

Network and Cybersecurity Essentials

Module Name: Network and Cybersecurity Essentials

Module Code: ACCA4024 Student Name: Dolapo Farouk Owolabi Student ID: 2518096 Group: 2

Lecturer's Name: Amit Naik

Introduction

Industry 4.0 and smart technologies have made manufacturing more connected but also more exposed in today's world in technology. SFM now uses IoT, automation, and cloud systems, yet faces malware, phishing, and unauthorised access risks. Protecting production, designs, and reputation is critical. This report sets out a clear cybersecurity and data governance policy, aligned with NIST, ISO 27001, and IEC62443. It identifies threats, defines policies, proposes mitigations, outlines incident response, and plans staff training to strengthen security, maintain operations, and secure SFM's future.

Identification of Threats

The increased interconnectivity across Steel Form manufacturing Ltd.'s IT and operational technology networks has expanded the organisation's attack surface, exposing critical systems and sensitive data to a wide range of cyber threats from both external and internal sources. As manufacturing environments become more integrated with IoT, cloud platforms, and remote monitoring, the distinction between IT and operational boundaries blurs, creating opportunities for adversaries to disrupt production, steal intellectual property, and compromise operational safety [1]. The section identifies and categorises main key threats facing the company, by drawing on established cybersecurity frameworks and manufacturing sector risk assessments.

External Threats

External threats started from actors being outside of the organisation and are among the most rapidly evolving risks facing modern manufacturing. Ransomware and malware are particularly dangerous in industrial settings, where malicious software can target industrial control systems and production machinery to encrypt operational data or lock equipment, halting manufacturing processes and causing significant financial loss through downtime and recovery costs [2]. Phishing attacks remain a common entry point for external actors, frequently targeting procurement and finance teams to trick staff into disclosing credentials or executing malicious files, which can then be used to gain deeper access to internal networks [3]. Industrial espionage and advanced persistent threats pose a serious risk to high-value manufacturing, where competitors or other actors may seek to steal proprietary design data, engineering specifications, and manufacturing processes for commercial advantage [4]. Supply chain

attacks exploit trust relationships with vendors and partners, using compromised third-party access to move laterally into core systems, creating risks that are difficult to detect at the perimeter [5]. IoT and connected devices often introduce technical vulnerabilities due to weak default configurations, unchanged administrative passwords, and a lack of regular firmware updates, providing attackers with accessible entry points into the production environment [6]. Distributed denial-of-service attacks can also disrupt cloud-based production management systems by overwhelming network resources, preventing staff and automated systems from accessing critical operational tools and data [7].

Internal Threats

Internal threats started from within the organisation that are often difficult to detect because they involve legitimate access to systems and information. Human error accounts for a large proportion of security incidents, including accidental misconfiguration of network devices, use of weak or easily guessed passwords, and unintentional data sharing or leakage through email, cloud services, or portable media [8]. Insider threats include both malicious actors and careless users, where employees, contractors, or privileged users may intentionally misuse access privileges to steal data, alter systems, or cause operational disruption, or may compromise security through negligence or lack of awareness [9]. Poor access control practices further increase vulnerability, such as granting excessive permissions beyond what is required for a role and failing to disable accounts promptly after staff departures or role changes, leaving orphaned or unnecessary access in place [10]. Shadow IT — the use of unapproved personal devices, software, or cloud services connected to the corporate or production network — bypasses central security protections and monitoring, introducing unknown vulnerabilities that cannot be patched or managed by the IT team.

Security Policies

Security policies set out clear, actionable rules to protect SteelForm Manufacturing Ltd's systems, data, and production operations. They are built around widely accepted industry standards and designed to close security gaps while keeping daytoday work practical and efficient.

Network and Architecture Policy

Network is split into separate zones such as office IT, production operations, and IoT devices each sit apart from one another, protected by firewalls that stop unauthorised movement between areas. We operate on the basis that no device or user gets automatic trust, even if they are already inside the building; every connection is verified before access is allowed. Remote access and cloud connections must be encrypted and use multifactor authentication to keep entry points secure [11].

