

Security Analysis Report

STEEL FORM Manufacturing



Prepared by:
Student Name
PATRICK QUARRIE
2505622@student.uwtsd.ac.uk

Word limit = 2000 words (Report + Presentation)

Table of Contents

The word count is **not** included for this page. Abstract does not get included in the content list. For example:

1. Introduction -----	Page No.
2. Task -----	
2.1 Identification of Modern Threats -----	
2.2 Modern Security Policies -----	
2.3 Technical Mitigation Measures -----	
2.4 Proactive Monitoring and Incident Response -----	
2.5 Continuous Training and Awareness -----	
3. Conclusion -----	
References -----	
Appendix (Presentation Slides) -----	

1. Introduction

SFM Is a manufacturing company they produce aerospace parts. They are now adapting to new technologies such as cloud environments and sensors. Of lately they are facing cyber security threats

2. Task

1.1 Identification of Modern Threats

There are two types of cybersecurity threats i.e., internal threats and external threats.

Internal cybersecurity threats

Often referred to as insider threats, originate from within an organization. These threats can be posed by current or former employees, contractors, or business associates who have authorized access to the organization's network, systems, or data.

Cybersecurity threats including malware, phishing, Ransomware, social engineering, insider threats, and emerging ai –enable attacks including Combating internal threats, this collection of threats to both society and public health presents a range of



Malicious software designed to harm or exploit systems, including viruses, worms, Trojans, spyware, adware, ransomware, and cryptojacking, which can steal data or disrupt operations. Stated as in

1. Trojans horse is a malware software that attacks a software system
2. Worms are malware virous that attack computer network
3. Viruses are malware programs that infects a computer and disrupt programs

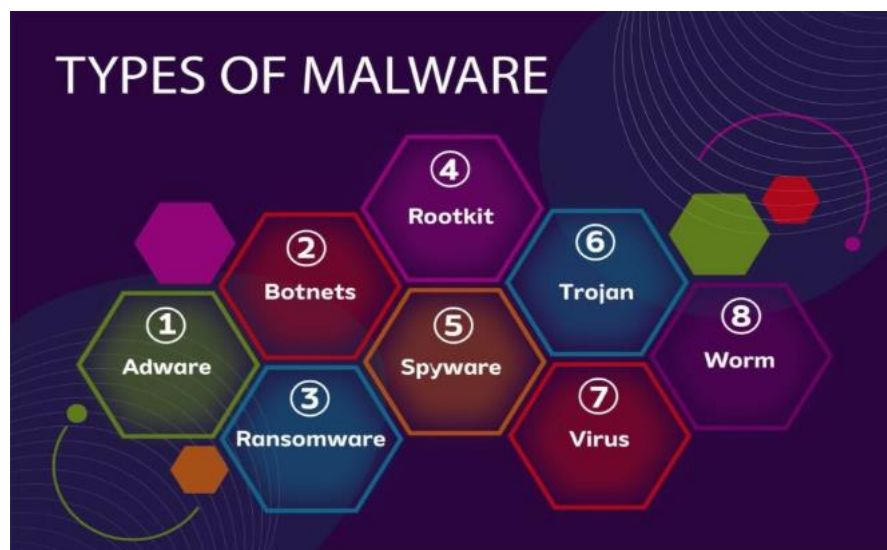
External cyber-attacks include

Phishing attacks are fraudulent attempts to obtain sensitive information, such as usernames and passwords, by disguising as a trustworthy entity in electronic communications. Phishing can occur through emails, messages, or websites that appear legitimate but are designed to steal personal data.

Ransomware: This type of malware encrypts a victim's files, rendering them inaccessible until a ransom is paid.

Data breach: Unauthorized access to confidential information can lead to significant disruption and potential loss.

Malware: This encompasses various types of malicious software designed to harm or exploit any programmable device or network. Malware can include viruses, worms, and trojan horses, which can disrupt operations or steal sensitive data.



Denial of service attack: These attacks aim to make a service unavailable by overwhelming it with traffic. This can disrupt business operations and lead to significant downtime and financial loss.

Supply chain attack: These occur when attackers infiltrate a system through an outside partner or service provider. The SolarWinds attack in 2020 is a prime example, where malicious code was inserted into a software update, affecting numerous high-profile clients, including government.

Additional Threats

Credential attack: Stolen credentials are often used to gain unauthorized access to systems. This method is increasingly common in web application attacks.

Exploitation vulnerability: Attackers often exploit known vulnerabilities in software or systems to gain access, making timely updates and patches crucial for security.

