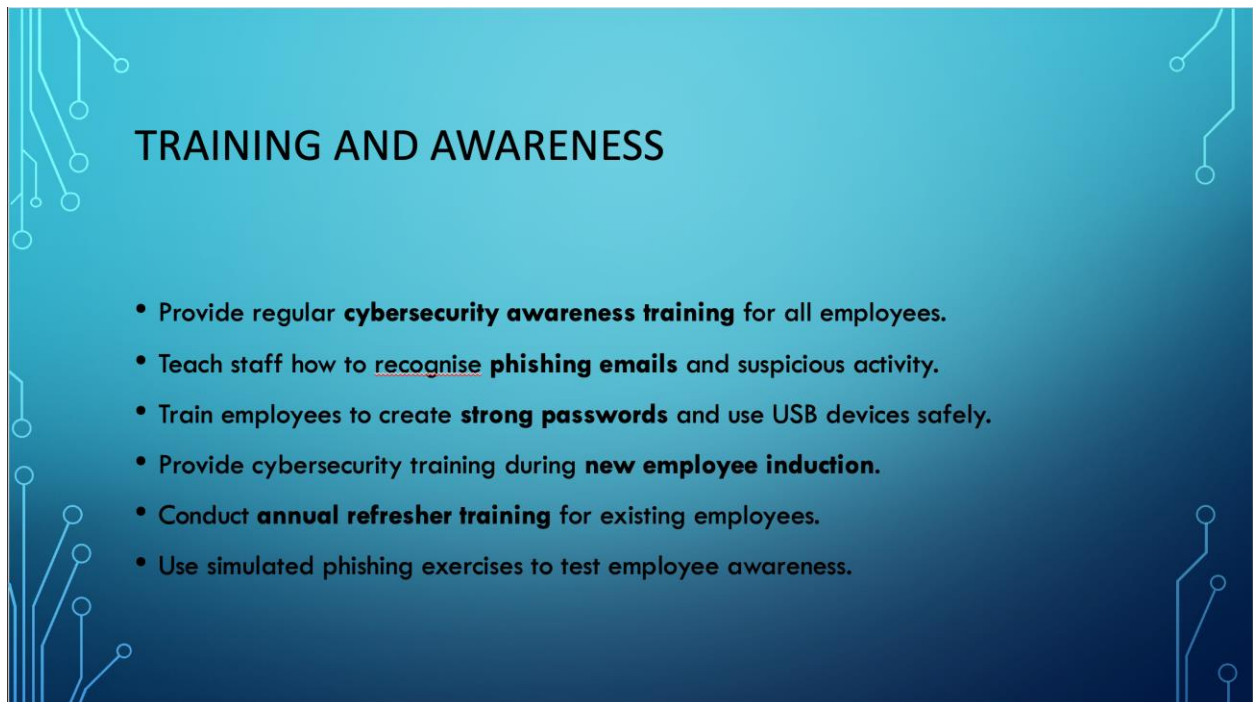
Slide 7



MONITORING AND RESPONSE

- Use **firewalls, IDS and SIEM** to monitor SFM's network.
- Detect suspicious activity and potential cyber threats.
- **Identify and analyse** security incidents.
- **Isolate affected systems** to prevent attacks from spreading.
- Remove the threat and **recover systems/data** using secure backups.
- Review incidents and improve security measures afterwards.
- Add your **incident response flowchart** to this slide.

Slide 8



TRAINING AND AWARENESS

- Provide regular **cybersecurity awareness training** for all employees.
- Teach staff how to **recognise phishing emails** and suspicious activity.
- Train employees to create **strong passwords** and use USB devices safely.
- Provide cybersecurity training during **new employee induction**.
- Conduct **annual refresher training** for existing employees.
- Use simulated phishing exercises to test employee awareness.

CONCLUSION

- Industry 4.0 provides benefits but also creates new cybersecurity risks.
- SFM faces both **internal and external cyber threats**.
- Strong security policies can reduce these risks.
- **MFA, network segmentation, backups and regular updates** improve protection.
- Continuous monitoring helps SFM detect and respond to attacks quickly.
- Employee training is essential for maintaining cybersecurity.
- Then you're basically **done with the presentation**.