

Synthesize a Solution To A Potential Problem

SteelForm Manufacturing Ltd (SFM)

Developing a comprehensive cybersecurity and data governance policy to strengthen protection against internal and external threats.

Module: ACCA4024 — Network and Cybersecurity Essentials

Student Name: Hannah Lwetutte

Student ID: 2509323

Group:2

Lecturer's name: Amit Naik

Table of Contents

- 1. Introduction**
- 2. Identification of Threats**
 - 2.1 Internal Threats
 - 2.2 External Threats
- 3. Security Policies**
 - 3.1 Access Control and Identity Management Policy
 - 3.2 Data Governance and Encryption Policy
 - 3.3 Patch and Vulnerability Management Policy
- 4. Mitigation Measures**
 - 4.1 Network Segmentation and the Industrial DMZ
 - 4.2 Ransomware and Malware Protection (EDR)
 - 4.3 Securing the Internet of Things (IoT)
 - 4.4 Supply Chain and Remote Access Security
- 5. Monitoring and Incident Response Plan**
 - 5.1 Continuous Security Monitoring
 - 5.2 The Incident Response Lifecycle
- 6. Training and Security Awareness Program**
 - 6.1 Role-Based Training Curriculum
 - 6.2 Continuous Awareness Tactics
 - 6.3 Measuring Program Effectiveness
- 7. Conclusion**

References

Appendix

1. Introduction

The integration of Industry 4.0 technologies at SteelForm Manufacturing Ltd (SFM) including IoT-enabled sensors and cloud-based production management has significantly changed the organization's risk profile.

Recent security incidents at SFM, such as malware infections and targeted phishing attempts against procurement staff, indicate that existing defenses are being actively tested by external actors.

This report proposes a defence-in-depth cybersecurity and data governance framework aligned with ISO/IEC 27001 and the NIST Cybersecurity Framework. It focuses on protecting the confidentiality, integrity and availability (CIA) of SFM's data and production systems against internal and external threats.

2. Identification of Threats

The convergence of Operational Technology (OT) and Information Technology (IT) has created a "security gap" where legacy industrial hardware meets modern cloud connectivity [1].

2.1 Internal Threats

- **Insider Threats (Accidental and Malicious):** Human error remains the primary driver of security incidents. The recent phishing attempts at SFM demonstrate how well-meaning staff can inadvertently leak credentials [2]. Beyond accidents, the high-value nature of SFM's aerospace blueprints makes the firm a target for industrial espionage. A disgruntled employee or contractor with legitimate access could exfiltrate proprietary designs for financial gain or to benefit a competitor.
- **Privilege Creep and Over-Provisioning:** Over time, employees often accumulate access rights to systems they no longer require. If a "super-user" account (e.g., someone with access to both Procurement and the Production Floor) is compromised, the attacker gains lateral movement across the entire company.

- **Shadow IT and Unauthorised Hardware:** The use of personal USB drives or unapproved mobile devices on the factory floor is a major risk. These devices can bypass corporate firewalls and introduce malware directly into isolated PLC (Programmable Logic Controller) systems, which control the automated machinery.

2.2 External Threats

- **Ransomware-as -a-Service (RaaS):** This is the single greatest threat to SFM's Availability. Attackers can encrypt the factory's production management system, preventing staff from using it and forcing the assembly line to stop. For SFM, even a few hours of downtime could trigger massive financial penalties from automotive partners who rely on "Just-in-Time" delivery [4].
- **Advanced Phishing and Business Email Compromise (BEC):** The targeted emails toward SFM's procurement staff are a classic sign of BEC. These attacks aim to intercept high value financial transactions or harvest administrative logins for the cloud-based production system [2], [5].
- **IoT and Supply Chain Vulnerabilities:** The new smart sensors at SFM lack the processing power to run modern security agents. These "weak links" can be exploited to gain a foothold in the network. Furthermore, a compromise at one of SFM's cloud providers or logistics partners could allow an attacker to "hitchhike" into SFM's systems via trusted software updates [3], [6].
- **State-Sponsored Cyber-Espionage:** Given SFM's role in the aerospace supply chain, the company is a target for sophisticated foreign actors. Their goal is often not immediate financial gain, but the long-term theft of sensitive engineering data to undermine national competitive advantages [5].

