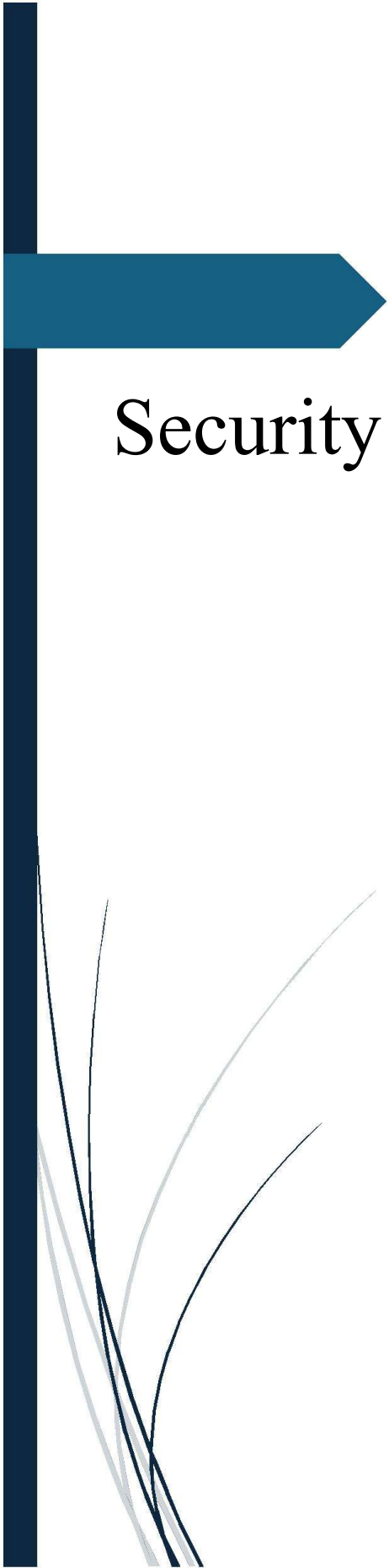




Security Networks and Cyber Essentials

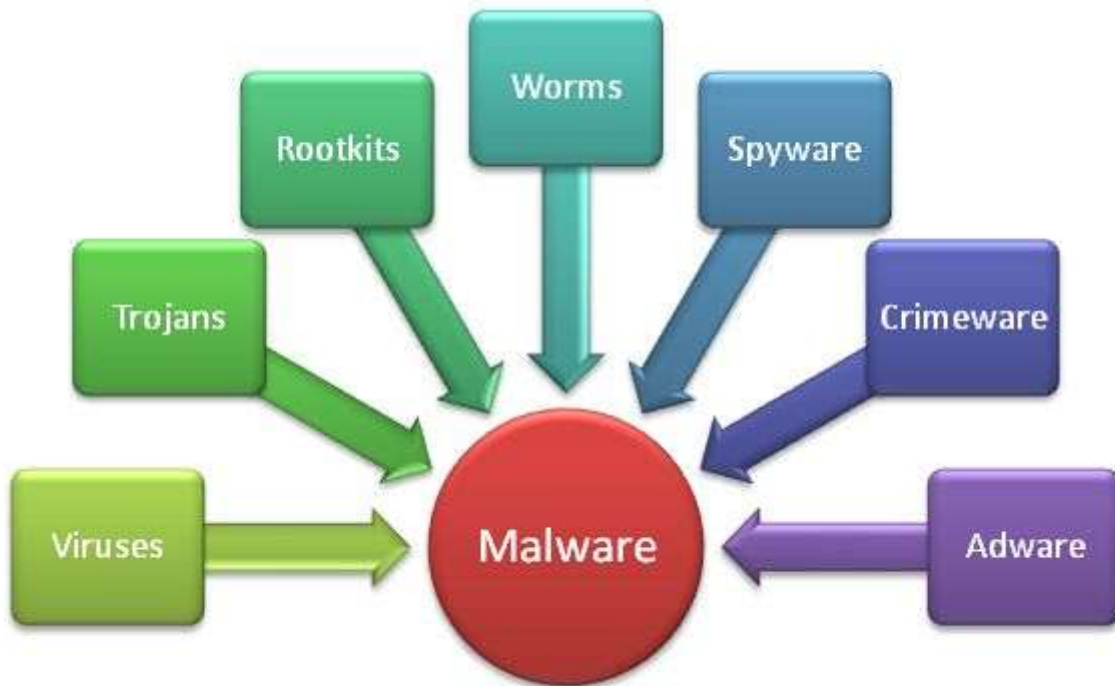
Pedro Claudio Martinez Almanzar
(2510674)

UNIVERSITY OF WALES TRINITY SAINT DAVID

Content

Identification of Threats	1
Security Policies.....	2
Mitigation Measures.....	3
Monitoring and Response.....	4
Training and Awareness.....	5

Introduction:



SteelForm Manufacturing Ltd relies increasingly on information technology, operational technology, IoT-enabled sensors, automated machinery and cloud-based production management systems. These technologies improve manufacturing efficiency but also increase SFM's exposure to cyber threats.

Recent malware infections, phishing attacks targeting procurement personnel and unauthorised attempts to access the production network demonstrate the need for a comprehensive cybersecurity and data governance framework.

1. Identification of Threats

should have simple but effective security policies to protect its computers, employees, production systems and company information.

