

1/8/2026

Assessment

MODULE NAME: NETWORK AND CYBERSECURITY ESSENTIALS

MODULE CODE: ACCA4024_LON

LECTURER: KOUSHIK MODAK

TRINITY SAINT DAVID UNIVERSITY OF WALES (LONDON CAMPUS)

Student Name: SINAN KYAZIM

STUDENT ID: 2513882

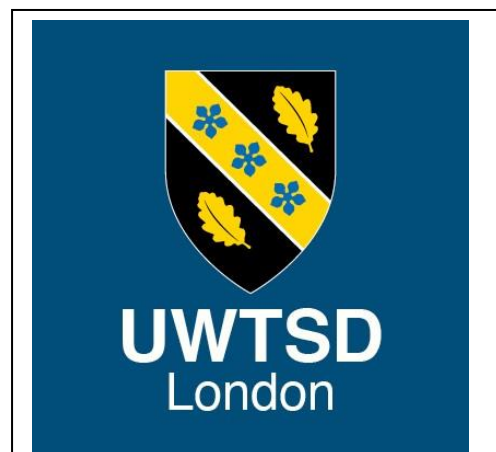


Table of Contents

Introduction	2
1. Identification of Threats	3
1.1 Internal Threats	3
1.2 External Threats.....	5
2. Security Policies	9
2.1 Password and Authentication Policy	10
2.2 Access Control Policy	10
2.3 Data Protection Policy.....	11
2.4 Software Update and Patch Management Policy.....	11
2.5 Backup and Recovery Policy	11
2.6 Acceptable Use Policy.....	11
2.7 Security Monitoring Policy	11
3. Mitigation Measures	11
3.1 Employee Security Awareness Training	11
3.2 Multi-Factor Authentication (MFA)	12
3.3 Network Segmentation.....	12
3.4 Endpoint Protection	13
3.5 Regular Vulnerability Assessments.....	13
3.6 Secure Backups	13
3.7 Supplier Security Checks	14
4. Monitoring and Incident Response	14
5. Staff Training and Awareness Program	15
Conclusion	15
References	16

Cybersecurity and Data Governance Policy for SteelForm Manufacturing Ltd

Introduction

Nowadays, technology is integrated into every aspect of business operations. Many factories use smart machines, cloud-based systems, and the Internet of Things (IoT) to meet the growing customer demand. The innovation and increased efficiency enabled by these technologies deliver results within a short period: production time and costs are reduced, output is increased, and the errors caused by human factors are minimised.



Figure 1. Smart machines in manufacturing industries (Source: [1])

The usage of innovative technologies and internet-based systems appears to be a good strategic decision, but also introduces a significant risk—cyberattacks. As, in most cases, all operations are connected through a centralised cloud-based system and managed from a single control point, so a single cyberattack may be sufficient to cause substantial damage. Such attacks can disrupt a company's production processes while also negatively affecting its economic performance, reputation, and public relations.

SteelForm Manufacturing Ltd (SFM) is a medium-sized company that produces engineering components for the automotive and aerospace industries. In recent years, the company has introduced IoT sensors, automated machines and a cloud-based production management system to improve the way it works. However, according to the case study, the company has already experienced several security problems, including malware infections, phishing emails and unauthorised attempts to access its production network.

While researching this topic, I realised that manufacturing companies are becoming one of the main targets for cybercriminals. If attackers manage to gain access to a company's manufacturing systems and engineering solutions, the organisation may suffer substantial financial losses arising from a variety of factors: cybercriminals may disrupt production systems, resulting in the manufacture of defective products. This can lead to the loss of raw materials and lost revenue due to the inability to sell the

productions; sensitive confidential information and operational models may also can be stolen and subsequently sold to competitors or exploited for the attackers own wellbeing; In addition, attackers may simply disrupt business operations by deleting critical data or rendering the entire system inoperable. Any of these scenarios could result in significant resource losses, economic decline, reputational damage, and, in extreme cases, the bankruptcy of the manufacturing company.

In my opinion, investing in cybersecurity measures and preventing cyberattacks is a far more effective management decision than attempting to recover losses after such an incident has already occurred.

The aim of this report is to identify the main cybersecurity threats that SteelForm Manufacturing Ltd may face and recommend practical security policies to reduce these risks. The report also discusses possible mitigation measures, an incident response plan and a staff training program based on recognised standards such as ISO 27001, the NIST Cybersecurity Framework and GDPR.

1. Identification of Threats

Like many modern manufacturing companies, SteelForm Manufacturing Ltd faces different types of cybersecurity threats. Some of these threats come from inside the company, while others come from hackers or criminal groups outside the organisation. During my research, I noticed that many successful cyberattacks happen because companies focus only on external hackers and forget that employees can also create security risks.

1.1 Internal Threats

Cybersecurity risks faced by organisations generally arise from two main categories of threats: internal and external.