3. Security Policies

To address the identified threats, SFM must establish a formal policy framework that aligns with ISO/IEC 27001 standards [3].

3.1 Access Control and Identity Management Policy

To mitigate the risk of unauthorised access and lateral movement by attackers, SFM will implement a Zero Trust approach to identity. These controls should be reviewed annually and after significant security incidents to ensure that access requirements remain appropriate to SFM's changing IT and OT environment.

Principle of Least Privilege (PoLP)

Access rights should be granted based strictly on job necessity. For example, production engineers will have access to PLC logic but will be restricted from procurement financial systems.

Multi-Factor Authentication (MFA)

Mandatory MFA should be enforced for all cloud-based production management systems, remote VPN connections, and administrative accounts. This reduces the risk of compromised credentials from phishing [2].

Account Lifecycle Management

Access reviews should be conducted quarterly to prevent privilege creep. Furthermore, a strict Immediate Revocation policy will ensure that accounts for departing staff or contractors are disabled within one hour of their exit.

3.2 Data Governance and Encryption Policy

Data Classification Schema:

All organisational data will be categorized into four levels: Public, Internal, Confidential, and Highly Confidential. Proprietary engineering blueprints and customer contracts are automatically classified as Highly Confidential.

Encryption Standards:

All highly confidential data must be encrypted using AES-256 standards while at rest on servers and TLS 1.3 while "in transit" across networks [5].

Removable Media Control:

To prevent malware entry into isolated production zones, the use of personal USB devices is strictly prohibited. Only company-issued, hardware-encrypted drives that have been cleared by the IT Security team may be used.

3.3 Patch and Vulnerability Management Policy:

Unpatched software is a primary entry point for ransomware. SFM will adopt a risk-based patching schedule. Critical vulnerabilities should be prioritised according to exploitability, exposure and potential impact on production.

Critical Systems:

Security patches for office workstations and cloud gateways must be applied within 14 days of release.

Operational Technology (OT) Exceptions: For automated machinery where a reboot could cause production failure, "compensating controls" such as network isolation and enhanced monitoring will be used until a scheduled maintenance window allows for a full patch [6].

4. Mitigation Measures

SFM should implement a defence-in-depth strategy so that failure of one security control does not result in complete system compromise.

4.1 Network Segmentation and the Industrial DMZ

The most critical technical mitigation for SFM is the logical and physical separation of the Corporate (IT) Network and the Operational Technology (OT) Network

Implementation

SFM should deploy an Industrial Demilitarised Zone (IDMZ). This acts as a buffer between the office computers (where phishing is a risk) and the factory floor (where the smart sensors and PLCs reside).

Firewall Rules:

Only essential data traffic should be allowed to pass through the IDMZ. For example, the cloud-based production management system can pull data from the sensors, but a compromised laptop in the office will be physically unable to send commands to the automated machinery [6]. Firewall rules should follow a deny by default approach, allowing only approved traffic between required systems.

4.2 Ransomware and Malware Protection (EDR)

Endpoint Detection and Response (EDR)

SFM will deploy EDR agents on all workstations and servers. Unlike basic antivirus, EDR uses behavioural analysis to spot ransomware like activity (such as mass file encryption) and can automatically isolate an infected device before the malware spreads [4], [7].

Immutable Backups

To ensure availability, SFM will implement the 3-2-1 backup rule: three copies of data, on two different media types, with one copy stored offline or in an immutable cloud vault. This ensures that even if ransomware encrypts the live network, the company can restore production without paying a ransom [8].

4.3 Securing the Internet of Things (IoT)

Device Profiling

All IoT devices should be registered in a central asset inventory. Any device not on the "allow-list" will be automatically blocked from the network.

VLAN Isolation

All IoT sensors will be placed on their own dedicated Virtual Local Area Network (VLAN) with no direct access to the internet. This prevents a compromised sensor from being used as a gateway for external attackers [1].

Default passwords should be changed before devices are connected, and firmware should be updated where supported.

4.4 Supply Chain and Remote Access Security

Secure VPN with MFA

All vendor access will be conducted via a dedicated Virtual Private Network (VPN) protected by MFA.

