

Details	Information
---------	-------------

Student Name	Eulalio Fernandes
--------------	-------------------

Student ID	2441942
------------	---------

Module	ACCA4024 – Networks and Cyber Security Essentials
--------	---

Subject	Cybersecurity and Data Governance
---------	-----------------------------------

Assignment Title	Synthesize a solution to a potential real life scenario
------------------	---

Lecturer	Amit Naik
----------	-----------

Contents

1. Introduction :	4
-------------------------	---

2. Identification of Cybersecurity Threats	4
3. Cybersecurity and Data Governance Policies	6
3.1 Access Control and Authentication Policy	6
3.2 Network and Operational Technology Security Policy	6
3.3 Data Governance and Classification Policy	7
3.4 Acceptable Use and Email Security Policy	7
3.5 Vulnerability and Patch Management Policy	7
3.6 Incident Response and Reporting Policy	7
3.7 Supplier and Third-Party Security Policy	7
3.8 Backup, Recovery and Business Continuity Policy	8
4. Mitigation Measures and Implementation	8
4.1 Network Segmentation	8
4.2 Multi-Factor Authentication and Access Control	8
4.3 Endpoint and Malware Protection	8
4.4 Vulnerability and Patch Management	9
4.5 Secure Backup and Recovery	9
4.6 Email and Phishing Protection	9
4.7 IoT and OT Security	9
4.8 Implementation Roadmap	9
5. Monitoring and Incident Response	10
5.1 Continuous Security Monitoring	10
5.2 Incident Detection and Triage	10
5.3 Incident Response Process	11
5.4 Roles and Responsibilities	13
5.5 Incident Testing and Improvement	13
6. Staff Training and Security Awareness Programme	13
6.1 Core Cybersecurity Awareness Training	14
6.2 Role-Based Training	14
6.3 Phishing Simulations and Practical Exercises	14
6.4 Training Schedule	15
6.5 Measuring Training Effectiveness	15
7. Conclusion :	16

References :.....	16
-------------------	----

1. Introduction :

The integration of Industry 4.0 has enhanced the interrelation among information technology (IT), operational technology (OT), Internet of Things (IoT) gadgets, and cloud services, rendering cybersecurity crucial for contemporary production. SteelForm Manufacturing Ltd (SFM), a mid-sized enterprise specialising in bespoke-engineered parts for the automotive and aerospace industries, employs IoT-integrated sensors, automated equipment, and a cloud-driven production management system. While these technologies enhance operational efficacy, they may simultaneously heighten vulnerability to cyber threats (NCSC, 2026). SFM has encountered malware infestations, phishing assaults aimed at procurement personnel, and unauthorised efforts to infiltrate its manufacturing network. These assaults may lead to interruptions in production, monetary losses, theft of intellectual property, data compromises, and harm to reputation. This document delineates SFM's principal internal and external vulnerabilities and recommends cybersecurity protocols, risk mitigation strategies, surveillance, incident management, and employee training to enhance the organization's security and resilience.

2. Identification of Cybersecurity Threats

SteelForm Manufacturing Ltd (SFM) functions within a cohesive ecosystem that encompasses IT, OT, IoT devices, and cloud services. While this facilitates production and economic activities, it concurrently heightens cybersecurity vulnerabilities. Assaults may impact information systems, production capabilities, equipment accessibility, and operational continuity. NIST emphasises the necessity of safeguarding industrial control systems from cybersecurity risks (Stouffer et al., 2019; NIST, 2022).

2.1 Outside Dangers

Ransomware poses a considerable danger as it can impede access to systems and information, thereby disrupting operations and impacting technical and customer data. It might also encompass data larceny and intimidation to reveal pilfered information (NCSC, 2026).

Phishing and social engineering pose significant threats since SFM has already encountered phishing emails aimed at procurement personnel. Perpetrators could masquerade as vendors or executives to acquire credentials or sensitive data. Malware may infiltrate via fraudulent emails, contaminated devices, breached websites, or susceptible software, and might disseminate throughout IT, OT, and IoT infrastructures.

Industrial espionage poses a significant threat as SFM possesses crucial technological designs, manufacturing information, and intellectual property. Rivals might seek to get this data, undermining SFM's competitive edge. Supply-chain assaults can transpire via breached vendors, software, or third-party remote access, underscoring the significance of supplier security (NIST, 2025). Attacks on IoT and OT can leverage feeble passwords, obsolete software, or insecure connections, thereby interrupting production.