Internal threats typically originate from employees or any individual who has authorised access to the company's systems. Some authors refer to these individuals as malicious or careless users and classify their actions into the following categories: fraud, IT sabotage, intellectual property theft, espionage, and unintentional actions (resulting from carelessness, which may also lead to serious security breaches). [2]

Human factor

The most common internal threat is generally considered to be human error. Organizational security professionals are worried about workers with low-security awareness who can accidentally give access to trickery hackers. [3]



Figure 2. Origins of the cyberattacks (source: [4])

One of the simplest examples of unintentional actions carried out by employees with a low level of security awareness is receiving an email in their corporate inbox that appears to have been sent by a trusted business partner. If the employee opens the email and downloads the attached files, or clicks on a link to download them without carefully verifying its authenticity, malware may be installed on the device and subsequently gain access to the company's network. This directly compromises the organisation's cybersecurity, creating risks such as the loss of critical business data, financial fraud, misuse and theft of sensitive data, as well as disruption the daily manufacturing and operational activities.

Sometimes current or former employees misuse their access to company systems too. This may happen because they want financial gain, feel unhappy with the company or simply ignore security rules. For a company like SFM, this could include stealing engineering drawings, customer information or production data before leaving the organisation. Since these designs are valuable, insider threats should not be ignored.

Weak Passwords

Weak passwords are still one of the easiest ways for attackers to gain access to company accounts. Some employees use easy passwords such as „Password123“ or reuse the same password for different systems. If an attacker discovers one password, they may be able to access several company services, especially if multi-factor authentication is not enabled.

Unpatched Systems

Software developers regularly release security updates to fix newly discovered vulnerabilities. If these updates are ignored, cybercriminals can take advantage of these weaknesses to attack company systems.

To prevent internal cybersecurity threats, SFM should implement enhanced monitoring and control mechanisms. An effective Insider Threat Program should incorporate a range of best practices designed to minimise the overall level of risk. These should include administrative controls, technical controls, physical controls, security awareness training, and a well-defined incident response capability. [2]

1.2 External Threats

External threats are cyber risks that come from outside the company. These attacks are usually carried out by hackers, cybercriminals or organised groups looking to steal information, make money or disrupt business operations. According to the “Global Cybersecurity Outlook 2026” report 73% of respondents reported that they or someone in their network had been personally affected by cyber-enabled fraud over the course of 2025. [5] Since SFM relies on internet-connected systems and cloud technology, external attacks could have a serious impact on both production and business performance.