Just-in-Time (JIT) Access

Vendor accounts will be disabled by default and only activated during scheduled maintenance windows, reducing the window of opportunity for attackers.

Suppliers with network access should also undergo security assessments and provide evidence of appropriate security controls before access is approved.

5. Monitoring and Incident Response Plan

By integrating automated detection with a structured response plan, the organisation can minimise the dwell time of an attacker and the period between an initial breach and its discovery.

5.1 Continuous Security Monitoring

SFM will implement a centralized Security Information and Event Management (SIEM) platform. This system will collect and correlate logs from firewalls, EDR agents, cloud services, and the Industrial DMZ.

Anomaly Detection

The SIEM will be configured to alert the IT Security team to "out-of-character" behaviour, such as a procurement account attempting to access the production network at 3:00 AM, or a sudden spike in data exfiltration toward an unknown external IP address [1], [2].

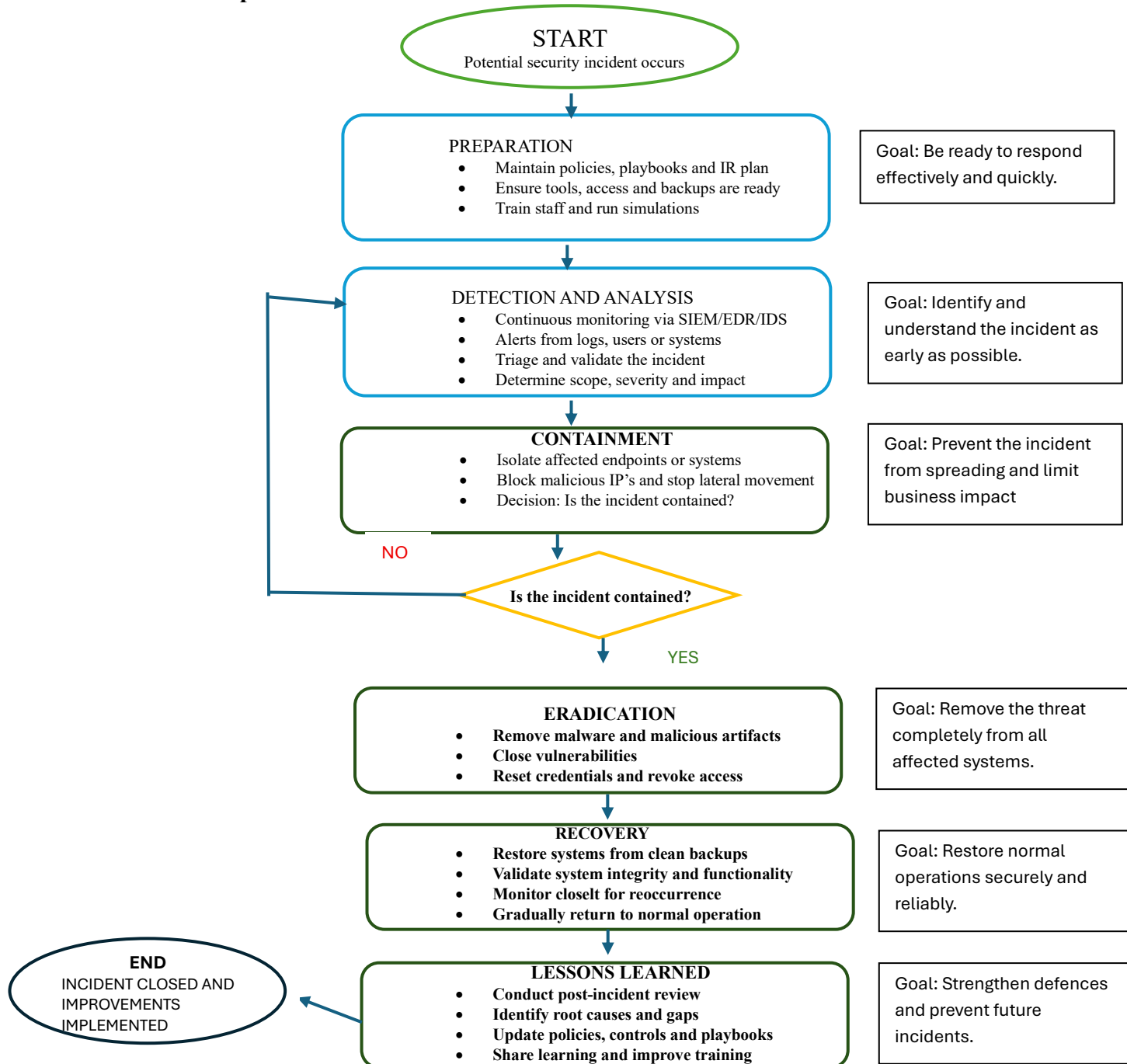
Operational Technology (OT) Monitoring

Due to the fact that active scanning can disrupt sensitive manufacturing equipment, SFM will use passive network monitoring on the factory floor. This allows the team to see what is happening on the IoT network without risking a production shutdown [6]. Alerts should be prioritised according to severity so that the security team can respond first to events posing the greatest risk to production and sensitive data

5.2 The Incident Response Lifecycle

In the event of a confirmed security breach, SFM will follow a six-stage response framework based on NIST 800-61 standards

The Incident response Flowchart:



As shown in Figure 5.2, SFM's response lifecycle prioritizes early Detection and Analysis to minimize 'dwell time.' The Containment phase is particularly critical, ensuring that threats are blocked from lateral movement before moving to the Eradication and Recovery stages.

The lifecycle ensures that SFM can detect, contain and recover from incidents while limiting disruption to production. Containment should consider operational requirements, with compromised office systems isolated before production systems are disrupted where safely possible. Following recovery, a post-incident review should identify root causes and update controls and training.

6. Training and Security Awareness Program

At SFM, the recent phishing success against procurement staff highlights a critical need for a human-centric security culture.

6.1 Role-Based Training Curriculum

Procurement and Finance: This Focuses heavily on Business Email Compromise (BEC) and social engineering. Staff will be trained to verify any changes to supplier bank details via a secondary, "out-of-band" communication method (e.g., a phone call) rather than relying on email [2].

