APPENDIX

16 RECOMMENDATIONS FROM SINGHEALTH COI REPORT

(extracted from "Public Report of the Committee of Inquiry Into the Cyberattack on Singapore Health Services Pte Ltd's Patient Database on or around 27 June 2018, published on 10 Jan 2019)

Arising from the cyberattack on Singapore Health Service Pte Ltd's patient database and its key findings, the COI made sixteen recommendations, comprising seven Priority Recommendations and nine Additional Recommendations:

(i) The seven Priority Recommendations include strategic and operational measures to uplift the cybersecurity posture of SingHealth and IHiS, and steps must be taken to implement these Priority Recommendations immediately; and

(ii) The nine Additional Recommendations relate to other specific concerns raised in the course of this Inquiry, including technical, organisational, training, and process- related issues. The measures, which are similarly aimed at uplifting the cybersecurity posture of SingHealth and IHiS, must be implemented or seriously considered.

For IHiS, SingHealth and other organisations responsible for large databases of personal data, getting the fundamentals right is a necessary and vital step in building cybersecurity competencies and the ability to counter the real, present, and constantly evolving cybersecurity threats.

(I) Priority Recommendations

Recommendation #1: An enhanced security structure and readiness must be adopted by IHiS and Public Health Institutions

- Cybersecurity must be viewed as a risk management issue, and not merely a technical issue.
- Decisions should be deliberated at the appropriate management level, to balance the trade-offs between security, operational requirements, and cost.
- IHiS must adopt a "defence-in-depth" approach.
- Gaps between policy and practice must be addressed.

Recommendation #2: The cyber stack must be reviewed to assess if it is adequate to defend and respond to advanced threats

- Identify gaps in the cyber stack by mapping layers of the IT stack against existing security technologies.
- Gaps in response technologies must be filled by acquiring endpoint and network forensics capabilities.
- The effectiveness of current endpoint security measures must be reviewed to fill the gaps exploited by the attacker.

- Network security must be enhanced to disrupt the “Command and Control” and “Actions on Objective” phases of the Cyber Kill Chain.
- Application security for email must be heightened.

Recommendation #3: Staff awareness on cybersecurity must be improved, to enhance capacity to prevent, detect, and respond to security incidents

- The level of cyber hygiene among users must continue to be improved.
- A Security Awareness Programme should be implemented to reduce organisational risk.
- IT staff must be equipped with sufficient knowledge to recognise the signs of a security incident in a real-world context.

Recommendation #4: Enhanced security checks must be performed, especially on CII systems

- Vulnerability assessments must be conducted regularly.
- Safety reviews, evaluation, and certification of vendor products must be carried out where feasible.
- Penetration testing must be conducted regularly.
- Red teaming should be carried out periodically.
- Threat hunting must be considered.

Recommendation #5: Privileged administrator accounts must be subject to tighter control and greater monitoring

- An inventory of administrative accounts should be created to facilitate rationalisation of such accounts.
- All administrators must use two-factor authentication when performing administrative tasks.
- Use of passphrases instead of passwords should be considered to reduce the risk of accounts being compromised.
- Password policies must be implemented and enforced across both domain and local accounts.
- Server local administrator accounts must be centrally managed across the IT network.
- Service accounts with high privileges must be managed and controlled.

Recommendation #6: Incident response processes must be improved for more effective response to cyber attacks

- To ensure that response plans are effective, they must be tested with regular frequency.

- Pre-defined modes of communication must be used during incident response.
- The correct balance must be struck between containment, remediation, and eradication, and the need to monitor an attacker and preserve critical evidence.
- Information and data necessary to investigate an incident must be readily available.
- An Advanced Security Operation Centre or Cyber Defence Centre should be established to improve the ability to detect and respond to intrusions.

Recommendation #7: Partnerships between industry and government to achieve a higher level of collective security

- Threat intelligence sharing should be enhanced.
- Partnerships with Internet Service Providers should be strengthened.
- Defence beyond borders - cross-border and cross-sector partnerships should be strengthened.
- Using a network to defend a network applying behavioural analytics for collective defence.

(II) Additional recommendations

Recommendation #8: IT security risk assessments and audit processes must be treated seriously and carried out regularly

- IT security risk assessments and audits are important for ascertaining gaps in an organisation's policies, processes and procedures
- IT security risk assessments must be conducted on CII and mission-critical systems annually and upon specified events.
- Audit action items must be remediated.

Recommendation #9: Enhanced safeguards must be put in place to protect electronic medical records

- A clear policy on measures to secure the confidentiality, integrity, and accountability of electronic medical records must be formulated.
- Databases containing patient data must be monitored in real-time for suspicious activity.
- End-user access to the electronic health records should be made more secure.
- Measures should be considered to secure data-at-rest.
- Controls must be put in place to better protect against the risk of data exfiltration.
- Access to sensitive data must be restricted at both the front-end and at the database-level

Recommendation #10: Domain controllers must be better secured against attack

- The operating system for domain controllers must be more regularly updated to harden these servers against the risk of cyber attack.
- The attack surface for domain controllers should be reduced by limiting login access.
- Administrative access to domain controllers must require two-factor authentication.

Recommendation #11: A robust patch management process must be implemented to address security vulnerabilities

- A clear policy on patch management must be formulated and implemented.
- The patch management process must provide for oversight with the reporting of appropriate metrics.

Recommendation #12: A software upgrade policy with focus on security must be implemented to increase cyber resilience

- A detailed policy on software upgrading must be formulated and implemented.
- An appropriate governance structure must be put in place to ensure that the software upgrade policy is adhered to.

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.