Access Control Policy

Staff working for the organisation are given only the access they need to do their jobs, and nothing more. Every account must use multifactor authentication alongside passwords that are at least 12 characters long, changed every 90 days, and never reused across different systems. A check is carried out every quarter to confirm permissions are still appropriate, and accounts are disabled within 24 hours whenever someone leaves or changes role [4].

Data Governance Policy

Information gotten from the network are grouped into four tiers: public, internal, confidential, and restricted. Design files, engineering specifications, and intellectual property fall under restricted — these must be encrypted both when stored and when sent across any network. Data is kept only as long as required, disposed of securely when obsolete, and never shared externally without formal written approval from authorised managers [8].

IoT and Operational Technology Policy

Every connected sensor, smart device, and automated machine must be logged and registered with IT before being plugged in. Default passwords are replaced immediately, and any features or ports not actually needed are turned off to reduce exposure. These devices run on their own isolated network section so that even if one is compromised, attackers cannot easily reach core business or production systems [6].

ThirdParty and Supply Chain Policy

Partner given access to our systems or data must meet the same security expectations we apply internally. Contracts will clearly state these requirements, and outside parties receive only the exact access necessary for their work. All external connections are routed through secure, monitored channels and are logged for audit and review purposes [12].

Mitigation Measures

Threat	Mitigation Measure	Implementation Details
Ransomware / Malware	Endpoint Detection & Response (EDR) + network antivirus; air-gapped immutable backups	Deploy EDR across all servers/PCs; daily incremental + weekly full backups; test quarterly
Phishing	Email filtering + URL rewriting + sandboxing; block known malicious domains	Roll out in 2 weeks; quarantine suspicious emails
IoT Vulnerabilities	Network segmentation + dedicated IoT VLAN; regular firmware patching schedule	Deploy next-gen firewall; monthly vulnerability scans; critical patches within 72h
Unauthorised Access	Zero Trust architecture + MFA everywhere + network access control	Phase 1: MFA for all admins (2w); Phase 2: network segmentation (8w)
Data Breach / IP Theft	Data Loss Prevention (DLP) tools + encryption + strict removable media controls	Deploy DLP; block unauthorised USB; encrypt all Restricted data
Insider Risk	Activity logging + periodic audits + separation of duties	SIEM log retention 12m; quarterly independent reviews
Supply Chain	Vendor security assessment + secure portal for file exchange	Standardised security questionnaire; no unrestricted network access

Protecting Against Ransomware and Malware

Every computer, server, and connected device will be protected with endpoint detection and response tools that watch for unusual behaviour and known threats. Backups are kept separate from the main network — stored offline or in a secure, unlinked location such so systems can be restored cleanly if an attack happens. We take a layered approach: email filtering catches malicious messages before they reach staff, while regular security updates fix known weaknesses. This combination makes it far harder for malware to spread or cause lasting harm [2].

Defending Phishing and Credential Theft

Email security tools will scan incoming messages and flag anything suspicious, isolating it until it can be checked. Staff will also take part in regular awareness sessions, so they learn to spot telltale signs of fake emails and requests. Multifactor authentication is turned on everywhere, so even if someone's password is stolen, attackers still cannot get into accounts without a second form of verification. This simple step is one of the most effective ways to stop unauthorised access [3].

Securing IoT Devices and Operational Systems

All connected sensors and machinery will sit on their own separate network, cut off from office systems so a weakness in one device cannot be used to reach core data. We will change every default password before a new device goes live, and keep a full inventory of what is connected, where, and what software it runs. Firmware updates will be applied on a set schedule, with critical security fixes installed within 72 hours. Vulnerability scans will run monthly to spot gaps early.

