1. What is your assessment of malware infection at the SME Hypothetical Inc?

Multiple controls need to be implemented to improve Hypothetical Inc's security posture and better ensure the confidentiality of sensitive information. See table below for list of recommended measures.

The firewall should be set to lock down traffic until the malware incident is contained and passwords are changed, to prevent exfiltration of data or further breaches. Images of the infected devices should also be made for forensic investigation purpose, and the police and CSA should be contacted and relevant evidence shared for learning and co-ordination purpose. The company can also co-ordinate with SingCert to contain the situation.

Top 3 measures in the immediate phase: contain malware and ransomware infection (and prevent future infections with **EDR**, **MDR** and **XDR** tools), change passwords, ensure integrity of backups. Top 3 measures in the longer term phase: implement multi-factor authentication; regular monitoring, maintenance and intervention for legacy systems; set up next generation firewall.

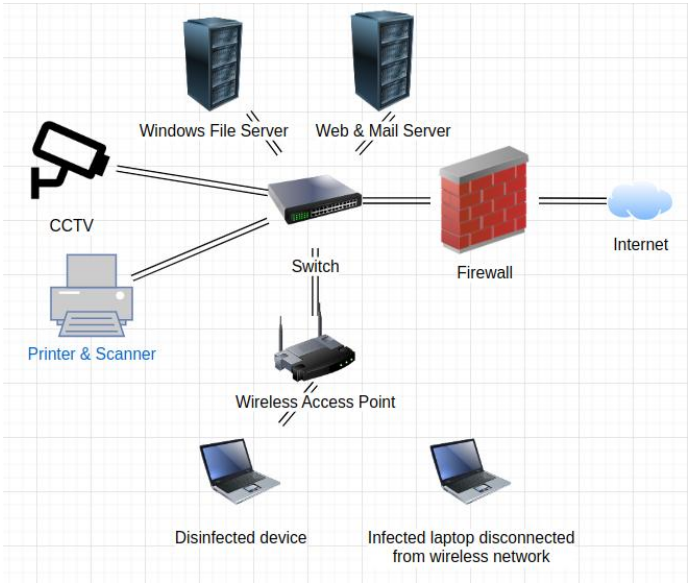

Image 2a. Redesigned network diagram for phase one. Infected machine(s) disconnected from network and firewall is locked down until malware/ransomware infection is contained and passwords are changed. Only disinfected devices should have access to internet.

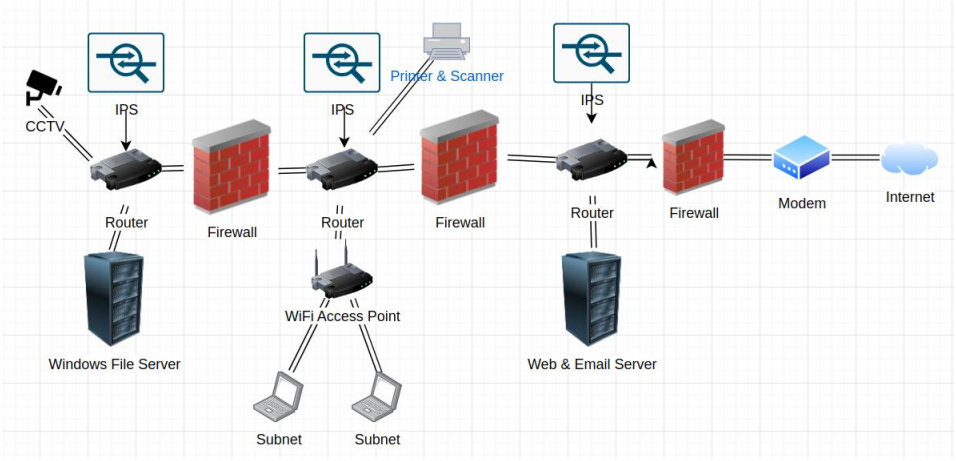

Image 2b. Redesigned network diagram for phase two. Intrusion protection systems and internal firewalls installed, picture of laptop represents laptops connected to particular subnet.