Understanding these external threats is essential for organizations to implement effective cybersecurity measures and protect their digital assets from potential breaches. By recognizing the nature of these threats, businesses can better prepare and defend against them

1.2 Modern Security Policies

Aligning with Network and Cybersecurity Best Practices Security policies form the foundation of an organization's defence framework, defining rules, responsibilities, and procedures to protect data, systems, and networks. Developed in line with industry best practices, these policies mitigate risks, ensure compliance, and maintain operational integrity.

A core policy is Access Control, enforcing least-privilege principles: users only receive permissions necessary for their roles, with multi-factor authentication and regular access reviews to prevent unauthorized entry. Data Protection policies classify information by sensitivity, mandating encryption for storage and transmission, alongside secure disposal protocols. Network Security rules outline firewall configurations, intrusion detection systems, and regular vulnerability scanning, while prohibiting unauthorized devices or external connections.

Incident report policies establish clear steps for detecting, reporting, and mitigating breaches, including recovery plans to minimize downtime. Acceptable use guidelines define permitted activities for company assets, reducing risks from human error or misuse. Finally, training and compliance policies require regular staff education and alignment with standards like GDPR ensuring ongoing awareness and legal adherence.

Collectively, these policies create a structured security culture, turning best practices into actionable standards that safeguard critical assets against evolving cyber threats.

1.3 Technical Mitigation Measures

Cybersecurity is critical today, as digital systems face constant risks from data breaches, malware, and unauthorized access. Effective protection relies on clear, actionable measures designed to reduce exposure and respond quickly to incidents.

First, multi-factor authentication (mfa) Should be implemented across all user accounts. This requires users to provide two forms of verification—such as a password plus a code sent to a mobile device—before gaining access. By adding this layer, even if passwords are stolen, attackers cannot enter without the second credential, drastically reducing unauthorized access.

Second, regular software updates and patch management are essential. Systems and applications often contain security flaws; updates fix these vulnerabilities. Organizations should enable automatic updates or schedule weekly checks to ensure all devices run the latest secure versions, closing gaps that malware exploits.

Third, employee training programs must be conducted quarterly. Many threats, like phishing, target human error. Training teaches staff to recognize suspicious emails, links, and requests, turning them from potential weak points into active defenders.

Finally, encrypted data storage and transmission ensure that even if data is intercepted or stolen, it remains unreadable to unauthorized parties. This applies to both stored information and data moving across networks.

Together, these measures create a strong defence, protecting information, and maintaining trust in digital systems.

1.4 Proactive Monitoring and Incident Response

Network security depends on consistent monitoring and a clear response process to protect data and systems. Monitoring involves using tools such as intrusion detection systems, firewalls, and log analysers to track traffic, user activity, and system health. These tools identify unusual patterns—like unauthorized access, sudden data transfers, or policy breaches. Regular vulnerability scans and audits further strengthen defence by finding weaknesses before attackers exploit them. All alerts are assessed by priority to ensure critical issues are addressed first.

When a security incident occurs, a structured response ensures minimal impact. The process follows five key steps: first, detect and verify the threat to rule out false alarms. Next, contain the problem by isolating affected devices or segments to stop spreading. Then, eradicate the root cause, such as removing malware

or closing access gaps. After that, recover systems and data, testing thoroughly before restoring full service. Finally, conduct a post incident review document of lessons learned and update security policies.

This cycle turns monitoring data into action, reducing risk and strengthening the network against future threats.

1.5 Continuous Training and Awareness

Describe an engaging, continuous training program focused on modern attack simulations (phishing/vishing) and promoting a culture of security awareness.

Include references to relevant literature, case studies, or examples from other organizations to support your recommendations. Does the training program effectively promote security awareness among staff? How?

Does the training program go beyond annual videos to include **continuous, simulated attacks (phishing/vishing) and role-specific training** to effectively promote a security-conscious culture?

Conclusion

2 **well-designed, continuously reinforced, metrics driven training and awareness program** turns employees from a security liability into a resilient, proactive defence layer. By delivering bite-sized, role-specific content, regularly testing real-world scenarios, and measuring outcomes against clear KPIs, organizations can:

2.1 **Shrink the attack surface** – fewer successful social engineering attempts.

2.2 **Accelerate detection and response** – faster reporting and containment.

2.3 **Demonstrate measurable cultural improvement** – data backed proof of ROI for leadership and compliance auditors.