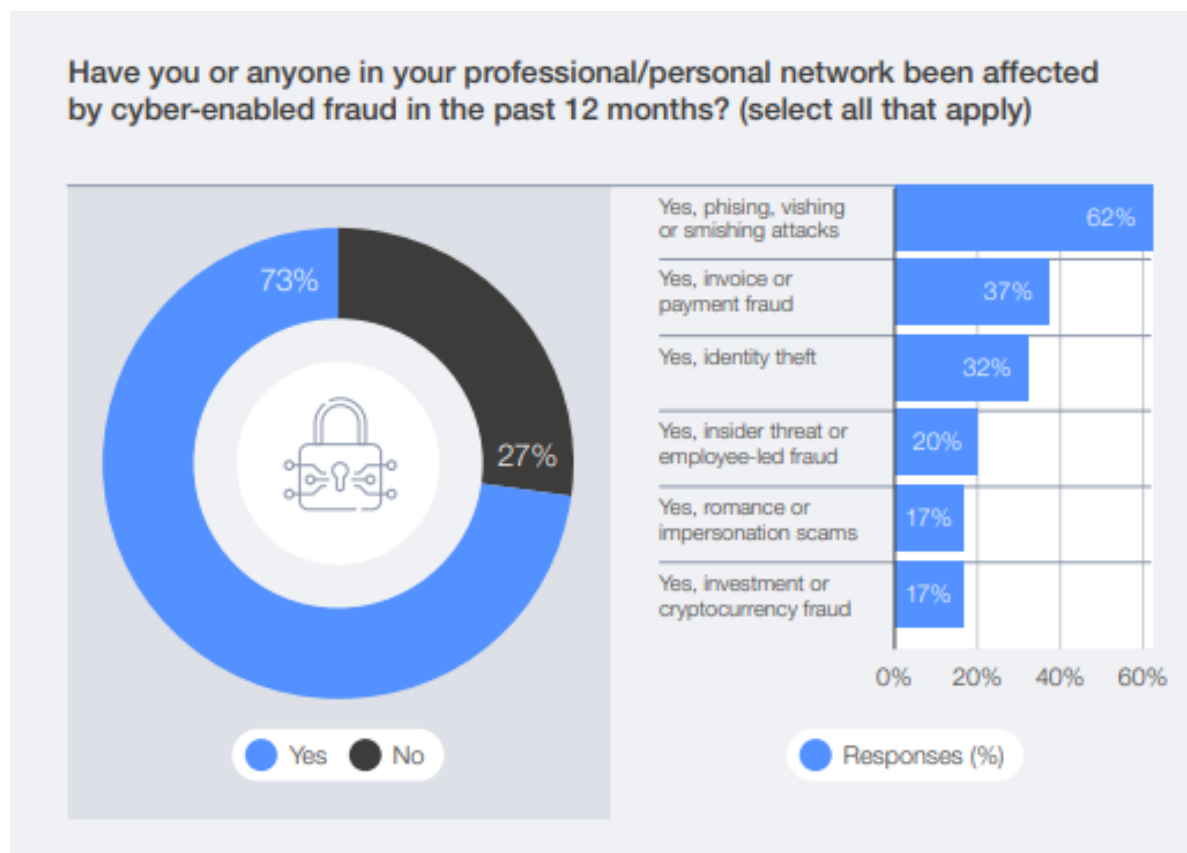


Figure 3. Global Cybersecurity Outlook 2026 survey (source: [5])

Phishing Attacks

In 2026 Cyber-enabled fraud and phishing remain the top cybersecurity concerns for CEOs of insufficiently resilient organizations. [5] Attackers send fake emails pretending to be trusted organisations, suppliers or banks to trick employees into clicking malicious links or sharing sensitive information.

As the company has already experienced phishing emails targeting the Procurement Department, it can be assumed that cybercriminals have identified a vulnerable point. If a phishing attack is successful, the company may suffer a range of consequences, depending on the severity of the incident. These may include compromised user credentials, the theft of sensitive contacts, confidential business data, and customer information; financial fraud; installation of malware on the company's computers; and unauthorised access to critical business systems.

Ransomware

Ransomware is a type of malware that encrypts files and prevents users from accessing them until a ransom is paid. [6] Manufacturing companies are common targets because they typically operate on a continuous production basis. This means that even a few hours of partial or complete disruption to production can result in significant financial losses, including delayed orders and lost revenue.

If SFM became a victim of ransomware, production could stop completely while IT staff work to recover the systems. During my research, I found that many organisations choose not to pay the ransom because there is no guarantee that attackers will restore the data. [7] For this reason, prevention and regular backups are much more reliable than paying cybercriminals.

Industrial Espionage

Industrial espionage involves stealing confidential business information such as engineering designs, production methods or customer contracts. [2] Since SFM manufactures custom components for the automotive and aerospace industries, its technical data is valuable and could be targeted by competitors or organised cybercriminals. Their information is critical and once stolen, the company could lose its competitive advantage and customers might lose confidence in its ability to protect sensitive data.

Supply Chain Attacks

SFM works closely with suppliers, software providers and other business partners. If one of the business partners falls victim to a cyberattack, the attackers may exploit the trusted relationship between the two organisations to gain unauthorised access to SFM's systems and obtain sensitive information. For example, a software supplier could

unknowingly distribute an infected update, allowing malware to enter the company's systems. This type of attack has become more common in recent years because attackers know that suppliers are often trusted automatically. The possible consequences include: malware entering the network; data breaches; increased recovery costs.

Distributed Denial of Service (DDoS)

Distributed Denial of Service (DDoS) flooding attacks are one of the biggest concerns for security professionals.

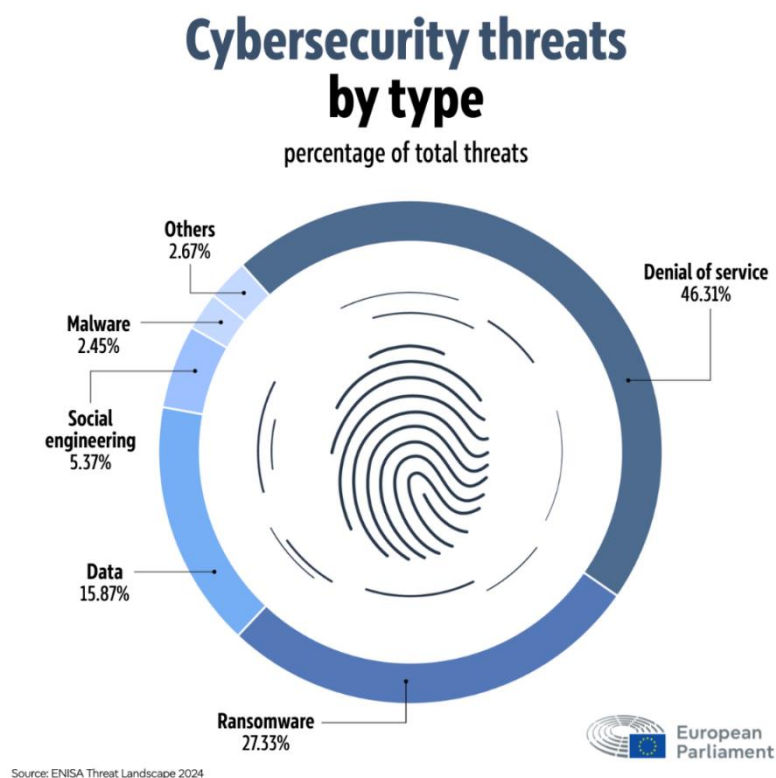


Figure 4. DDoS percentage part of the all threats (Source: [8])