Preventing Unauthorised Access and Data Loss

Access to folders, files, and tools will be reviewed regularly so people only have permission to see what they need for their work. Restricted files such as designs and specifications will be encrypted, and USB drives will be blocked or restricted on company machines to stop data being copied or leaked unnoticed. We will also keep logs of who accesses sensitive material and when, so unusual patterns can be spotted and investigated quickly [4].

Managing Supply Chain and ThirdParty Risks

Partner or vendor is given access; we will check their security standards match ours. Contracts will state clearly what is and is not acceptable, and outside users will be given only the minimum access they need to complete their work. Connections from outside the company will be limited to secure, controlled channels and watched closely. Any access granted will be timebound and removed as soon as work is finished [5].

Monitoring and Incident Response

The section explains on how we will be able to keep track of what is happening across the system and on how exactly the step needed to be taken should if a security incident occurs.

Continuous Network Monitoring

We will maintain a clear picture of normal activity across the whole network — office systems, production machinery, and cloud tools alike — so anything unusual stands out. Logs from firewalls, servers, and connected devices will be brought together into one central system where automated alerts flag suspicious behaviour such as repeated failed logins or unexpected data transfers. Routine checks are built in too: automated scans run every week to spot known security gaps, and a deeper review takes place every three months. This way, issues are caught early, before they can be exploited. Performance measures such as how quickly we detect and respond to alerts will be tracked, so our monitoring keeps improving over time.

Incident Response Procedure

When an alert appears, the first step is to confirm whether it is a genuine concern or a false alarm. If confirmed as real, the affected systems are isolated straight away to stop whatever is happening from spreading further. Once contained, we work to remove the cause — closing gaps, removing harmful software, or tightening access where needed. Systems are then restored from clean backups and carefully tested before being brought back online, to ensure nothing remains hidden. After the situation is resolved, we look closely at how it happened, what could have been done better, and update our policies accordingly so the same issue does not happen twice. Clear roles are assigned ahead of time which

including an incident lead, communications point of contact, and operational representative — so everyone knows what to do and who to speak to, with no confusion when time is critical.

Training & Awareness

Induction and Ongoing Training

Security awareness will be included as a standard part of every new starter's induction, so safe habits are established from day one. All staff will complete short, regular training sessions each quarter covering key topics such as spotting phishing emails, creating strong passwords, handling company data, and knowing how and where to report anything that looks suspicious. Rolespecific sessions will also be run for the example, procurement teams will learn how to spot supplierrelated scams, while engineering staff will focus on safe use and configuration of connected devices. This keeps training relevant and practical rather than generic or overly technical.

Reinforcement and Compliance

Learning will be backed up with regular, lowkey tests such as simulated phishing emails, so staff can practise what they have learned without real risk. Those who need extra support will receive additional guidance rather than punishment. Quick reference guides, posters, and internal updates will keep key reminders visible around the workplace. Attendance and completion will be recorded, and all staff will confirm each year that they understand and agree to follow these policies, so everyone shares responsibility for keeping the company safe.

Conclusion

SteelForm Manufacturing Ltd's shift toward smart, connected technology brings clear benefits — but it also opens the door to real risks that cannot be ignored. The threats outlined in this report, from ransomware and phishing to insider error and supply chain gaps, are not theoretical: they have already appeared in our recent incidents and could cause serious harm to production, reputation, and customer trust if left unaddressed.

The policies, safeguards, monitoring arrangements, and training programme set out here create a practical, layered defence built around established industry standards. No single measure can guarantee full protection, but working together — separating networks, tightening access, watching for anomalies, and building staff awareness — they significantly reduce risk and make it far harder for attackers to succeed. Equally important is that this approach is not a oneoff fix; it is designed to grow and adapt as our systems and the threat landscape change.

Success will depend on ongoing commitment from across the company. With boardlevel support, consistent implementation, and regular review, this policy will help protect SFM's operations, preserve valuable intellectual property, and support the company's longterm growth and resilience in an increasingly connected world.

