

Recommendation #13: An internet access strategy that minimises exposure to external threats should be implemented

- The internet access strategy should be considered afresh, in the light of the Cyber Attack.
- In formulating its strategy, the healthcare sector should take into account the benefits and drawbacks of internet surfing separation and internet isolation technology, and put in place mitigating controls to address the residual risks.

Recommendation #14: Incident response plans must more clearly state when and how a security incident is to be reported

- An incident response plan for IHiS staff must be formulated for security incidents relating to Cluster systems and assets.
- The incident response plan must clearly state that an attempt to compromise a system is a reportable security incident.
- The incident response plan must include wide-ranging examples of security incidents, and the corresponding indicators of attack.

Recommendation #15: Competence of computer security incident response personnel must be significantly improved

- The Computer Emergency Response Team must be well trained to more effectively respond to security incidents.
- The Computer Emergency Response Team must be better equipped with the necessary hardware and software.
- A competent and qualified Security Incident Response Manager who understands and can execute the required roles and responsibilities must be appointed.

Recommendation #16: A post-breach independent forensic review of the network, all endpoints, and the SCM system should be considered

- IHiS should consider working with experts to ensure that no traces of the attacker are left behind.
-