1. **Chosen CII:** Healthcare
2. **Potential threats chosen CII faces:**

Technological threats: Phishing malware [1] (such as Trojan Horses, spyware, viruses, worms); Ransomware [2], non-ransomware denial of service [2], distributed denial of service; identity theft, data breaches [5]; internet of things medical device exploitation [4], diagnostic medical device exploitation [2], advanced persistent threats, zero-day exploits [2].

Threat actors: organised criminal syndicates, nation state backed agents [2][3]

3. **Tactics cyber criminals are using:**

Phishing: emails impersonating the World Health Organization or Center for Disease Control and prevention, or referring to fake purchases of personal protective equipment [1], or fake offers of N95 masks and ventilators [2]. Phishing switching from targeting administrators to targeting clinicians and hospice workers [1].

Zero-day exploits [2]

4. **Steps to mitigate threats:**

Identity verification technology and training: implementing email authentication technology such as domain based message authentication reporting and conformance (DBMARC) [1].

Perimeter and application level: strong authentication policies and technology, controlling access to protected health info, requiring authentication to receive authorisation to access data and services, securing password and adhering to regular password change policy, using **multi-factor authentication**.

Network level: requiring virtual private networks to connect to office remotely, deploying network segmentation to contain damage from intrusions, and using intrusion protection systems.

End-point level: installing updates and patches promptly, using cloud enabled Endpoint Detection Response (**EDR**) software to serve as anti-malware solution and **next generation firewall** services to block malware and intrusions, augmenting EDR software with Managed Detection and Response (**MDR**) and eXtended Detection and Response (**XDR**) tools [6], securing mobile devices and employee personal devices.

Data level: **encrypting** sensitive information, maintaining regular encrypted backups; maintaining a physical **air-gap** for restricted or highly confidential information and **legacy or vulnerable industrial control** networks to guard against zero-day exploits.

General measures: implementing a security culture, investing in threat simulation and training of all staff; investing in cybersecurity through setting up security information and event monitoring (SIEM) tools and security orchestration automation and response (SOAR) tools, and hiring and training cybersecurity personnel; keeping security playbooks updated; sharing information with government agencies like CSA, police cyber crime department;

adhering to principles of least privilege and separation of duties; ensuring regular auditing of policies, standards and procedures for compliance with industry best practices and frameworks like National Institute of Standards and Technology **Cybersecurity Framework**, auditing regularly to review privileged activities and review privileges, closing or limiting accounts of personnel no longer working with the organisation, hiring penetration testers regularly; investing in physical security [5].

5. **Sources**

[1] Grimes, B. (2020) 'How cybercriminals are exploiting the pandemic (and how to stop them),' Technology Solutions That Drive Healthcare, 15 Oct 2020. https://healthtechmagazine.net/article/2020/10/how-cybercriminals-are-exploiting-pandemic-and-how-stop-them.
[2] Riggi, J. (2020) Ransomware attacks on hospitals have changed | Cybersecurity and Risk Advisory Services | American Hospital Association (Circa May 2020). https://www.aha.org/center/cybersecurity-and-risk-advisory-services/ransomware-attacks-hospitals-have-changed
[3] CNBC Television (2021) What to know about a ransomware group that's targeting the healthcare industry. https://www.youtube.com/watch?v=3isz4nP_28M.
[4] SANS Institute (2022) SANS Healthcare Forum 2022: Healthcare IoT and OT Vulnerabilities. https://www.youtube.com/watch?v=J-lL1cEbqlY.
[5] HealthCareITNews (2018) Hackers breach 1.5 million Singapore patient records, including the prime minister. https://www.healthcareitnews.com/news/asia/hackers-breach-15-million-singapore-patient-records-including-prime-ministers.
[6] CrowdStrike (2023) EDR vs MDR vs XDR: Everything You Need To Know. https://www.crowdstrike.com/cybersecurity-101/endpoint-security/edr-vs-mdr-vs-xdr/.