Table 1: Mitigation Measures for Hypothetical Inc

Phase/Priority	Proposed Measure	Rationale	Estimated Cost
1.1 Response Administrative Preventative	Change passwords, adhere to strong password creation policy and change passwords every 6 months	Access control for sensitive data, services. Protect the network from ex-employees with insider knowledge.	Free
1.1 Response Technical Corrective Preventative	Regular firewall maintenance	Firewall rules should be updated regularly, especially during an incident to prevent possible data ex-filtration.	Free
1.2 Plans Administrative Corrective	Create/update disaster recovery plan, simulate incidents, and update playbooks	Ensure robust disaster recovery and business continuity plans in event of different security incidents.	Free
1.3 Authorization Administrative Auditing Preventative	Separation of duties	Access control and audit trail for sensitive data, services. Limit the possibility of fraud/access to critical data.	Free
1.3 Authorization Administrative Preventative	Principle of least privilege	Authorisation and access control for sensitive data, services. Limit access to reduce the risk of additional breaches. Only authorised users should have access to sensitive data/services, and only for the purpose of doing their jobs.	Free
1.2 Data Mgmt. Administrative Detective	Asset inventory, classification of assets (restricted, confidential, internal-only, public)	Access control for sensitive data. Identify information which should be kept private/ secure.	Free
1.3 Authorization Administrative Preventative	Access control policies	Protect confidentiality and integrity of data by deciding who can access or modify it	Free
1.4 Data Mgmt. Technical Deterrent Preventative	Encryption	Access control for sensitive data. Especially to protect restricted or confidential data in event of a breach.	Free
1.2 Data Mgmt. Administrative Corrective	Backups	Regular backups of data and systems ensure business continuity in event of a breach.	Low, cost of backup media or cloud storage for encrypted backups.

1.1 Endpoint Technical Corrective	Endpoint detection and response (EDR), managed detection and response (MDR) and extended detection and response (XDR) tools	Replacement for existing breached anti-malware solution. Should enable cloud detection, and may be used to help contain and eradicate existing malware and ransomware infections, and prevent future infections. If possible, infected systems should be isolated and reverted to known safe baseline images once data has been backed up.	Free trial for some EDR solutions like MalwareBytes EDR, otherwise vendor dependent. Contact vendors for pricing.
1.1 Endpoint Technical Preventative	Prompt installation of patches/updates	Helps prevent future malware breaches.	Free
2.1 Authentication Technical Preventative	Multi-factor authentication	Defense in depth measure to prevent a breach in event of password compromise.	Varies with vendor. Contact vendors for pricing.
2.2 Monitoring & Operations Administrative Detective Preventive	Regular monitoring, maintenance and intervention for legacy or industrial control systems	Limit extent of damage in event of security breach. Vulnerable legacy or industrial control systems should not be connected to internet networks.	Possibly free for configuration of legacy systems, possibly vendor and intervention dependent.
2.2 Monitoring & Operations Technical Detective	Security operations centre, security information event monitoring (SIEM), IDS, and security orchestration automation response (SOAR) tools	Help to semi-automate monitoring, and ensure consistent and adaptive response to contain incidents.	Vendor dependent. Contact vendors for pricing. Some Intrusion Detection Systems like Suricata and Snort are free.
2.3 Network Technical Preventative	Network segmentation and internal network firewall	Isolate sensitive data/services and helps to contain extent of possible security breaches.	Low for cost of router hardware. Vendor dependent for next generation network firewall. Contact vendors for pricing.
2.3 Network Technical Preventative	Require secure mobile devices and use of VPN to work remotely	Endpoint detection and response tools and VPN helps prevent security incidents due to breach of mobile devices or man-in-the-middle attacks.	Free
2.3 Network Technical Preventative	Intrusion protection system	Helps prevent simple possible intrusion by threat actors.	Free to vendor-dependent. Free solutions like Suricata, or contact vendors for pricing.
2.3 Network Technical Preventative	Next generation firewall	A next generation firewall can be used to block malware and provide integrated intrusion prevention system service.	Varies with vendor. Contact vendors for pricing.

2.4 Data Mgmt. Technical Preventative	Secure disposal	Helps prevent data exfiltration by threat actors.	Free
2.5 Physical Deterrent	Surveillance and signage (CCTV, sign boards stating that area is secured)	Discourage physical security breaches.	Vendor dependent. Contact vendors for pricing.
2.5 Physical Preventative	Badge readers, locks	Prevent physical security breaches	Vendor dependent. Contact vendors for pricing.
2.5 Physical Corrective Preventative	Fire sprinklers, time controlled safe	Limit extent of damage in event of an incident.	Vendor dependent. Contact vendors for pricing.