1. Password and Access Policy

- Employees should use strong and unique passwords.
- MFA should be used for important accounts.
- Employees should only have access to the information they need.
- Accounts should be removed when an employee leaves the company.

2. Network Security Policy

- Use firewalls and antivirus software.
- Separate the office network from the production network.
- Secure Wi-Fi networks with strong passwords.
- Monitor unusual network activity.

3. Email and Phishing Policy

- Employees should not open suspicious links or attachments.
- Suspicious emails should be reported to IT.
- Staff should receive regular phishing-awareness training.
- Payment or supplier-bank changes should be verified before approval.

4. Data Protection Policy

- Important company information should only be stored on approved systems.

- Sensitive information should only be available to authorised employees.
- Important files should be encrypted and backed up.
- Company information should not be copied to personal devices or accounts.

5. Malware Protection Policy

- Computers should have updated antivirus/EDR software.
- Operating systems and applications should be regularly updated.
- Employees should not install unauthorised software or connect unknown USB devices.

6. Incident Response Policy

Employees must report security problems immediately. The IT team should investigate, isolate affected systems, remove the threat and restore systems from safe backups.

Step 1 – Identify: Find the company's important computers, data, IoT devices and production systems.

Step 2 – Protect: Use strong passwords, MFA, antivirus, firewalls, backups and employee training.

Step 3 – Monitor: Check networks and systems for suspicious activity.

Step 4 – Respond: If an attack happens, isolate the affected system and report the incident.

Step 5 – Recover: Restore affected systems from backups and check that they are secure.

Step 6 – Improve: After every incident, identify what went wrong and improve the security controls.

This plan would give SFM a practical starting point for reducing common risks such as phishing, malware, unauthorised access, data theft and production downtime.

2.Security Policies

The company should use simple security policies to protect its employees, data and production systems:

- Access Control: Use strong passwords and MFA. Employees only access information needed for their jobs.
- Network Security: Separate the office network from the production and IoT networks.
- Email Security: Train employees to recognise phishing emails and avoid suspicious links or attachments.
- Data Protection: Protect confidential engineering and customer information and make regular backups.
- Malware Protection: Keep antivirus, software and IoT devices updated.
- Incident Response: Report security problems quickly and isolate affected systems.
- Employee Training: Provide regular cybersecurity awareness training.

3.Mitigation Measures

We can reduce cybersecurity risks by using simple and practical measures:

Strong passwords and MFA: Protect employee and administrator accounts.

Regular updates: Keep computers, software and IoT devices updated.

Antivirus and firewall: Protect systems from malware and unauthorised access.

Employee training: Teach staff how to recognise phishing and suspicious emails.

Network separation: Keep the production network separate from the office network.

Regular backups: Backup important data to recover from ransomware or system failures.

Access control: Only allow employees to access the information they need.

Security monitoring: Check systems for unusual or suspicious activity.

Incident response: Have a simple plan for reporting and dealing with cyberattacks.

Regular security checks: Review security controls and identify weaknesses regularly.

4. Monitoring and Response

Should regularly monitor its network, computers and production systems for suspicious activity. Employees should report phishing emails, malware or unusual behaviour to the IT team.

If a security incident occurs, SFM should:

Detect the problem.

Report it to IT.

Isolate the affected system.

Remove the threat.

Recover using secure backups.

Review what happened and improve security.

5. Training and Awareness

Provide regular cybersecurity training to all employees. Staff should learn how to identify phishing emails, use strong passwords, protect company data and report suspicious activity. This helps reduce human errors and prevent cyberattacks.

Conclusion:

In conclusion, SteelForm Manufacturing Ltd faces several cybersecurity risks because of its increasing dependence on IT systems, cloud services, IoT devices and automated production equipment. The company's recent malware infections, phishing attacks and unauthorised access attempts show that cybersecurity should be treated as an important business priority.

The main threats include phishing, malware, ransomware, unauthorised access, insider threats, IoT vulnerabilities and industrial espionage. These threats could result in financial losses, stolen intellectual property, data breaches and disruption to manufacturing operations.

SFM can reduce these risks by implementing simple but effective controls such as strong passwords, MFA, firewalls, antivirus software, network separation, regular backups and employee training. Monitoring and a clear incident-response process will also help the company detect and respond to attacks more quickly.

Data governance is equally important because SFM holds valuable engineering, customer and production information. Controlling who can access this information and ensuring that sensitive data is securely stored and backed up can reduce the risk of data loss and industrial espionage.

Overall, SFM does not need to rely on a single security solution. A combination of technology, employee awareness, access controls, monitoring, data protection and regular security reviews will provide a stronger level of protection. By following the

proposed security plan and continuously improving its controls, SFM can reduce cyber risks while maintaining safe and reliable manufacturing operations.

References

1. National Institute of Standards and Technology (NIST). (2024). *The NIST Cybersecurity Framework (CSF) 2.0*.
[NIST Cybersecurity Framework 2.0](#)
2. International Organization for Standardization (ISO). *ISO/IEC 27001 — Information security management systems*.
ISO/IEC 27001
3. National Cyber Security Centre (NCSC). *Cyber Security Guidance*.
[NCSC – Cyber Security Guidance](#)
4. Cybersecurity and Infrastructure Security Agency (CISA). *Cybersecurity Best Practices*.
[CISA – Cybersecurity Best Practices](#)
5. International Electrotechnical Commission (IEC). *IEC 62443 – Industrial communication networks – Network and system security*.
IEC 62443 Industrial Cybersecurity