2.2 Intrinsic Hazards

Internal dangers might be deliberate or unintentional. A nefarious employee might appropriate sensitive information, or inadvertent exposure could happen if secret data is transmitted to an incorrect destination. Human mistakes, such as inadequate passwords, phishing attempts, unauthorised software, and unapproved devices, may jeopardise systems.

Overly broad access rights amplify the potential consequences of breached accounts.

SFM ought to implement the principle of least privilege, granting employees only the access necessary for their positions.

2.3 Possible Effects on Sustainable Forest Management

These hazards may result in operational interruptions, monetary losses, data compromises, theft of intellectual property, and harm to reputation. Given that SFM serves the automotive and aerospace industries, cybersecurity represents a significant commercial and operational risk, extending beyond mere IT issues.

Yes. For **Section 3**, we can reduce it to about **400–450 words** while keeping all 8 policies and the important meaning.

3. Cybersecurity and Data Governance Policies

SFM should implement a structured cybersecurity and data governance framework based on recognised security principles. The NIST Cybersecurity Framework (CSF) 2.0 provides a suitable basis through **Govern, Identify, Protect, Detect, Respond and Recover** (NIST, 2024). The policies should apply to employees, contractors, suppliers, IT, OT, IoT and cloud systems to protect SFM's data and production operations.

3.1 Access Control and Authentication Policy

SFM should apply **least privilege** and role-based access control, giving employees only the permissions required for their roles. MFA should be required for cloud services, remote access and privileged accounts. User accounts should be unique, reviewed regularly and removed when employees leave or change roles (NIST, 2026).

3.2 Network and Operational Technology Security Policy

SFM should separate corporate IT from OT and manufacturing networks. Network segmentation, firewalls and controlled communication should separate IT, OT and IoT systems. Remote production access should be restricted, authorised and protected with strong authentication. Security controls should also consider industrial reliability and safety requirements (NIST, 2020).

3.3 Data Governance and Classification Policy

SFM should classify information as **Public, Internal, Confidential or Highly Confidential**. Sensitive information, including engineering designs, intellectual property, production specifications and customer information, should have restricted access and encryption. Appropriate retention and secure disposal procedures should also be established.

3.4 Acceptable Use and Email Security Policy

Employees should follow rules for company computers, email, cloud services and removable media. Unauthorised software and devices should not be used. Procurement staff should verify unusual payment requests, links, attachments and supplier bank-detail changes. Email filtering, malware detection and MFA should support these controls.

3.5 Vulnerability and Patch Management Policy

SFM should maintain an inventory of hardware and software and regularly assess vulnerabilities. Security updates should be prioritised according to risk and asset importance. Patches affecting production machinery should be tested before deployment. Where patching is delayed, network isolation or increased monitoring should be used.

3.6 Incident Response and Reporting Policy

Employees should immediately report phishing, malware, unauthorised access, lost devices and suspected data breaches. The policy should define responsibilities for detection, containment, investigation, recovery and communication. An incident register should record incidents and lessons learned.

3.7 Supplier and Third-Party Security Policy

Suppliers, contractors and cloud providers should be assessed before receiving access to SFM systems or information. Contracts should include cybersecurity requirements, access restrictions and incident-reporting obligations. Third-party access should be reviewed regularly and removed when no longer required.

3.8 Backup, Recovery and Business Continuity Policy

SFM should regularly back up critical business and production information and protect backups from unauthorised modification. Restoration should be tested periodically, and recovery priorities should be established for critical systems. These measures can reduce the impact of ransomware and other disruptive incidents (NIST, 2026).

4. Mitigation Measures and Implementation

SFM should support its cybersecurity policies with practical technical and organisational controls. Measures should be prioritised according to identified risks while protecting information systems and manufacturing operations. OT security measures must also consider reliability, performance and safety requirements (NIST, 2024).

4.1 Network Segmentation

SFM should separate corporate IT from OT and manufacturing networks. IoT devices should operate in controlled network segments, with firewalls regulating communication between IT, OT and IoT environments. This can limit attackers' ability to move from compromised office systems to production systems.