Production and Engineering: This Focuses on Operational Technology (OT) hygiene. This includes the dangers of using unauthorised USB drives on PLC terminals and recognising physical tampering with IoT sensors on the factory floor.

Executive Board: Focused on Strategic Risk and Crisis Management, ensuring the leadership team understands their roles during a major ransomware incident.

6.2 Continuous Awareness Tactics

To ensure security remains a priority SFM will deploy the following:

Simulated Phishing Exercises: Monthly, non-punitive phishing tests will be sent to all staff. Employees who click will receive immediate, bite sized just-in-time training. Employees who click should receive immediate, non-punitive refresher training.

The "Clean Desk and Port" Policy: Production floor audits should check for unauthorised USB devices and removable media

6.3 Measuring Program Effectiveness

Phishing Reporting Rate: We want to see an increase in staff using the "Report Phishing" button. Phishing click rates should also be tracked, with a target reduction over time.

Mean Time to Detect (MTTD): Measuring if staff are noticing and reporting anomalies faster over time.

Training Completion: 100% compliance for all new hires before they are granted network credentials.

7. Conclusion

By implementing a defence in depth strategy combining network segmentation (IDMZ), robust incident response (NIST-aligned), and a role-based training culture. SFM can significantly reduce its risk profile. Continuous investment in both technical defences and human awareness will ensure that SFM remains secure, compliant, and competitive in an increasingly hostile digital landscape.

References

- [1] C. Pascoe, S. Quinn, and K. Scarfone, “The NIST Cybersecurity Framework (CSF) 2.0,” National Institute of Standards and Technology, NIST CSWP 29, Feb. 2024. doi: 10.6028/NIST.CSWP.29.
- [2] Verizon Business, “2025 Data Breach Investigations Report (DBIR),” Verizon, 2025. [Online]. Available: <https://www.verizon.com/business/resources/reports/dbir/>
- [3] International Organization for Standardization, “ISO/IEC 27001:2022—Information security, cybersecurity and privacy protection—Information security management systems—Requirements,” ISO, Geneva, Switzerland, 2022.
- [4] IBM Security, “Cost of a Data Breach Report 2024,” IBM, 2024. [Online]. Available: <https://www.ibm.com/reports/data-breach>

[5] Information Commissioner's Office, "A guide to data security and UK GDPR compliance," ICO, May 2023. [Online]. Available: <https://ico.org.uk>

[6] Cybersecurity and Infrastructure Security Agency (CISA), "Industrial Control Systems (ICS) Security Recommended Practices," CISA, 2023. [Online]. Available: <https://www.cisa.gov/resources-tools/services/ics-security-recommended-practices>

[7] NCSC, "Device Security Guidance: EDR," 2023.