DDoS flooding attacks are typically explicit attempts to disrupt legitimate users' access to services. [9] Basically this is a cyberattack in which multiple compromised devices simultaneously send excessive volumes of traffic or service requests to a target system with the intention of exhausting its resources and rendering its services unavailable to legitimate users. There are 3 main types of DDoS:

Volumetric attacks

Volumetric attacks are the most common type of DDoS attack. Their objective is to consume the target's available network bandwidth by overwhelming it with extremely large volumes of malicious traffic, preventing legitimate users from accessing online services. [10]

Protocol Attacks

Protocol attacks cause a service disruption by over-consuming server resources and/or the resources of network equipment like firewalls and load balancers.

Application layer attacks

The goal is to overwhelm the target with requests, since a single HTTP request can be expensive for the target server to respond to. For example: attackers establish numerous HTTP connections but intentionally keep them open by sending incomplete requests, gradually exhausting the web server's available connection pool. [11]

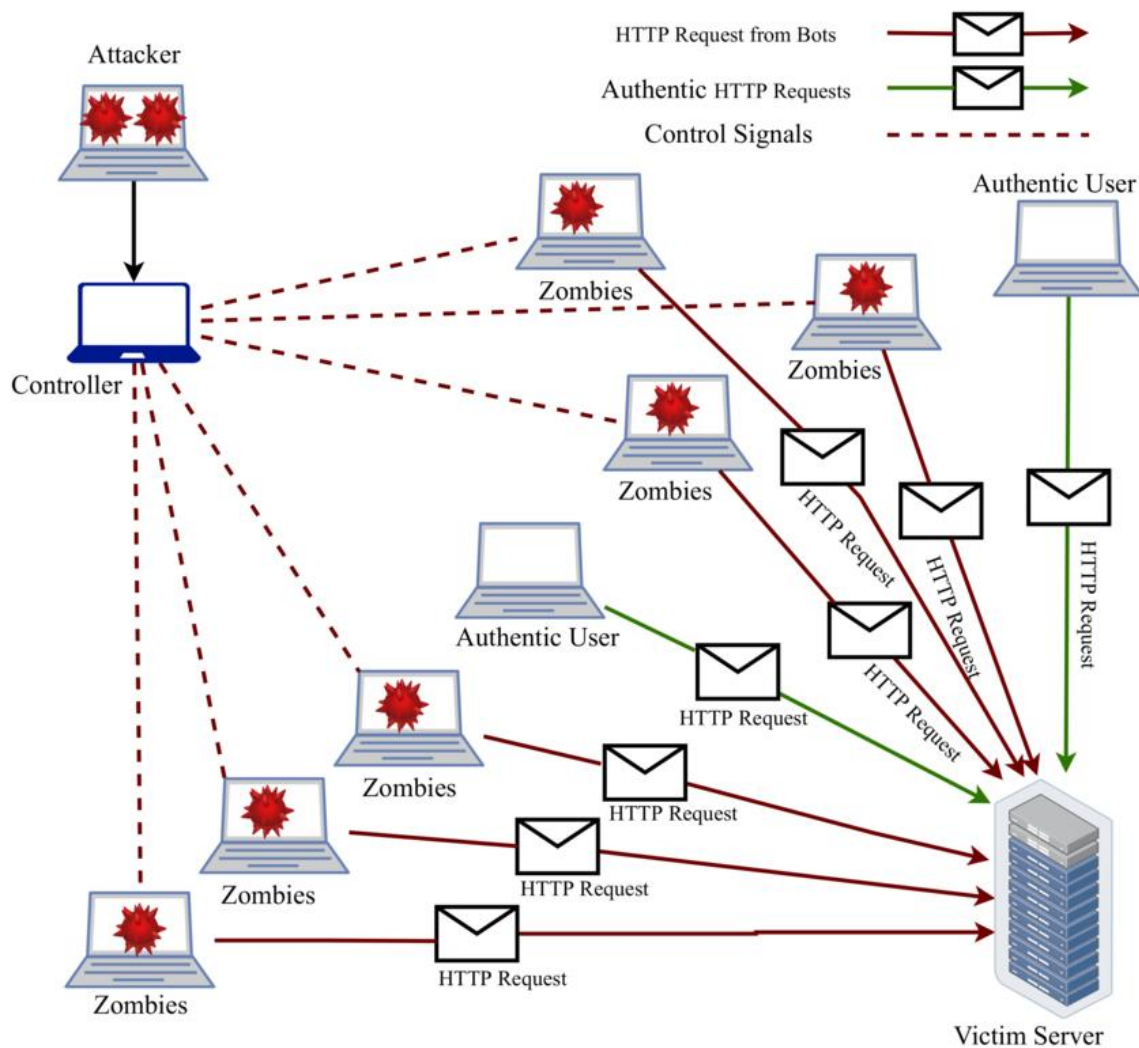


Figure 5. Schematic diagram of a DDoS attack (source: [12])