4.2 Multi-Factor Authentication and Access Control

MFA should be implemented for cloud services, remote connections and privileged accounts. Access should follow job responsibilities, with privileged accounts separated from normal accounts and reviewed regularly. These controls reduce the risk of stolen credentials being used to access sensitive systems.

4.3 Endpoint and Malware Protection

SFM should use centrally managed endpoint security on computers and relevant servers to detect malware and suspicious activity. Unauthorised applications should be restricted, while removable media should be controlled. Approved USB devices should be checked before use on manufacturing systems.

4.4 Vulnerability and Patch Management

SFM should maintain an inventory of hardware, software, IoT devices and OT assets and regularly assess vulnerabilities. Critical vulnerabilities should receive priority, while production-system patches should be tested before deployment. Where immediate patching is not possible, network isolation or increased monitoring should be used (NIST, 2024).

4.5 Secure Backup and Recovery

Critical business and production information should be backed up regularly. Important backups should be protected from unauthorised modification or deletion, and restoration should be tested. SFM should also establish recovery priorities to restore essential production systems quickly following an incident.

4.6 Email and Phishing Protection

SFM should use email filtering to detect suspicious messages, malicious attachments and fraudulent links. Employees should report suspicious emails, while payment requests and supplier bank-detail changes should be independently verified. MFA should provide additional protection against compromised passwords.

4.7 IoT and OT Security

SFM should maintain an inventory of IoT/OT devices, change default passwords, disable unnecessary services and apply supported updates. Where patching is not possible, network isolation and increased monitoring should be used (NIST, 2024).

4.8 Implementation Roadmap

SFM should implement the controls in phases:

Period	Key measures
0–3 months	Asset inventory, MFA, training, backup and access review
3–6 months	IT/OT segmentation, endpoint and email security
6–9 months	SIEM monitoring, supplier assessment and IoT/OT improvements
9–12 months	Incident exercises, recovery testing and policy review

This phased approach allows SFM to prioritise high-risk weaknesses while reducing disruption to manufacturing operations. NIST CSF 2.0 supports organisations in

prioritising cybersecurity improvements according to their circumstances (Pascoe, Quinn and Scarfone, 2024).

5. Monitoring and Incident Response

Robust surveillance and incident management are crucial for SteelForm Manufacturing Ltd (SFM) as preemptive security measures cannot entirely exclude the risk of a cyber assault. Ongoing surveillance can assist SFM in detecting dubious behaviour promptly, whereas a systematic incident-response protocol can mitigate the operational and financial repercussions of a successful breach. The National Cyber Security Center (NCSC) advises businesses to create incident-reaction strategies beforehand, delineate roles and escalation protocols, and consistently evaluate their response competencies (NCSC, 2025).

5.1 Continuous Security Monitoring

SFM ought to establish centralised security surveillance throughout its IT, OT, IoT, and cloud ecosystems. Security logs ought to be gathered from critical sources like firewalls, servers, endpoints, authentication systems, cloud services, and network devices. A Security Information and Event Management (SIEM) system may be employed to aggregate and analyse these logs, producing alerts upon the identification of potentially dubious activities. For instance, multiple failed login attempts, atypical access to sensitive engineering documents, unforeseen messages from an IoT device, or irregular network activity from a production system ought to trigger alerts for further examination. Oversight must extend to the interface between SFM's corporate IT infrastructure and its operational technology environment. Atypical interactions between these contexts may suggest an effort to transition from a compromised office system to production systems. Security staff must set suitable alert thresholds to ensure that legitimate threats are acknowledged while minimising the occurrence of false alarms.