[8] NCSC, "Ransomware-Resistant Backups," 2024

Appendix



Board Presentation. ACCA4024

SYNTHESIZE A SOLUTION TO A POTENTIAL PROBLEM

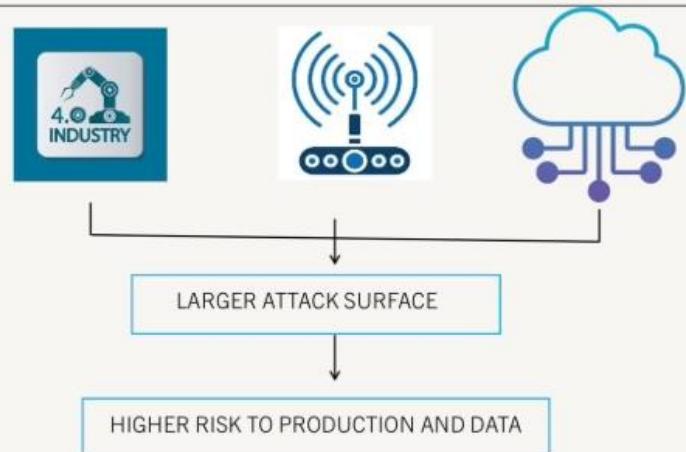
Developing a comprehensive cybersecurity and data governance policy to strengthen protection against internal and external threats

By Hannah Lweutte

WHY SFM NEEDS TO ACT

- SFM INCREASINGLY RELIES ON INDUSTRY 4.0 TECHNOLOGIES, INCLUDING IOT SENSORS AND CLOUD-BASED PRODUCTION SYSTEMS.
- GREATER CONNECTION BETWEEN IT AND OT NETWORKS HAS EXPANDED THE ATTACK SURFACE.
- RECENT MALWARE INFECTIONS AND PHISHING ATTEMPTS SHOW THAT SFM IS ALREADY BEING TARGETED.
- A SUCCESSFUL CYBERATTACK COULD CAUSE PRODUCTION DOWNTIME, FINANCIAL LOSS, DATA THEFT, AND CONTRACT AND REPUTATIONAL DAMAGE.
- SFM MUST PROTECT BOTH PRODUCTION AVAILABILITY AND SENSITIVE ENGINEERING DATA.

Classified as Microsoft Confidential



The Evolving Threats

1. EXTERNAL THREATS

RANSOMWARE, PHISHING, MALWARE AND SUPPLY-CHAIN ATTACKS CAN DISRUPT SFM'S SYSTEMS

2. INTERNAL THREATS

HUMAN ERROR, EXCESSIVE ACCESS PRIVILEGES AND UNAUTHORISED DEVICES CAN EXPOSE SENSITIVE SYSTEMS.

3. INCREASING SOPHISTICATION

ATTACKERS ARE USING MORE ADVANCED METHODS TO TARGET CONNECTED IT AND OT ENVIRONMENTS

4. BUSINESS IMPACT

A SUCCESSFUL ATTACK COULD CAUSE DOWNTIME, DATA LOSS, FINANCIAL DAMAGE AND LOSS OF CUSTOMER TRUST.

Classified as Microsoft Confidential

Our Strategic Approach

1. RISK-BASED PRIORITISATION

FOCUS ON THE HIGHEST RISKS TO SFM'S PRODUCTION SYSTEMS, SENSITIVE DATA AND BUSINESS OPERATIONS.

2. PEOPLE & SECURITY CULTURE

IMPROVE STAFF AWARENESS AND REDUCE RISKS CAUSED BY PHISHING, HUMAN ERROR AND UNSAFE BEHAVIOUR.

3. STRONG SECURITY CONTROLS

USE MEASURES SUCH AS MFA, NETWORK SEGMENTATION, EDR AND SECURE BACKUPS TO PREVENT AND CONTAIN ATTACKS.

