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.

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.

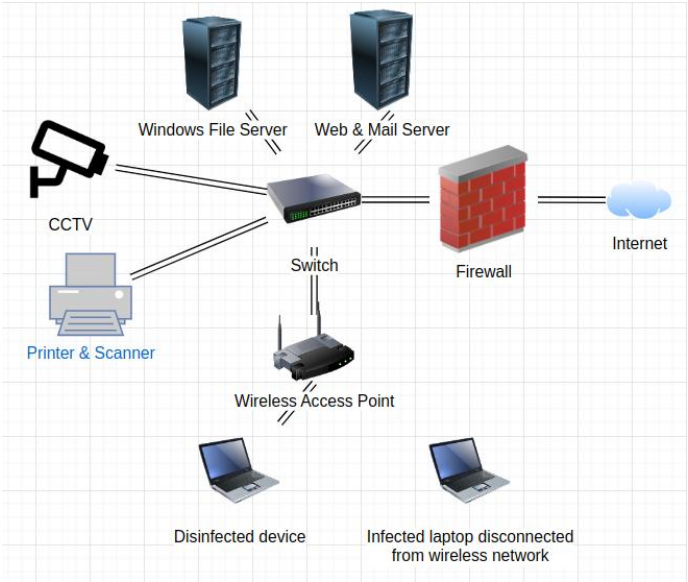

Image 2a. Redesigned network diagram for phase one. Infected machine(s) disconnected from network and firewall is locked down until malware/ransomware infection is contained and passwords are changed. Only disinfected devices should have access to internet.

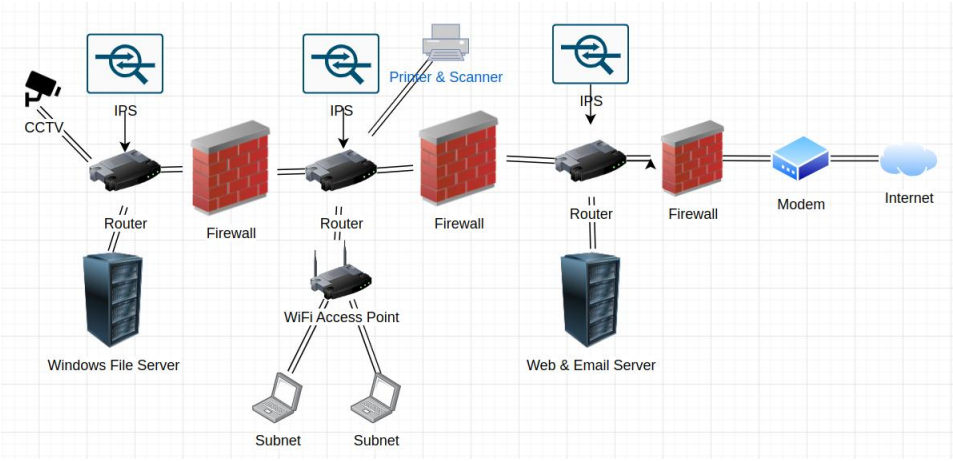

Image 2b. Redesigned network diagram for phase two. Intrusion protection systems and internal firewalls installed, picture of laptop represents laptops connected to particular subnet.

Table 1: Mitigation Measures for Hydrogen Inc

Phase	Proposed Measure	Rationale	Estimated Cost
1.1	Change passwords, adhere to strong password policy and adhere to policy to regularly change passwords every 6 months	Access control for sensitive data, services. Protect the network from ex-employees with insider knowledge.	Free
1.2	Separation of duties	Access control and audit trail for sensitive data, services. Limit the possibility of fraud/ access to critical data.	Free
1.2	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
1.3	Create/update disaster recovery plan, simulate incidents, and update playbooks	Ensure robust business continuity plans in event of different security incidents.	Free
1.3	Asset inventory, classification of assets (restricted, confidential, internal-only, public)	Access control for sensitive data. Identify information which should be kept private/secure.	Free
1.4	Encryption	Access control for sensitive data. Especially to protect restricted or confidential data in event of a breach.	Free
1.4	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.
1.5	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.	Free trial for some EDR solutions like MalwareBytes EDR, otherwise vendor dependent. Contact vendors for pricing.
1.5	Prompt installation of patches/ updates	Helps prevent future malware breaches.	Free
1.1	Regular firewall maintenance	Firewall rules should be updated regularly, especially during an incident to prevent possible data ex-filtration.	Free

2	Multi-factor authentication	Defense in depth measure to prevent a breach in event of password compromise.	Varies with vendor. Contact vendors for pricing.
2	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	Security operations centre, security information event monitoring (SIEM) 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.
2	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	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	Physical security measures (locks, fire sprinklers)	Prevent physical security breaches and limit extent of damage in event of an incident.	Vendor dependent. Contact vendors for pricing.
2	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	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	Secure disposal	Helps prevent data exfiltration by threat actors.	Free