5.2 Incident Detection and Triage

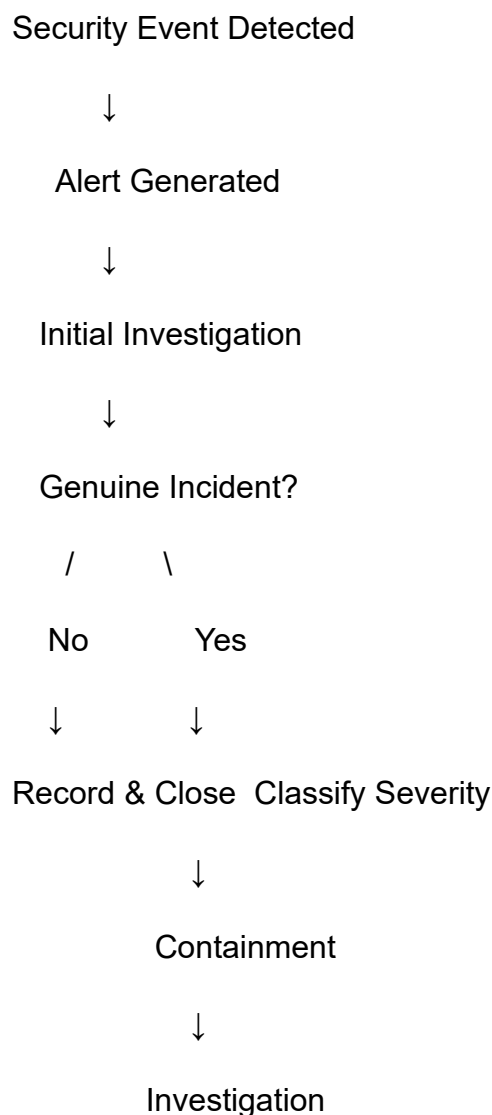
Upon the generation of a security alert, the IT security team must first ascertain if the occurrence constitutes a legitimate security incident. The event must subsequently be categorised based on its seriousness and its ramifications for the business. A solitary

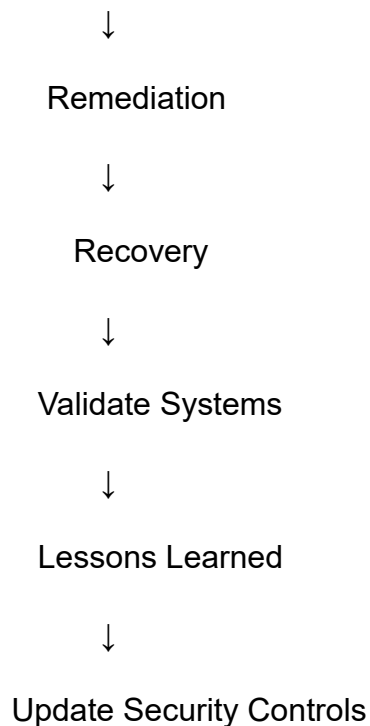
stopped phishing email can be deemed a minor occurrence, but ransomware impacting production systems ought to be categorised as a severe incident. SFM ought to uphold recorded incident-response protocols for its paramount dangers, encompassing phishing, malware infiltration, ransomware, unauthorised access, and data breaches. The NCSC advises that incident-response strategies should encompass essential contacts, escalation protocols, a fundamental incident-response procedure, and instructions for documenting and handling occurrences (NCSC, 2019).

5.3 Incident Response Process

The SFM incident-response process should follow a structured approach from detection to recovery and lessons learned.

Figure 1: Proposed Cybersecurity Incident-Response Flow for SFM





Upon detection of an alert, the security team must examine and ascertain if it constitutes a legitimate occurrence. Verified occurrences ought to be categorised based on their severity, succeeded by suitable containment strategies. This may involve segregating infected devices, deactivating compromised accounts, or limiting impacted network connections. SFM must subsequently examine the origin, ascertain impacted systems, and eliminate malware or vulnerabilities. In the case of significant incidents, the involvement of external cybersecurity experts may be necessary. During the recovery process, impacted systems must be securely reinstated utilising authenticated backups as required. Systems must be inspected prior to resuming regular functionality.

Ultimately, SFM ought to perform a post-incident analysis to ascertain the events that transpired, which safeguards were ineffective, and what enhancements are necessary. Insights gained ought to be utilised to enhance forthcoming incident-response protocols and security measures (NCSC, 2019).

5.4 Roles and Responsibilities

SFM should establish a small incident-response team appropriate to its size. The IT Security Manager should coordinate the technical response, while senior management should make major business decisions. IT administrators can support system isolation and recovery, while HR, legal and communications personnel should be involved when an incident affects employees, personal data, customers or external communications.

Where SFM does not have sufficient specialist expertise internally, it should maintain arrangements with an external cyber incident-response provider. The NCSC recommends preparing access to appropriate external support before a serious incident occurs.

5.5 Incident Testing and Improvement

SFM ought to consistently evaluate its incident-response strategy via tabletop drills, including ransomware situations. These activities can evaluate employee reporting, system segregation, and managerial decision-making. The NCSC advises evaluating response protocols to uncover vulnerabilities prior to an actual event (NCSC, 2019). SFM's oversight and reaction plan ought to integrate ongoing surveillance, defined roles, swift containment, secure restoration, and insights gained. This will mitigate the effects of assaults on production, sensitive data, and operational continuity.