4. POLICIES & DATA GOVERNANCE

INTRODUCE CLEAR RULES FOR ACCESS CONTROL, DATA CLASSIFICATION, ENCRYPTION AND SECURE USE OF COMPANY SYSTEMS.

5. CONTINUOUS IMPROVEMENT

MONITOR THREATS, REVIEW SECURITY CONTROLS AND UPDATE PROTECTIONS AS SFM'S TECHNOLOGY AND RISKS CHANGE.

Classified as Microsoft Confidential



Six Pillar Security and Data Governance Framework

1. RISK-BASED PRIORITISATION

IDENTIFY AND FOCUS ON THE HIGHEST RISKS TO PRODUCTION, DATA AND BUSINESS OPERATIONS.

2. PEOPLE & SECURITY CULTURE

BUILD AWARENESS, PROMOTE SECURE BEHAVIOURS AND REDUCE RISKS CAUSED BY HUMAN ERROR AND PHISHING.

3. STRONG SECURITY CONTROLS

DEPLOY TECHNICAL AND ADMINISTRATIVE CONTROLS TO PREVENT, DETECT AND RESPOND TO THREATS.

4. POLICIES & DATA GOVERNANCE

ESTABLISH CLEAR POLICIES, DEFINE RESPONSIBILITIES AND ENSURE PROPER DATA CLASSIFICATION, ACCESS CONTROL AND ENCRYPTION.

5. CONTINUOUS IMPROVEMENT

MONITOR THREATS AND PERFORMANCE, REVIEW CONTROLS AND ADAPT TO NEW RISKS AND BUSINESS CHANGES.

6. COLLABORATION & COMPLIANCE

WORK WITH PARTNERS, SUPPLIERS AND REGULATORS TO MEET REQUIREMENTS AND STRENGTHEN OVERALL RESILIENCE.

Classified as Microsoft Confidential



Network Segmentation & Industrial DMZ

1. SEPARATE IT AND OT NETWORKS

KEEP OFFICE SYSTEMS ISOLATED FROM PRODUCTION MACHINERY AND PLCs.

2. INDUSTRIAL DMZ AS A BUFFER

PLACE AN INDUSTRIAL DMZ BETWEEN THE CORPORATE IT NETWORK AND THE OT NETWORK.

3. STRICT FIREWALL RULES

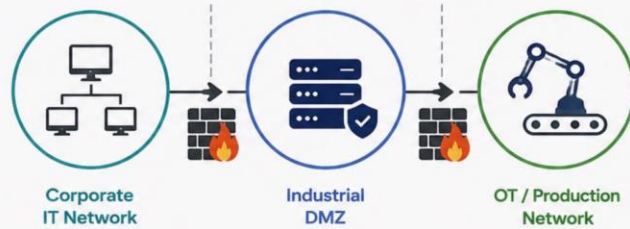
ALLOW ONLY ESSENTIAL TRAFFIC TO MOVE BETWEEN IT, THE DMZ AND PRODUCTION SYSTEMS.

4. PREVENT LATERAL MOVEMENT

A COMPROMISED OFFICE LAPTOP SHOULD NOT BE ABLE TO DIRECTLY CONTROL FACTORY MACHINERY.

5. PROTECT PRODUCTION AVAILABILITY

SEGMENTATION LIMITS THE SPREAD OF MALWARE AND REDUCES THE RISK OF PRODUCTION SHUTDOWN.