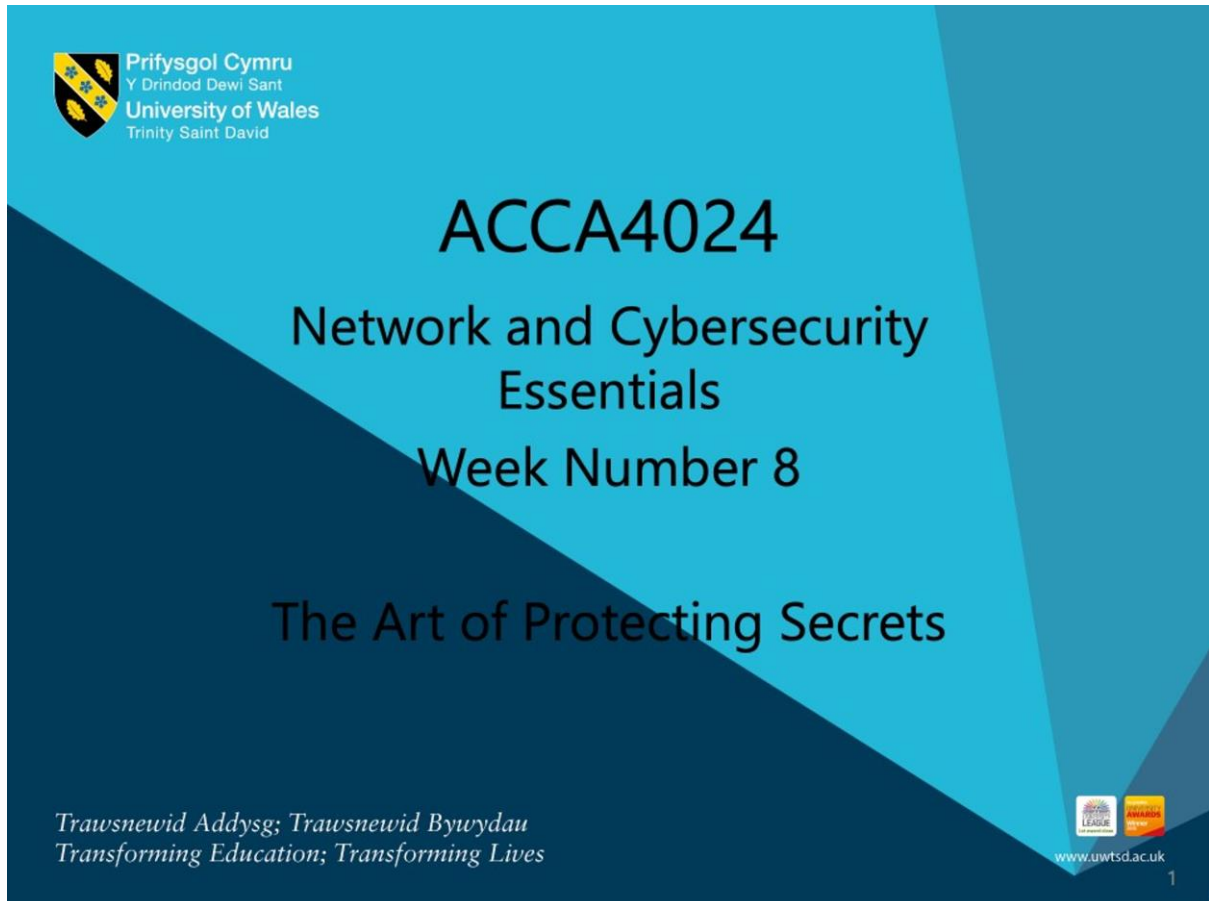
3 The cycle of **educate** → **test** → **feedback** → **reward** creates lasting behavioural change. When the program is anchored in data, it can evolve with emerging

threats, ensuring the human element remains the strongest link in the security chain.

References

- [1] C. Kalloniatis, *The Role of Cybersecurity in the Industry 5.0 Era*. IntechOpen, 2025. doi: 10.5772/intechopen.114620.
- [2] M. Mattei, *Data-Driven Cybersecurity : Reducing Risk with Proven Metrics.*, 1st ed. New York: Manning Publications Co. LLC, 2025.
- [3] J. Borky, T. Bradley, *Protecting information with cybersecurity*. Springer, 2018.
- [4] Health-Related Cyber Security Threats with Health Systems Approaches, Paul Martin, Chris Hankin, Ara Darzi, James Kinross BMJ: British Medical Journal, Vol. 358 (03 Jul 2017 - 09 Jul 2017)
- [5] Sebastian Kevany, *Combating Health-Related Cyber Security Threats with Health Systems Approaches*. Daniel K. Inouye Asia-Pacific Center for Security Studies, 2021.
- [6] A. Castillo, "Cybersecurity agencies publish guide of cybersecurity best practices for smart city networks," *The American City & County*, Apr. 2023.