6. Staff Training and Security Awareness Programme

Staff training is an important component of SFM's cybersecurity strategy because employees interact directly with email, cloud services, production systems, customer information and other organisational resources. Technical controls alone cannot eliminate risks caused by human error, phishing or inappropriate handling of information. The NCSC recommends that organisations develop a positive cybersecurity culture in which employees understand their responsibilities, know how to report concerns and receive training appropriate to their roles. It also recommends using different training methods and providing regular refresher activities rather than relying on a single annual training session (NCSC, 2025).

6.1 Core Cybersecurity Awareness Training

All SFM employees should complete mandatory cybersecurity awareness training when they join the organisation and receive regular refresher training. The core programme should cover password security, multi-factor authentication, phishing and social engineering, safe use of company devices, data classification, secure use of cloud services, removable-media risks and procedures for reporting suspected incidents. These subjects are particularly relevant to SFM because the company has already experienced phishing attempts and malware infections. The NCSC's training for staff similarly focuses on practical areas including strong passwords, device security, phishing and incident reporting, making this approach appropriate for an organisation such as SFM.

6.2 Role-Based Training

Training must not be uniform for all employees, as various departments encounter distinct cybersecurity threats. Procurement personnel must undergo more instruction on supplier impersonation, phishing schemes, fake invoices, and requests for alterations in payment details. Engineering personnel ought to get training on safeguarding intellectual property, engineering schematics, and sensitive technical data. Production personnel ought to receive training on the secure use of OT systems, IoT devices, and portable storage media. IT administrators want to obtain enhanced training that encompasses privileged accounts, network security, vulnerability management, and incident response. This role-oriented methodology aligns with NCSC recommendations, which assert that cybersecurity education must mirror actual work practices and be customised to individual business functions.

6.3 Phishing Simulations and Practical Exercises

SFM ought to implement regulated phishing-awareness drills at regular intervals to evaluate employees' ability to recognise dubious communications. The objective should be instruction instead of retribution. Personnel who engage with a simulated phishing communication ought to obtain prompt instruction detailing the warning indicators they overlooked and the procedure for reporting analogous messages subsequently. Concise scenario-driven exercises may be employed to evaluate employees' reactions to circumstances like a potential malware breach, a misplaced corporate gadget, or an unsolicited demand for sensitive information.

6.4 Training Schedule

SFM could implement the following training cycle:

Frequency	Activity	Target
At induction	Core cybersecurity training	All new employees
Monthly	Short security awareness message	All employees
Quarterly	Phishing simulation and short refresher	All employees
Every 6 months	Role-specific cybersecurity training	Higher-risk departments
Annually	Full cybersecurity awareness review	All employees
After an incident	Targeted lessons-learned training	Relevant employees

NCSC guidance recommends delivering training in **small, frequent chunks**, rather than relying only on a long annual session, because regular communication can help maintain awareness and engagement.

6.5 Measuring Training Effectiveness

SFM ought to assess if training is genuinely enhancing employee conduct instead of merely tracking attendance. Appropriate metrics may encompass training completion percentages, outcomes of phishing simulations, the quantity of suspicious emails flagged by staff, the duration of incident reporting, and repeated breaches of policy. Training materials ought to be evaluated upon the identification of deficiencies. The NCSC recommendations likewise stress that businesses have to assess training initiatives and preserve suitable training documentation.

In summary, SFM ought to establish an ongoing cybersecurity awareness initiative that integrates compulsory training, role-specific instruction, hands-on exercises, and consistent communication. The initiative ought to foster a constructive security ethos where personnel feel accountable for safeguarding corporate data and are motivated to disclose dubious behaviour without apprehension of retribution. This methodology would enhance the human aspect of SFM's comprehensive cybersecurity framework and augment the technical measures suggested earlier.

7. Conclusion :

Cybersecurity is crucial for SFM due to its IoT, OT, automated equipment, and cloud infrastructures heightening vulnerability to cyber threats. Principal hazards encompass ransomware, phishing, malware, corporate espionage, supply-chain assaults, and human mistake, all of which may interrupt production and result in data or monetary losses.