Such attacks can have serious consequences for manufacturing companies that operate on a continuous production basis. These may include the inability of customers to place orders, disruption of communication between business systems, and delays to production processes. Consequently, organisations may incur financial losses amounting to thousands of pounds.

DDoS attacks are particularly difficult to mitigate because the malicious traffic originates from a vast number of compromised devices located across the world, each using different IP addresses and typically forming part of a botnet infected with malware.

To reduce the risk of such attacks, SFM should implement a range of preventative security measures, including Web Application Firewalls (WAFs), rate limiting to restrict the number of requests from a single IP address, continuous network traffic monitoring, and dedicated DDoS protection services, such as Cloudflare or Akamai, in line with Open Web Application Security Project (OWASP) recommendations for layered security and denial-of-service mitigation. The table below summarises the main internal and external threats facing SteelForm Manufacturing Ltd and the overall level of risk they present.

Threat	Type	Risk Level
Phishing	External	High
Malware	External	High
Ransomware	External	Very High
Insider Threat	Internal	High
Human Error	Internal	High
Weak Passwords	Internal	Medium
Unpatched Software	Internal	High
Supply Chain Attack	External	High
Industrial Espionage	External	Very High
DDoS Attack	External	Medium

Table 1. Internal and external threats

2. Security Policies

During my research, I noticed that many successful companies follow international standards such as ISO 27001 which is the world's best known standard for information security management systems. [13] The implementation of ISO standards within an organisation and its business operations is essential, as they provide a standardised framework for information security and ensure that the organisation follows the best practices and principles established by the International Standard. In addition, ISO certification enhances customer trust by demonstrating the organisation's commitment to maintaining high standards. However, obtaining certification to ISO/IEC 27001 may represent a significant financial investment for some manufacturing companies. Depending on the size, complexity, and operational capacity of the organisation, certification costs may exceed £10,000.

There is the NIST Cybersecurity Framework too - voluntary set of guidelines, standards, and best practices created by the National Institute of Standards and Technology to help organizations manage and reduce cybersecurity risk. Their framework contains the following steps: identify, protect, detect, respond, recover.



Figure 6. Cybersecurity framework (source: [14])

2.1 Password and Authentication Policy

One of the simplest ways to improve security is by creating stronger password rules. Employees should create passwords that are at least 12 characters long and include uppercase letters, lowercase letters, numbers and special symbols. Passwords should never be shared with colleagues or written down where other people can see them. In addition, Multi-Factor Authentication (MFA) should be enabled for all important systems, especially cloud services and administrator accounts. Even if a password is stolen, MFA provides an extra layer of protection before an attacker can gain access.

2.2 Access Control Policy

With the growing threat of cyberattacks, it is essential for organisations to implement measures aimed at minimising internal cybersecurity risks. The Principle of Least Privilege (PoLP) and Segregation of Duties (SoD) are two fundamental security principles that, when properly implemented, can significantly reduce organisational risk. [15]

Not every employee needs access to all business systems. Instead, access permissions should be granted according to each employee's specific role and responsibilities. For example, production staff should have access only to manufacturing systems, while employees in the Procurement Department should be restricted to the systems required for their day-to-day responsibilities.

Both principles are designed to minimise the risk of unauthorised access, human error, and malicious activities that may result in security breaches, fraud, or operational disruptions.

2.3 Data Protection Policy

SFM stores different types of sensitive information, including customer records, engineering drawings, financial information and employee details. This information should always be protected using encryption. This policy also supports GDPR requirements by helping to protect personal data from unauthorised access.

2.4 Software Update and Patch Management Policy

Outdated software often contains security vulnerabilities that hackers already know about. SFM should regularly update operating systems, production software, antivirus programs and IoT devices. Critical security updates should be installed as soon as possible after they are released.

2.5 Backup and Recovery Policy

Backups should be created automatically day-to-day and have to be stored in a secure locations, including offline or cloud copies too. This policy will help the company recover quickly after ransomware attacks or hardware failures.

2.6 Acceptable Use Policy

Employees should be made fully aware of the organisation's information security policies and their responsibilities for complying with them. These policies should include, among other measures, prohibiting the installation of unauthorised software, the use of personal USB storage devices, and access to unsafe or untrusted websites using company's equipment.