Reflection on Measures

The measures synergize and co-ordinate to provide multiple layers of protection per the defense in depth strategy.

There are a lot of measures listed. I separate and group them by type and organise them logically to better reflect on them in order to improve understanding and ability to generalise to new situations.

1.1 Goal (Why)
Responsive (immediate response to limit extent of damage)
Data Management (identify what assets require what kinds of protection and from whom)
Planning (protection playbooks, disaster recovery, business continuity plans)

1.2 Security Elements (What)
Authentication, Authorization, Auditing (protective, detective)
Monitoring & Operations (detective and responsive)

1.3 Location (Where)
Physical: In the real world.
Network: Online.
Endpoint: On the device.

2.1 Type of Agent (Who)
Administrative/Managerial: Human component of cybersecurity. Policies/procedures that define employee responsibilities, how organization manages risk and resources.
Technical: Software solutions.
Physical: Hardware solutions.

2.2 Stage (When)
Corrective: Remedy incidents after they occur.
Detective: Identify incidents after they occur.
Deterrent: Discourage incidents before they occur.
Preventative: Stop incidents before they occur.

These measures are only listed on paper but have yet to be tested in a prolonged audit, such as an SOC class 2 type 2 audit [3].

Reflection on Priorities/Phases

Immediate Phase
1.1 Security hole patching to prevent breaches
1.2 Identifying and backing up data before and in case of breach, planning what to do in response to breach
1.3 Access control: Authorization and auditing best practices to detect and limit breaches
1.4 Encryption to limit the extent of damage in event of a breach
Longer-term Phase
2.1 Priority access control (authentication) to prevent breaches
2.2 Measures that primarily detect or respond to pre-emptive detection of breaches
2.3 Additional network measures to prevent breaches
2.4 Additional data management measures to prevent breaches
2.5 Additional physical measures to prevent breaches

Compliance with International Payment Card Industry Data Security Standard (PCI DSS)

1. Only authorised users have access to customers' credit card information.
2. Credit card information is internally transmitted, accepted, processed and stored in a secure environment.
3. Enforce secure password management policies.
4. Encrypt credit card information at transaction touchpoints.

Compliance with European Union General Data Protection Regulation (GDPR)

The GDPR is a European law that was enacted on 25 May 2018, and affects businesses targeting or doing business with European customers. The GDPR applies to companies outside the EU dealing with EU customers located outside the EU, regardless of the size or industry of the company [4]; this means that Singaporean or American small companies dealing with EU customers are also subject to the GDPR, although enforcement usually targets larger companies.

1. EU customers' data access is kept private and secure.
2. Enforce privacy policies, procedures and processes to properly document, maintain and process data. Grant data subjects the right to revoke consent [1], request erasure [1], update records [1] and opt out of profiling [2] or data processing [1].
3. Ensure data is properly classified and inventoried.
4. There is a plan in place to notify customer(s) within 72 hours if a breach occurs.

Compliance with the American Institute Certified Public Accountants (AICPA) Service Organization Control (SOC) Type 1 and Type 2 [3]

1. User access policies are established.
2. Data is only available to users authorised to access it.
3. Sensitive data (personally identifiable information, sensitive personally identifiable information such as medical records, political affiliation and religious belief) is private and secure.
4. Ensure data integrity, ensure that data is validated, consistent, accurate and complete.

Reflection on Compliance Checklists Best Practices

The emphasis is on ensuring access controls are in place, such that users can only access the data they need and only have privileges to access/modify the data they require for their jobs. Effort, such as encryption, is made to secure the confidentiality of the system. Password management systems are used to prevent passwords fatigue and increase password security.

The integrity of the system is improved by validating information and giving users the opportunity to correct records.

Privacy is respected by requiring consent to store or process data.
Users are promptly notified if a breach occurs.

References

1. Proton Technologies (2023) GDPR compliance checklist - https://gdpr.eu/checklist/.
2. IT Governance Ltd (2022) EU GDPR summary |What is the GDPR? https://www.youtube.com/watch?v=I-VuonciKWk.
3. Mike Chapple (2021) CertMike explains SOC audits. https://www.youtube.com/watch?v=KIE2grb4qo0.
4. Steinberg, J. (2020) Cybersecurity For Dummies. John Wiley & Sons. ISBN 978-1-119-56032-6. GDPR: pg. 166.