Network and Cybersecurity Essentials

Module Name: Network and Cybersecurity Essentials

Module Code: ACCA4024 Student Name: Dolapo Farouk Owolabi Student ID: 2518096 Group: 2

Lecturer's Name: Amit Naik

Introduction

Industry 4.0 and smart technologies have made manufacturing more connected but also more exposed in today's world in technology. SFM now uses IoT, automation, and cloud systems, yet faces malware, phishing, and unauthorised access risks. Protecting production, designs, and reputation is critical. This report sets out a clear cybersecurity and data governance policy, aligned with NIST, ISO 27001, and IEC62443. It identifies threats, defines policies, proposes mitigations, outlines incident response, and plans staff training to strengthen security, maintain operations, and secure SFM's future.

Identification of Threats

The increased interconnectivity across Steel Form manufacturing Ltd.'s IT and operational technology networks has expanded the organisation's attack surface, exposing critical systems and sensitive data to a wide range of cyber threats from both external and internal sources. As manufacturing environments become more integrated with IoT, cloud platforms, and remote monitoring, the distinction between IT and operational boundaries blurs, creating opportunities for adversaries to disrupt production, steal intellectual property, and compromise operational safety [1]. The section identifies and categorises main key threats facing the company, by drawing on established cybersecurity frameworks and manufacturing sector risk assessments.

External Threats

External threats started from actors being outside of the organisation and are among the most rapidly evolving risks facing modern manufacturing. Ransomware and malware are particularly dangerous in industrial settings, where malicious software can target industrial control systems and production machinery to encrypt operational data or lock equipment, halting manufacturing processes and causing significant financial loss through downtime and recovery costs [2]. Phishing attacks remain a common entry point for external actors, frequently targeting procurement and finance teams to trick staff into disclosing credentials or executing malicious files, which can then be used to gain deeper access to internal networks [3]. Industrial espionage and advanced persistent threats pose a serious risk to high-value manufacturing, where competitors or other actors may seek to steal proprietary design data, engineering specifications, and manufacturing processes for commercial advantage [4]. Supply chain

attacks exploit trust relationships with vendors and partners, using compromised third-party access to move laterally into core systems, creating risks that are difficult to detect at the perimeter [5]. IoT and connected devices often introduce technical vulnerabilities due to weak default configurations, unchanged administrative passwords, and a lack of regular firmware updates, providing attackers with accessible entry points into the production environment [6]. Distributed denial-of-service attacks can also disrupt cloud-based production management systems by overwhelming network resources, preventing staff and automated systems from accessing critical operational tools and data [7].

Internal Threats

Internal threats started from within the organisation that are often difficult to detect because they involve legitimate access to systems and information. Human error accounts for a large proportion of security incidents, including accidental misconfiguration of network devices, use of weak or easily guessed passwords, and unintentional data sharing or leakage through email, cloud services, or portable media [8]. Insider threats include both malicious actors and careless users, where employees, contractors, or privileged users may intentionally misuse access privileges to steal data, alter systems, or cause operational disruption, or may compromise security through negligence or lack of awareness [9]. Poor access control practices further increase vulnerability, such as granting excessive permissions beyond what is required for a role and failing to disable accounts promptly after staff departures or role changes, leaving orphaned or unnecessary access in place [10]. Shadow IT — the use of unapproved personal devices, software, or cloud services connected to the corporate or production network — bypasses central security protections and monitoring, introducing unknown vulnerabilities that cannot be patched or managed by the IT team.

Security Policies

Security policies set out clear, actionable rules to protect SteelForm Manufacturing Ltd's systems, data, and production operations. They are built around widely accepted industry standards and designed to close security gaps while keeping daytoday work practical and efficient.