2.7 Security Monitoring Policy

SFM should continuously monitor its network for unusual activity. Security logs from servers, cloud services and IoT devices should be reviewed regularly so that suspicious behaviour can be detected quickly. The Security monitoring policies also support the three main principles of the CIA Triad: confidentiality, integrity, availability.

3. Mitigation Measures

SFM needs practical measures to prevent the risks. These controls should be realistic, affordable and suitable for a medium-sized manufacturing company like SFM.

3.1 Employee Security Awareness Training

When addressing the human factor in cybersecurity, it is important to recognise that there are various measures that can be implemented to prevent errors and strengthen security awareness.

One of the most effective steps that SFM can take is to provide regular cybersecurity training and awareness programs for its employees. [16] Topics such as phishing awareness and the safe use of company software and hardware should be considered essential and delivered at least once a year.

In addition to formal training sessions, SFM should implement ongoing security awareness campaigns, including educational posters, email messages, surveys, and simple online quizzes. These initiatives encourage employees to assess their own cybersecurity knowledge, reinforce good security practices, and promote a security-conscious organisational culture.

3.2 Multi-Factor Authentication (MFA)

MFA should be enabled on all important company accounts, especially cloud services, email accounts and administrator accounts. Even if attackers steal a password through phishing, they will still need a second verification method before accessing the account.

3.3 Network Segmentation

SFM should separate its office network from its production systems and IoT devices. This means that if malware infects an office computer, it will be much harder for the attack to spread to factory equipment.



Figure 7. Difference between segmented and unsegmented network diagram (source: [17])

3.4 Endpoint Protection

Every company computer and server should have modern antivirus and Endpoint Detection and Response (EDR) software installed. These tools can detect and prevent cyberattacks.

3.5 Regular Vulnerability Assessments

As part of the previous step - Endpoint Protection, SFM should regularly scan its systems to identify security weaknesses before attackers find them. Any vulnerabilities should be prioritised according to their level of risk and fixed as quickly as possible.

3.6 Secure Backups

Important company information should be backed up every day. To improve security, SFM should follow the “3-2-1 Backup Rule”: store three copies of any important file (a primary and two backups); the file should be stored on two different media types (for example: a hard drive and optical media) and one copy should be stored off-site. Numerous recommendations have been developed based on this principle, all of which aim to protect critical data and facilitate its recovery in the event of a security incident. [18]

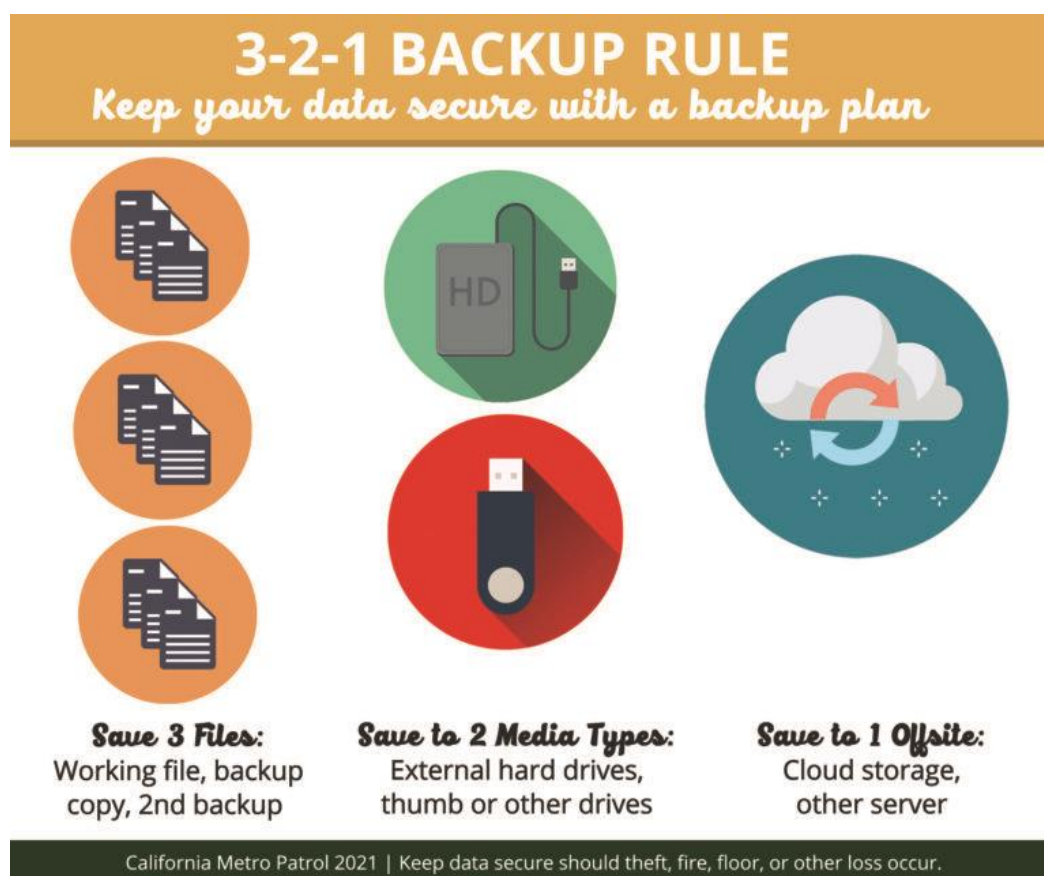


Figure 8. “3-2-1 backup rule” scheme (source: [19])