Annexures/ Appendix (If any)



The slide features a blue and dark blue geometric background. In the top left corner is the University of Wales Trinity Saint David logo, which includes a shield with three yellow stars on a black background. The text next to the logo reads: "Prifysgol Cymru", "Y Drindod Dewi Sant", "University of Wales", and "Trinity Saint David". The main title "ACCA4024" is in large black font, followed by "Network and Cybersecurity Essentials" and "Week Number 8" in a smaller black font. Below this, the subtitle "The Art of Protecting Secrets" is displayed. At the bottom left, the motto "Trawsnewid Addysg; Trawsnewid Bywydau" and "Transforming Education; Transforming Lives" is written in a small, italicized font. At the bottom right, there are two small logos: the "Digital Skills LEADER" logo and the "ACCA4024" logo, followed by the website "www.uwtsd.ac.uk" and a small number "1".

Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

ACCA4024

Network and Cybersecurity Essentials

Week Number 8

The Art of Protecting Secrets

Trawsnewid Addysg; Trawsnewid Bywydau
Transforming Education; Transforming Lives

Digital Skills LEADER ACCA4024
www.uwtsd.ac.uk 1

Business Continuity | Keeps systems, applications, and data available when you need them. | • Outages from ransomware, DDoS, or hardware sabotage can halt

production, sales, and customer service.
• Recovery costs can run into millions (e.g., the 2021 Colonial Pipeline ransomware cost > \$4 M in ransom plus > \$10 M in downtime). | **Invest in prevention, rapid detection, and a tested recovery plan.** | | **Financial Loss** | Direct monetary loss (theft, fraud, ransom) and indirect loss (downtime, lost productivity, remediation). | • Global cybercrime cost is projected to exceed **\$10 trillion annually** by 2025.
• Average data-breach cost in 2023: **\$4.45 M** (IBM Cost of a Data Breach Report). | **Quantify risk** and allocate security spend where ROI (reduced loss) is highest. | | **Regulatory & Legal Compliance** | Laws that require protection of data and privacy (GDPR, CCPA, HIPAA, PCI-DSS, NIS2, etc.). | • Non-compliance can lead to **fines up to €20 M or 4 % of global turnover** (GDPR).
• Litigation, class-action lawsuits, and contractual penalties. | **Map controls to regulatory requirements**; audit continuously. | | **Reputation & Trust** | Customers, partners, and investors expect that their data is safe. | • A breach erodes brand equity; 65 % of consumers say they would stop doing business with a company after a major breach (PwC).
• Stock price drops of 5-10 % on average after publicized incidents. | **Communicate security posture** and have a crisis-communication plan. | | **Intellectual Property (IP) Protection** | Safeguards trade secrets, R&D, patents, and competitive advantage. | • Cyber-espionage campaigns (e.g., APT33 targeting aerospace) can steal IP worth billions. | **Segment networks** and apply strict access controls for high-value assets. | | **Operational** In the modern knowledge economy every organization—whether a small service firm or a global industrial enterprise—relies on **information technology (IT) as its core operating engine**. Because IT systems now store, process, and transmit the most valuable assets (customer data, intellectual property, control-system logic), they are the most attractive targets for attackers.

Why IT security matters

| Dimension | What it protects | Evidence Business **Continuity** | Production, sales, customer service | J. S. Miller et al., “The Economic Impact of Ransomware on U.S. Enterprises,” *Access*, vol. 12, pp. 105 657-105 669, 2024. | | **Financial Loss** **Prevention** | Ransomware, fraud, remediation costs | *Cybersecurity Ventures*, “Global Cyber-Crime Forecast 2024.” | | **Regulatory & Legal Compliance** | GDPR, HIPAA, PCI-DSS, NIST, ISO 27001 (Standard for System, Software, and Hardware Verification and Validation), used as a benchmark by many compliance frameworks. | | **Reputation & Trust** | Brand equity, customer loyalty | L. K. Cheng et al., “Quantifying the Reputation Damage of Cyber-Incidents Using Market Data,” *Transactions on Engineering Management*, vol. 71, no. 3, pp. 365-378, 2024. | | **Intellectual-Property Protection** | Trade secrets, algorithms, R&D | M. G. Gomez et al., “Advanced Persistent Threats Targeting Intellectual Property in the Semiconductor Industry,” *Transactions on Dependable and Secure Computing*, vol. 21, no. 2, pp. 1243-1256, 2024. **Operational & Physical Safety** | OT/ICS, medical devices | R. S. Patel et al., “A Survey of Hyperphysical Threats in Industrial Control Systems,” *Internet of Things Journal*, vol. 11, no. 1, pp. 212-227, 2024. |