Network and Architecture Policy

Network is split into separate zones such as office IT, production operations, and IoT devices each sit apart from one another, protected by firewalls that stop unauthorised movement between areas. We operate on the basis that no device or user gets automatic trust, even if they are already inside the building; every connection is verified before access is allowed. Remote access and cloud connections must be encrypted and use multifactor authentication to keep entry points secure [11].

Access Control Policy

Staff working for the organisation are given only the access they need to do their jobs, and nothing more. Every account must use multifactor authentication alongside passwords that are at least 12 characters long, changed every 90 days, and never reused across different systems. A check is carried out every quarter to confirm permissions are still appropriate, and accounts are disabled within 24 hours whenever someone leaves or changes role [4].

Data Governance Policy

Information gotten from the network are grouped into four tiers: public, internal, confidential, and restricted. Design files, engineering specifications, and intellectual property fall under restricted — these must be encrypted both when stored and when sent across any network. Data is kept only as long as required, disposed of securely when obsolete, and never shared externally without formal written approval from authorised managers [8].

IoT and Operational Technology Policy

Every connected sensor, smart device, and automated machine must be logged and registered with IT before being plugged in. Default passwords are replaced immediately, and any features or ports not actually needed are turned off to reduce exposure. These devices run on their own isolated network section so that even if one is compromised, attackers cannot easily reach core business or production systems [6].

ThirdParty and Supply Chain Policy

Partner given access to our systems or data must meet the same security expectations we apply internally. Contracts will clearly state these requirements, and outside parties receive only the exact access necessary for their work. All external connections are routed through secure, monitored channels and are logged for audit and review purposes [12].

Mitigation Measures

Threat	Mitigation Measure	Implementation Details
Ransomware / Malware	Endpoint Detection & Response (EDR) + network antivirus; air-gapped immutable backups	Deploy EDR across all servers/PCs; daily incremental + weekly full backups; test quarterly
Phishing	Email filtering + URL rewriting + sandboxing; block known malicious domains	Roll out in 2 weeks; quarantine suspicious emails
IoT Vulnerabilities	Network segmentation + dedicated IoT VLAN; regular firmware patching schedule	Deploy next-gen firewall; monthly vulnerability scans; critical patches within 72h
Unauthorised Access	Zero Trust architecture + MFA everywhere + network access control	Phase 1: MFA for all admins (2w); Phase 2: network segmentation (8w)
Data Breach / IP Theft	Data Loss Prevention (DLP) tools + encryption + strict removable media controls	Deploy DLP; block unauthorised USB; encrypt all Restricted data
Insider Risk	Activity logging + periodic audits + separation of duties	SIEM log retention 12m; quarterly independent reviews
Supply Chain	Vendor security assessment + secure portal for file exchange	Standardised security questionnaire; no unrestricted network access

Protecting Against Ransomware and Malware

Every computer, server, and connected device will be protected with endpoint detection and response tools that watch for unusual behaviour and known threats. Backups are kept separate from the main network — stored offline or in a secure, unlinked location such so systems can be restored cleanly if an attack happens. We take a layered approach: email filtering catches malicious messages before they reach staff, while regular security updates fix known weaknesses. This combination makes it far harder for malware to spread or cause lasting harm [2].

Defending Phishing and Credential Theft

Email security tools will scan incoming messages and flag anything suspicious, isolating it until it can be checked. Staff will also take part in regular awareness sessions, so they learn to spot telltale signs of fake emails and requests. Multifactor authentication is turned on everywhere, so even if someone's password is stolen, attackers still cannot get into accounts without a second form of verification. This simple step is one of the most effective ways to stop unauthorised access [3].

Securing IoT Devices and Operational Systems

All connected sensors and machinery will sit on their own separate network, cut off from office systems so a weakness in one device cannot be used to reach core data. We will change every default password before a new device goes live, and keep a full inventory of what is connected, where, and what software it runs. Firmware updates will be applied on a set schedule, with critical security fixes installed within 72 hours. Vulnerability scans will run monthly to spot gaps early.