SFM ought to use least-privilege access, multi-factor authentication, IT/OT segmentation, data categorisation, patch management, secure backups, supplier security, and ongoing monitoring. The NIST Cybersecurity Framework 2.0 endorses this methodology via Govern, Identify, Protect, Detect, Respond, and Recover (NIST, 2024).

Efficient incident management and staff awareness are likewise crucial. A gradual execution of these strategies, endorsed by upper management, will enhance SFM's robustness, safeguard sensitive data, and ensure consistent production.

References :

1. National Cyber Security Centre (NCSC) (2025) *Principle B6: Staff awareness and training*. Available at: [NCSC Staff Awareness and Training](#) (Accessed: 13 August 2026).
2. National Cyber Security Centre (NCSC) (2025) *Planning your response to cyber incidents*. Available at: [NCSC: Planning your response to cyber incidents](#) (Accessed: 13 August 2026).

3. National Cyber Security Centre (NCSC) (2019) *Incident management*. Available at: [NCSC Incident Management](#) (Accessed: 13 August 2026).
4. National Cyber Security Centre (NCSC) (2025) *Engagement and training*. Available at: [NCSC Engagement and Training](#) (Accessed: 13 August 2026).
5. National Cyber Security Centre (NCSC) (2025) *Top tips for staff*. Available at: [NCSC Top Tips for Staff](#) (Accessed: 13 August 2026).
6. National Institute of Standards and Technology (NIST) (2024) *The NIST Cybersecurity Framework (CSF) 2.0*. NIST Cybersecurity White Paper 29. Gaithersburg, MD: National Institute of Standards and Technology. Available at: [NIST Cybersecurity Framework 2.0](#) (Accessed: 13 August 2026).
7. National Institute of Standards and Technology (NIST) (2023) *Guide to Operational Technology (OT) Security*. NIST Special Publication 800-82 Revision 3. Gaithersburg, MD: National Institute of Standards and Technology. Available at: [NIST SP 800-82 Rev. 3](#) (Accessed: 13 August 2026).
8. National Institute of Standards and Technology (NIST) (2020) *Security and Privacy Controls for Information Systems and Organizations*. NIST Special Publication 800-53 Revision 5. Gaithersburg, MD: National Institute of Standards and Technology. Available at: [NIST SP 800-53](#) (Accessed: 13 August 2026).
9. National Institute of Standards and Technology (NIST) (2003) *Building an Information Technology Security Awareness and Training Program*. NIST Special Publication 800-50. Gaithersburg, MD: National Institute of Standards and Technology. Available at: [NIST SP 800-50](#) (Accessed: 13 August 2026).
10. National Institute of Standards and Technology (NIST) (2025) *Cybersecurity Framework Manufacturing Profile*. NIST Interagency/Internal Report 8183 Revision 2. Gaithersburg, MD: National Institute of Standards and Technology. Available at: [NIST Manufacturing Profile](#) (Accessed: 13 August 2026).
11. National Institute of Standards and Technology (NIST) (2026) *Ransomware Risk Management: A Cybersecurity Framework 2.0 Community Profile*. NIST Interagency/Internal Report 8374 Revision 1. Gaithersburg, MD: National Institute of Standards and Technology. Available at: [NIST Ransomware Risk Management](#) (Accessed: 13 August 2026).

Appendix

ACCA4024 • INDIVIDUAL ASSESSMENT

Cybersecurity & Data Governance Policy

SteelForm Manufacturing Ltd (SFM)

Student Name: Eulalio Fernandes

Module: ACCA4024 – Networks & Cyber Security Essentials

Student Number: 2441942

Audience: Board of Directors



SFM Background & Cybersecurity Problem

Company Operational Context

- > Medium-sized UK manufacturer supplying highly demanding **automotive and aerospace sectors**.
- > Utilises advanced **IoT-enabled sensors** for real-time monitoring and quality management.
- > Operates automated machinery integrated with **Operational Technology (OT)** systems.
- > Relies on **cloud-based production management** platforms for supply chain integration.

Recent Security Incidents

- > **Malware Infections:** Disrupted workstation operations and compromised internal nodes.
- > **Targeted Phishing:** Social engineering campaigns directed at procurement and finance staff.
- > **Unauthorised OT Access:** Security gaps exposing production-network assets.