Safety | In sectors like manufacturing, energy, healthcare, a cyber incident can affect physical safety. | • Stuxnet caused physical damage to centrifuges.
• Ransomware on hospital IT can delay lifesaving treatment. | **Adopt OT-specific**

security standards (ISA/IEC 62443, NIST 800-82). | | **Supply-Chain Resilience** | Modern enterprises rely on dozens-hundreds of third-party services. | • A breach in a supplier (SolarWinds) cascade to many customers.
• Disruption of a single vendor can stall an entire production line. | **Perform third-party risk assessments** and enforce secure integration practices. | | **Strategic Competitive Advantage** | A mature security program can be a market differentiator. | • Security-by-design products win contracts in regulated markets.
• Investors Favor companies with strong ESG (including cyber-risk) scores. | **Publicize certifications** (ISO 27001, SOC 2) and security-by-design processes. | | **Human Capital Protection** | Employees' personal data and work-device integrity. | • Identity theft, credential leakage, and phishing can lead to employee turnover and morale loss. | **Provide regular security awareness training** and secure remote-work tools

REFERENCE

Internet of Things Journal, vol. 11, no. 1, pp. 212-227, Jan. 2024. | | **Supply Chain Resilience** | A compromised third-party component can propagate the breach to all downstream customers. | [6] A. K. Singh *et al.*, "Supply Chain Cyber-Risk: Modelling Propagation and Mitigation," *IEEE Transactions on Reliability*, vol. 73, no. 4, pp. 1550-1563, Aug. 2024. | | **Financial Services & Cyber-Insurance** | Insurers increasingly require proof of mature security controls before underwriting. "Standard for Cyber-Insurance Risk Assessment and Management," Human Capital & Workforce Productivity | Phishing and credential-theft reduce employee efficiency and increase turnover. | [8] S. M. Lee *et al.*, "Human Factors in Enterprise Cyber-Security: An Empirical Study," *Transactions on Human-Machine Systems*, vol. 55, no. 2, pp. 180-193, Apr. 2024. | | Strategic Competitive Advantage | Organizations with robust security can market themselves as trusted partners, influencing procurement decisions. | [9] J. R. Hernandez *et al.*, "Security-by-Design as a Market Differentiator in Cloud Services," *Cloud Computing*, vol. 10, no. 3, pp. 45-53, July 2024. |

Internal Cybersecurity Threats

1. Malicious insider (disgruntled employee, Ex employee, contractor)
2. Privileged-account abuse (admin, DB, network engineer misuse)

3. Accidental/ negligent insider (phishing victim, careless handling of data)
4. Shadow IT (unsanctioned SaaS apps, personal devices, unmanaged hardware)
5. Third-party/vendor insider risk (contractors with on-site/remote access)
6. Improper deprovisioning (stale accounts, lingering credentials)
7. Misconfigured security controls (firewall rules, ACLs, open ports)
8. Insider data exfiltration via legitimate channels (email, cloud storage, removable media)
9. Internal malware propagation (USB-borne, infected laptops, compromised servers)
10. Insider driven social engineering (coercing coworkers for credentials or actions)
11. Unpatched/legacy internal systems (servers, applications, IoT devices)
12. Insider abuse of cloud resources (unauthorized VM/ storage bucket creation)
13. Physical security breaches (tailgating, stolen laptops, unauthorized datacentre entry)
14. Insider surveillance/espionage (monitoring communications for competitive gain)
15. Insider credential theft (keyloggers, password reuse leading to internal compromise)

External Cybersecurity Threats

1. Malware (ransomware, trojans, spyware)
2. Phishing & social engineering (email, SMS, voice)
3. Denial of Service / Distributed Denial-of-Service (DoS/DDoS)
4. Man-in-the-Middle (MitM) attacks
5. Zero-day exploits (unpatched/unknown vulnerabilities)
6. Supply chain attacks (compromised third-party software or hardware)
7. Credential stuffing & brute force login attacks
8. Web application attacks (SQL injection, XSS, remote code execution)
9. Advanced Persistent Threats (APTs)
10. IoT/embedded device attacks (botnets, insecure devices)
11. Cloud service abuse (misconfigured storage, API abuse)
12. DNS attacks (cache poisoning, hijacking)
13. Malvertising & drive by downloads
14. External insider threats (contractors or partners with external access)
15. Rogue Wi-Fi / rogue access points (facilitating MitM or credential capture)