Preventing Unauthorised Access and Data Loss

Access to folders, files, and tools will be reviewed regularly so people only have permission to see what they need for their work. Restricted files such as designs and specifications will be encrypted, and USB drives will be blocked or restricted on company machines to stop data being copied or leaked unnoticed. We will also keep logs of who accesses sensitive material and when, so unusual patterns can be spotted and investigated quickly [4].

Managing Supply Chain and ThirdParty Risks

Partner or vendor is given access; we will check their security standards match ours. Contracts will state clearly what is and is not acceptable, and outside users will be given only the minimum access they need to complete their work. Connections from outside the company will be limited to secure, controlled channels and watched closely. Any access granted will be timebound and removed as soon as work is finished [5].

Monitoring and Incident Response

The section explains on how we will be able to keep track of what is happening across the system and on how exactly the step needed to be taken should if a security incident occurs.

Continuous Network Monitoring

We will maintain a clear picture of normal activity across the whole network — office systems, production machinery, and cloud tools alike — so anything unusual stands out. Logs from firewalls, servers, and connected devices will be brought together into one central system where automated alerts flag suspicious behaviour such as repeated failed logins or unexpected data transfers. Routine checks are built in too: automated scans run every week to spot known security gaps, and a deeper review takes place every three months. This way, issues are caught early, before they can be exploited. Performance measures such as how quickly we detect and respond to alerts will be tracked, so our monitoring keeps improving over time.

Incident Response Procedure

When an alert appears, the first step is to confirm whether it is a genuine concern or a false alarm. If confirmed as real, the affected systems are isolated straight away to stop whatever is happening from spreading further. Once contained, we work to remove the cause — closing gaps, removing harmful software, or tightening access where needed. Systems are then restored from clean backups and carefully tested before being brought back online, to ensure nothing remains hidden. After the situation is resolved, we look closely at how it happened, what could have been done better, and update our policies accordingly so the same issue does not happen twice. Clear roles are assigned ahead of time which

including an incident lead, communications point of contact, and operational representative — so everyone knows what to do and who to speak to, with no confusion when time is critical.

Training & Awareness

Induction and Ongoing Training

Security awareness will be included as a standard part of every new starter's induction, so safe habits are established from day one. All staff will complete short, regular training sessions each quarter covering key topics such as spotting phishing emails, creating strong passwords, handling company data, and knowing how and where to report anything that looks suspicious. Rolespecific sessions will also be run for the example, procurement teams will learn how to spot supplierrelated scams, while engineering staff will focus on safe use and configuration of connected devices. This keeps training relevant and practical rather than generic or overly technical.

Reinforcement and Compliance

Learning will be backed up with regular, lowkey tests such as simulated phishing emails, so staff can practise what they have learned without real risk. Those who need extra support will receive additional guidance rather than punishment. Quick reference guides, posters, and internal updates will keep key reminders visible around the workplace. Attendance and completion will be recorded, and all staff will confirm each year that they understand and agree to follow these policies, so everyone shares responsibility for keeping the company safe.

Conclusion

SteelForm Manufacturing Ltd's shift toward smart, connected technology brings clear benefits — but it also opens the door to real risks that cannot be ignored. The threats outlined in this report, from ransomware and phishing to insider error and supply chain gaps, are not theoretical: they have already appeared in our recent incidents and could cause serious harm to production, reputation, and customer trust if left unaddressed.

The policies, safeguards, monitoring arrangements, and training programme set out here create a practical, layered defence built around established industry standards. No single measure can guarantee full protection, but working together — separating networks, tightening access, watching for anomalies, and building staff awareness — they significantly reduce risk and make it far harder for attackers to succeed. Equally important is that this approach is not a oneoff fix; it is designed to grow and adapt as our systems and the threat landscape change.