 IoT Sensors



 OT Machinery



 Cloud Management



 Business Network

Key Impact: Unmitigated cyberattacks could halt production, expose confidential IP, and cause severe financial and reputational damage.

Key Cybersecurity Threats

External Threats

-  Ransomware targeting production control systems
-  Phishing & social engineering targeting procurement
-  Malware aimed at network disruption
-  Industrial espionage seeking trade secrets & aerospace IP
-  Supply-chain attacks via compromised vendor connections
-  IoT and Operational Technology (OT) targeted exploits

Internal Threats

-  Malicious insiders with direct network access
-  Human error & accidental data exposure
-  Weak or reused passwords across systems
- Unauthorised software or unvetted personal devices
-  Excessive access privileges granted to users

 Threat Vectors Target Both Corporate IT Networks and Factory-Floor Operational Technologies

Potential Business Impact

1. Production Impact

- Unplanned manufacturing downtime and idle assembly lines
- Severe disruption to automated machinery and IoT processes
- Inability to meet delivery deadlines for automotive & aerospace clients

2. Financial Impact

- Substantial incident response, forensic and system recovery costs
- Direct revenue loss from halted manufacturing output
- Potential contractual penalties and regulatory non-compliance fines

3. Information Impact

- Theft of proprietary intellectual property and precision engineering designs
- Data breaches exposing commercial agreements and customer records
- Loss of critical operational logs and configuration data

4. Reputational Impact

- Loss of trust among prime aerospace and automotive partners
- Long-term brand erosion in highly competitive industrial markets
- Termination of ongoing supplier agreements

"Cybersecurity is a vital business and operational risk — not merely an IT department issue."

Proposed Cybersecurity & Data Governance Policies



1. Access Control & MFA



2. IT/OT Network Security



3. Data Governance &
Classification



4. Acceptable Use & Email
Security



5. Vulnerability & Patch
Management



6. Incident Response &
Reporting



7. Supplier & Third-Party
Security



8. Backup, Recovery &
Continuity

 NIST Cybersecurity Framework 2.0:

Govern



Identify



Protect



Detect



Respond



Recover

Key Mitigation Measures (Defence in Depth)

- 1. People 
- 2. Access Control 
- 3. Network Boundary 
- 4. Endpoint & Devices 
- 5. Data Protection 
- 6. Continuous Monitoring 

Core Technical & Operational Controls

- ✓ **IT / OT / IoT Network Segmentation:** Strict firewalls isolating plant machinery from office IT.
- ✓ **Multi-Factor Authentication (MFA):** Mandated across administrative, cloud, and remote logins.
- ✓ **Endpoint & Malware Protection:** Next-gen antivirus and EDR deployed to workstations and servers.
- ✓ **Vulnerability & Patch Management:** Routine scanning and scheduled patching of industrial hardware.
- ✓ **Secure Backups & Recovery:** Immutable 3-2-1 offsite and cloud backup strategies.
- ✓ **Email & Phishing Protection:** Advanced spam filtering and link-verification gateways.
- ✓ **Supplier Security Assessments:** Risk evaluations prior to granting partner integrations.

12-Month Cybersecurity Implementation Roadmap

Months 0 – 3

FOUNDATIONS & MFA

- Complete IT/OT asset inventory
- Enforce mandatory MFA across email & remote access
- Launch basic staff cybersecurity induction
- Review offline backup readiness
- Audit privileged access accounts

Months 3 – 6

NETWORK & ENDPOINTS

- Deploy strict IT/OT/IoT network segmentation
- Roll out EDR endpoint security
- Implement email filtering and phishing protection
- Establish vulnerability patching schedules

Months 6 – 9

MONITORING & SUPPLIERS

- Deploy SIEM for centralized log monitoring
- Conduct supplier cybersecurity risk assessments
- Apply enhanced IoT/OT firmware security controls
- Initiate quarterly phishing simulations