3.7 Supplier Security Checks

As SFM works with external contractors and suppliers of goods and services, the company should be careful when selecting its business partners and prioritise organisations that demonstrate a strong cybersecurity culture. SFM should establish business relationships with suppliers that are certified to ISO/IEC 27001, as such organisations have implemented internationally recognised information security management practices and have undergone independent certification.

Threat	Mitigation Measure
Phishing	Staff training, MFA, email filtering, awareness campaigns
Ransomware	Secure backups, EDR, software updates
Weak Passwords	Strong password policy, MFA
Insider Threats	Access control, user monitoring
Supply Chain Attacks	Supplier security assessments
Unpatched Systems	Regular patch management
DDoS Attacks	Firewalls, network monitoring and cloud protection

Table 2. Summary of Mitigation Measures

Overall, these mitigation measures are practical for a medium-sized manufacturing company like SFM. They can greatly reduce cyber risks and help the company continue operating even if an attack occurs.

4. Monitoring and Incident Response

The IT team of SFM should regularly monitor network traffic, system logs and cloud services for any unusual activity. Security tools such as firewalls, antivirus software and intrusion detection systems will help identify and prevent threats. According to Eric Thompson, If a cyber incident is detected, the companies should follow the following steps: [20]

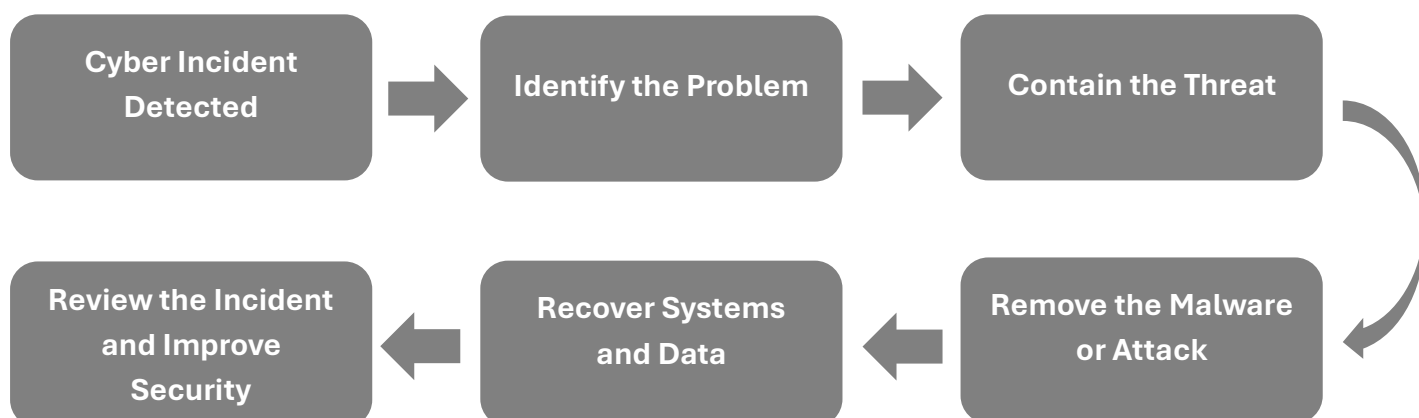


Figure 9. Incident Response Process scheme

After each incident, the IT team should investigate what happened and identify ways to prevent similar attacks in the future. In my opinion, learning from previous incidents is one of the best ways to improve cybersecurity over time.

5. Staff Training and Awareness Program

Since many cyberattacks are caused by human factor, regular training should be an important part of SFM's cybersecurity strategy. New employees should receive cybersecurity training during their induction, and all staff should complete refresher training at least once a year so they can evaluate their cybersecurity culture.

Organising ongoing security awareness campaigns by creating educational posters, reminder emails, surveys, and short online quizzes is an effective way to reinforce employees cybersecurity awareness and assess their understanding of good security practices in the workplace. I believe that regular training will help employees feel more confident and reduce the number of security incidents caused by simple mistakes.

Conclusion

Cybersecurity has become an integral component of modern business strategies, as companies across both the manufacturing and service sectors increasingly rely on advanced technologies, extensive internet connectivity, artificial intelligence, and cloud-based systems. While these innovations significantly enhance productivity, efficiency, and operational performance, they also introduce substantial cybersecurity risks that must be carefully identified, assessed, and managed.