Success will depend on ongoing commitment from across the company. With boardlevel support, consistent implementation, and regular review, this policy will help protect SFM's operations, preserve valuable intellectual property, and support the company's longterm growth and resilience in an increasingly connected world.

Why Cybersecurity Matters NOW

8 Reasons Cyber Security Is Important

- 1 Cyber Attacks Are Versatile
- 2 Cybercrimes Are Increasing and Evolving
- 3 Tech Users Are Vulnerable
- 4 Cloud Storage Needs Protection
- 5 Cybercrimes Are Costly
- 6 Cyber Security Enhances Credibility
- 7 Viruses Can Harm You or Your Business
- 8 The Dark Web Still Exists

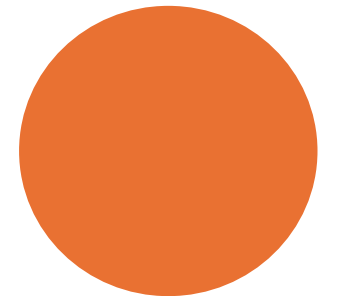
 **Matt Rosenthal, CEO**
IT and Cyber Security Expert



-  We've adopted IoT sensors, automation & cloud systems — boosting efficiency
-  More connections = more vulnerability points for attackers
-  Automotive & aerospace designs = high-value targets for criminals & competitors
-  Manufacturing cyberattacks rising sharply: ransomware, IP theft, supply-chain breaches

Current Situation at SteelForm

- ⚠️ Malware infections on production-network devices
- ⚠️ Phishing emails targeting procurement & finance staff
- ⚠️ Unauthorised access attempts to our production systems
- ❌ Gaps: inconsistent access controls · limited staff training · no unified security policy
- 🚨 Risks: operational downtime · IP theft · contract loss · regulatory penalties



What's At Stake?

- 🏭 Operational: Production halted · delayed shipments · machinery damage
- 💰 Financial: Ransom payments · recovery costs · GDPR/client fines · lost revenue
- ★ Reputational: Lost trust · lost certifications · disqualified from aerospace contracts
- 🕵️ Strategic: Stolen IP · industrial espionage · permanent competitive disadvantage



Proposed Cybersecurity Policy

- 🗝️ Access Control: Least-privilege permissions · multi-factor authentication
- 🛡️ Network Security: Separate IT/OT networks · firewalls · intrusion detection
- 🦠 Threat Protection: Endpoint security · automatic updates · offline backups
- 📋 Incident Response: Clear plan · assigned roles · rapid reporting & recovery
- 🤝 Supply Chain: Security clauses in contracts · vendor security audits



Data Governance: Protect Our Most Valuable Asset

-  Classify: Public → Internal → Confidential → Restricted (designs & client specs)
-  Protect: Encrypt sensitive data · track all access · automatic log retention
-  Cloud & IoT: Secure configurations · encrypted data transmission
-  Compliance: Align with GDPR · ISO 27001 · aerospace industry standards



Recommended Actions & Investment



-  Approve this policy framework today — foundation of all protection
-  Technology upgrades: Firewalls · endpoint protection · secure cloud tools
-  Staff training: Quarterly phishing awareness · security best practices
-  Monitoring: 24/7 threat visibility · quarterly security reviews
-  Budget: Phased investment — see attached breakdown · Modest vs potential losses

Return on investment



Benefits & Return on Investment

- ☒ Minimise downtime & production disruption
- ☒ Protect our IP & competitive advantage
- ☒ Meet client security requirements automatically
- ☒ Strengthen bids for aerospace & automotive contracts
- ☒ Reduce insurance premiums & avoid regulatory fines

CONCLUSION



Conclusion & Request

- Cyber threats to manufacturing are real & growing
- We have seen early warnings — act before disaster
- ☒ Request 1: Approve this Cybersecurity & Data Governance Policy Framework
- ☒ Request 2: Authorise phased implementation budget
- Next steps: Form security working group · Begin quick wins within 30 days

Q&A