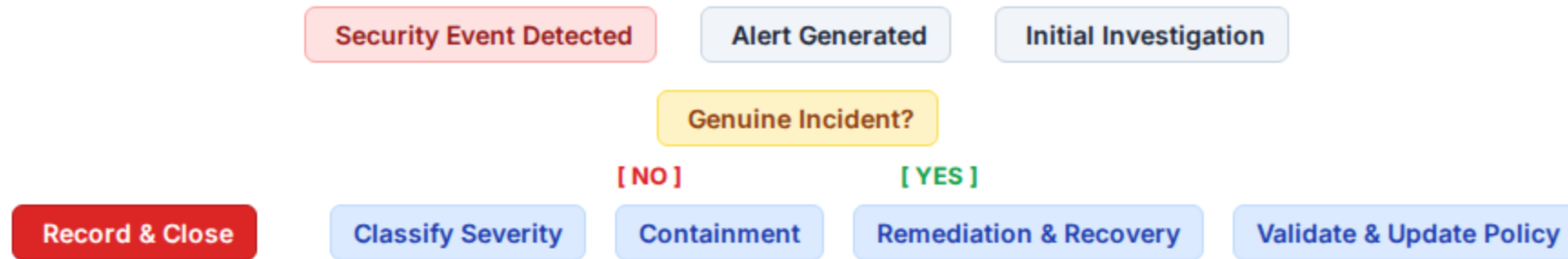
Months 9 – 12

TESTING & GOVERNANCE

- Execute Board & IT incident response exercises
- Perform full disaster backup recovery testing
- Conduct comprehensive policy reviews
- Embed continuous monitoring & improvement

Core Objective: "Prioritise high-risk controls while ensuring zero disruption to active production schedules."

Monitoring and Incident Response Workflow



 **Continuous Telemetry Data Sources:** Firewalls • Endpoints • Authentication Systems • Cloud Platforms • Network Hardware • IT/OT Traffic Scanners

Staff Training and Security Awareness

Training Programme Schedule

Frequency	Training Focus
At Induction	Core cybersecurity policy & hygiene basics
Monthly	Bite-sized security tips & threat updates
Quarterly	Simulated phishing tests & analysis
Bi-Annually	Role-based technical security training
Annually	Mandatory policy review & assessment
Post-Incident	Targeted lessons-learned workshops

Role-Specific Training Focus

- **Procurement:** Phishing, invoice fraud & supplier risk
- **Engineering:** IP protection & secure document sharing
- **Production:** Physical OT access & IoT security hygiene
- **IT Operations:** Privileged credentials & incident management

Success Metrics

Training Completion Rate %

Phishing Failure Rate %

Incident Reporting Speed

Policy Compliance Rate

Recommendations to the Board

RECOMMENDATION 1

IT/OT Network Segmentation

Isolate production controls from corporate internet access.

RECOMMENDATION 2

MFA & Least-Privilege Access

Enforce multi-factor verification across all user entry points.

RECOMMENDATION 3

Critical Data Protection

Classify aerospace/automotive IP with strict encryption.

RECOMMENDATION 4

Continuous Security Monitoring

Establish centralised SIEM logging across network assets.

RECOMMENDATION 5

Tested Incident Response

Conduct bi-annual executive table-top cyber crisis drills.

RECOMMENDATION 6

Immutable Backup & Recovery

Implement offline backups to guarantee ransomware resilience.

RECOMMENDATION 7

Supplier Cybersecurity Governance

Audit third-party vendor connections and compliance.

RECOMMENDATION 8

Continuous Employee Awareness

Fund ongoing phishing simulations and role-specific education.

"Strategic cybersecurity investment directly protects production continuity, intellectual property, customer trust, and long-term enterprise value."

Conclusion and Key References

Executive Summary Conclusion

SFM must treat cybersecurity as an **organisation-wide strategic responsibility** rather than an isolated IT operational task.

A phased combination of robust governance, technical controls, continuous monitoring, formal incident response, and active staff awareness will significantly strengthen resilience, safeguard confidential client IP, and ensure uninterrupted manufacturing operations.

Key Academic & Industry References

National Cyber Security Centre (NCSC) (2023) *10 Steps to Cyber Security*. London: NCSC.

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

NIST (2023) *Guide to Operational Technology (OT) Security* (SP 800-82 Rev. 3). Gaithersburg: NIST.

NIST (2021) *Ransomware Risk Management: A Cybersecurity Framework Profile* (NISTIR 8374). Gaithersburg: NIST.

NIST (2022) *Cybersecurity for Smart Manufacturing Systems*. Gaithersburg: NIST.

Image Sources



<https://industrialcyber.co/wp-content/uploads/2025/06/2025.06.25-Smart-manufacturing-at-turning-point-as-cybersecurity-IT-OT-convergence-reshape-industrial-strategy.webp>

Source: industrialcyber.co