Classified as Microsoft Confidential

Access Control & Identity Management

CONTROLLING ACCESS TO CRITICAL SYSTEMS

1. USE ROLE-BASED ACCESS CONTROL (RBAC) SO STAFF ONLY ACCESS WHAT THEY NEED.

2. REQUIRE MULTI-FACTOR AUTHENTICATION (MFA) FOR SENSITIVE SYSTEMS.

3. REMOVE OR UPDATE ACCESS IMMEDIATELY WHEN EMPLOYEES CHANGE ROLES OR LEAVE.

4. REGULARLY REVIEW PRIVILEGED ADMINISTRATOR ACCOUNTS.

5. APPLY THE LEAST PRIVILEGE PRINCIPLE TO REDUCE INSIDER AND ACCOUNT COMPROMISE RISKS.



Classified as Microsoft Confidential

Protecting Sensitive Business Data

1. ENCRYPT SENSITIVE DATA WHEN STORED AND WHEN BEING TRANSFERRED.

2. USE SECURE PROTOCOLS SUCH AS HTTPS AND VPNS FOR COMMUNICATION.

3. PROTECT CUSTOMER, EMPLOYEE AND COMMERCIAL INFORMATION FROM UNAUTHORISED ACCESS.

4. KEEP REGULAR ENCRYPTED BACKUPS OF CRITICAL SYSTEMS AND FILES.

5. RESTRICT ACCESS TO ENCRYPTION KEYS TO AUTHORISED PERSONNEL ONLY.



Classified as Microsoft Confidential

Ensuring Business Continuity

1. KEEP REGULAR BACKUPS OF CRITICAL BUSINESS DATA AND SYSTEMS.

2. STORE BACKUPS SECURELY IN A SEPARATE LOCATION OR CLOUD ENVIRONMENT.

3. TEST BACKUPS REGULARLY TO MAKE SURE DATA CAN BE RESTORED SUCCESSFULLY.

4. CREATE A DISASTER RECOVERY PLAN FOR CYBERATTACKS, SYSTEM FAILURES AND DATA LOSS.

5. RESTORE ESSENTIAL PRODUCTION AND BUSINESS SYSTEMS FIRST TO REDUCE DOWNTIME.



Classified as Microsoft Confidential

Detecting and Responding to Security Incidents

1. MONITOR NETWORKS AND SYSTEMS FOR SUSPICIOUS ACTIVITY.

2. USE ALERTS FOR UNUSUAL LOGINS, MALWARE AND UNAUTHORISED ACCESS.

3. CREATE A CLEAR INCIDENT RESPONSE PLAN FOR CYBERATTACKS.

4. RECORD AND INVESTIGATE INCIDENTS TO IDENTIFY THE CAUSE.

5. REVIEW INCIDENTS AND IMPROVE SECURITY CONTROLS.



Classified as Microsoft Confidential

Strengthening Staff Security Awareness

1. TRAIN EMPLOYEES TO RECOGNISE PHISHING EMAILS AND SUSPICIOUS LINKS.

2. TEACH STAFF HOW TO REPORT SECURITY CONCERNS QUICKLY.

3. USE REGULAR AWARENESS TRAINING TO REDUCE HUMAN ERROR.

4. REMIND STAFF TO CREATE STRONG PASSWORDS AND PROTECT LOGIN DETAILS.

5. BUILD A SECURITY-AWARE CULTURE ACROSS THE ORGANISATION.



Classified as Microsoft Confidential

Key Security Recommendations

1. STRENGTHEN ACCESS CONTROLS BY ENFORCING LEAST PRIVILEGE AND MULTI-FACTOR AUTHENTICATION.
2. PROTECT DATA WITH ENCRYPTION IN TRANSIT AND AT REST, AND MAINTAIN REGULAR, TESTED BACKUPS.
3. EMPOWER STAFF THROUGH ONGOING SECURITY TRAINING AND CLEAR SECURITY AWARENESS.
4. IMPLEMENT CONTINUOUS MONITORING TO DETECT, RESPOND TO AND PREVENT THREATS
5. REVIEW AND IMPROVE SECURITY POLICIES REGULARLY TO ADAPT TO EVOLVING RISKS AND REQUIREMENTS.

Classified as Microsoft Confidential



Conclusion and Next Steps

1. CYBERSECURITY IS AN ONGOING PRIORITY THAT REQUIRES COMMITMENT AT EVERY LEVEL.
2. STRENGTHEN SECURITY THROUGH ACCESS CONTROL, ENCRYPTION, BACKUPS AND STAFF TRAINING.
3. CONTINUOUSLY MONITOR SYSTEMS AND RESPOND QUICKLY TO POTENTIAL THREATS.
4. REGULARLY REVIEW SECURITY MEASURES TO ADAPT TO EVOLVING RISKS.
5. IMPLEMENT THE RECOMMENDATIONS AND CONTINUE IMPROVING SECURITY OVER TIME.

Classified as Microsoft Confidential