Overall, I believe that the company (SFM) from the case study can significantly improve its cybersecurity by combining strong security policies, regular employee training and continuous monitoring.

References

[1]	N. -. Blog, "Industry 4.0 – What, why, examples?," Nexelem, [Online]. Available: https://nexelem.com/en/blog/industry-4-0/ . [Accessed 31 07 2026].
[2]	A. D. J. Guerrino Mazzarolo, "Insider threats in Cyber Security: The enemy within the gates.," School of Computer Science, University College Dublin, Ireland, Dublin, Ireland, 2019.
[3]	L. Q. a. S. C. L. Xiangyu, "Social Engineering and Insider Threats," International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), 2017.
[4]	ReferralRock, "The Top 5 Cybersecurity Threats for Digital Marketers," ReferralRock, [Online]. Available: https://referralrock.com/blog/cybersecurity-threats-for-digital-marketers/ . [Accessed 31 07 2026].
[5]	E. W. W. B. K. H. a. e. Giulia Moschetta, "Global Cybersecurity Outlook 2026 Insight Report January 2026," 2026.
[6]	A. D. P. Jinal P. Tailor, "A Comprehensive Survey: Ransomware Attacks: Prevention, Monitoring and Damage Control," <i>International Journal of Research and Scientific Innovation (IJRSI)</i> , June 2017.
[7]	T. S. T. L. D. X. P. W. D. L. Y. H. A. N. M. H. Timothy McIntosh, "Ransomware Reloaded: Re-examining Its Trend, Research and Mitigation in the Era of Data Exfiltration," <i>ACM Computing Surveys</i> , 2024.
[8]	E. Parliament, "Cybersecurity: main and emerging threats," European Parliament, [Online]. Available: https://www.europarl.europa.eu/topics/en/article/20220120STO21428/cybersecurity-main-and-emerging-threats . [Accessed 31 07 2026].
[9]	S. T. Zargar, J. Joshi and D. Tipper, "A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks," <i>IEEE</i> , 2013.
[10]	C. L. Center, "What is a DDoS attack?," CloudFlare, [Online]. Available: https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/ . [Accessed 31 07 2026].
[11]	OWASP, "Denial of Service Cheat Sheet," OWASP, [Online]. Available: https://cheatsheetseries.owasp.org/cheatsheets/Denial_of_Service_Cheat_Sheet.html . [Accessed 31 07 2026].
[12]	M. F. M. ,. A. H. ,. M. S. F. ,. D. J. ,. I. A. Furqan Rustam, "Denial of Service Attack Classification Using Machine Learningwith Multi-Features," [Online]. Available: https://www.researchgate.net/publication/365618619_Denial_of_Service_Attack_Classification_Using_Machine_Learning_with_Multi-Features . [Accessed 31 07 2026].
[13]	ISO, "ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements," ISO, [Online]. Available: https://www.iso.org/standard/27001 . [Accessed 31 07 2026].
[14]	NIST, "Cybersecurity Framework," NIST, [Online]. Available: https://csrc.nist.gov/projects/cybersecurity-framework/filters#/csf/filters . [Accessed 01 08 2026].
[15]	A. Abbas, "Maximizing Security with the Policy of Least Privilege and Segregation of Duties in Organizations," 09 2024. [Online]. Available:

	https://www.researchgate.net/profile/Asad-Abbas-41/publication/384355851_Maximizing_Security_with_the_Policy_of_Least_Privilege_and_Segregation_of_Duties_in_Organizations/links/66f563dfb753fa724d4935a4/Maximizing-Security-with-the-Policy-of-Least-Privileg . [Accessed 01 08 2026].
[16]	E. U. Ş. E. Mete Eminağaoğlu, "The positive outcomes of information security awareness training in companies – A case study," <i>Information Security Technical Report, Volume 14, Issue 4</i> , pp. 223-229.
[17]	D. Teplinskiy, "How to Master Network Segmentation for Manufacturing," ACIS Alpha Cis, [Online]. Available: https://www.alphacis.com/how-to-master-network-segmentation-for-manufacturing/ . [Accessed 01 08 2026].
[18]	D. McCaffrey, "Evolving the 3-2-1 backup rule for more resilient data," [Online]. Available: https://publishing.escholarship.umassmed.edu/jeslib/article/id/1174/ . [Accessed 01 08 2026].
[19]	C. M. Patrol, "3-2-1 Backup Rule: Keeping Your Data Secure," California Metro Patrol, [Online]. Available: https://californiametropatrol.com/commercial-security/3-2-1-backup-rule-keeping-your-data-secure/ . [Accessed 01 08 2026].
[20]	E. C. Thompson, <i>Cybersecurity Incident Response: How to Contain, Eradicate, and Recover from Incidents</i> , Illinois, USA: Apress, 2018.