Prevention Is No Cure:

A Case Study of the 2018 SingHealth Breach

Shaun Kai Ern Ee

Key Takeaways

- In July 2018, Singapore experienced its worst breach of personal data ever: a state-linked actor infiltrated its largest healthcare provider, SingHealth, and stole data on 1.5 million patients, including the Prime Minister.
- SingHealth's case suggests that intrusions are inevitable – but that isn't cause for despair. Instead, it is a lesson. Organisations should strive for resilience, not impregnability; focus not just on prevention, but also on the cure.
- Central to this analysis is Singapore's 454-page Committee of Inquiry (COI) report, which provides an in-depth analysis of the attacker's access route.
- But the COI maps imperfectly onto more pro-market countries and smaller, rural organisations, so this paper complements Singapore's official analysis with other expert interviews to identify four major points of intervention.
- First, senior managers in the healthcare sector must adopt tools – organisational and technical alike – that give them better oversight. Beyond just complying with legal requirements, they must understand cybersecurity as a risk to their patients.
- Second, large institutions should staff up security teams that can proactively hunt intruders down, while resource-strapped, smaller institutions should partner with or outsource to other organisations for their security personnel needs.
- Third, healthcare organisations must eschew "castle moat" perimeter defence for "defence-in-depth": they need endpoint detection and response tools, and curbs on intruder movement within their network, like privileged account management.
- Fourth, organisations must prioritise the security of patients' electronic healthcare records (EHRs), not just by rigorously vetting third-party software solutions, but perhaps even by limiting EHR digitisation, such as keeping VIP records on paper.

1 Introduction

In July 2018, Singapore experienced the "worst breach of personal data in [its] history."[1] An unknown actor breached the systems of SingHealth, Singapore's largest healthcare provider, and exfiltrated information on 1.5 million patients – including the country's Prime Minister, whose medical records were specifically targeted. The fact that this could happen in Singapore, with its high level of cyber maturity, should alarm senior healthcare executives in other countries. Singapore's conclusion that the actor was a fellow nation-state should concern their politicians and policymakers too.

Like prominent breaches elsewhere, SingHealth's example raises a question: if breaches are going to happen anyway, why bother trying to stop them? Singapore's particularly detailed 454-page Committee of Inquiry (COI) report, however, provides compelling reasons to do so.[2] This post-incident report – perhaps the biggest reason peer institutions and policymakers should pay attention – presents a valuable public case study that allows others to pre-emptively isolate and disrupt elements of their own opponents' attack plans. Interviews with other US and German experts corroborate the COI report's main thrust, while suggesting further ways to map its recommendations onto the overall ecosystem.[3]

The report is compelling because of its central message: intrusions are inevitable, which means organisations should not strive for impregnability, but should instead prioritise the protection of core assets and functions – such as Electronic Health Records (EHRs).[4] Because large organisations' perimeters are inherently indefensible, rather than simply trying to freeze attackers out, institutions must be prepared to be breached, and should establish staggered internal barriers and response mechanisms. Even after penetrating SingHealth's network, the attackers took a full year to access the EHRs. They could have been interrupted at several key stages, but were not.

1 According to Singapore's Personal Data Protection Commission. Tan, Kiat How, and Zee Kin Yeong. 2019. "Breach of the Protection Obligation by SingHealth and IHiS." Singapore: Personal Data Protection Commission. (https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Commissions-Decisions/Grounds-of-Decision---SingHealth-IHiS---150119.pdf).

2 Magnus, Richard, et al. 2019. "Public Report of the Committee of Inquiry into the Cyber Attack on Singapore Health Services Private Limited's Patient Database on or around 27 June 2018." Singapore: Committee of Inquiry into the Cyber Attack on SingHealth. (https://www.mci.gov.sg/-/media/mcicorp/doc/report-of-the-coi-into-the-cyber-attack-on-singhealth-10-jan-2019.ashx).

3 Many thanks to the MITRE Corporation for providing background and context on healthcare cybersecurity in the US, as well as all others who were interviewed for or reviewed this study, including Anca Agachi, Hamsini Hariharan, Sven Herpig, Trey Herr, Ekaterina Kologrivaya, Todd Rosenblum, Safa Shahwan, Alexander Szanto, Paulina Uznańska, and other participants who spoke on background.

4 The report includes many commonly made (but important) recommendations, such as being wary of phishing campaigns, not using "P@ssw0rd" as a password for administrator accounts, and so on, but these will not be reiterated here.

2 Background

Healthcare cybersecurity is defined by three realities: vulnerability to life-threatening operational disruption, sensitive high-value patient data, and seriously inadequate budgets.[5] Though ransomware attacks depict the most common malicious cyber incidents, breaches are not infrequent, costing an average USD 6.45 million and taking nearly a year to discover.[6] Against this backdrop, the SingHealth breach, though severe, looks dismayingly typical.

2.1. Anatomy of a Breach

SingHealth is not a single institution: it is the largest of three "clusters" in Singapore's public healthcare sector, covering 20 institutions, from public hospitals to specialty clinics.[7] Integrated Health Information Systems (IHiS), the public healthcare system's central IT agency, deploys IT personnel to clusters to support them, but clusters administer their own IT budgets. To manage EHRs, SingHealth uses the Sunrise Clinical Manager (SCM) system from US-based Allscripts Healthcare Solutions; this SCM database contained over 5 million patients' data at the time of the attack.[8]

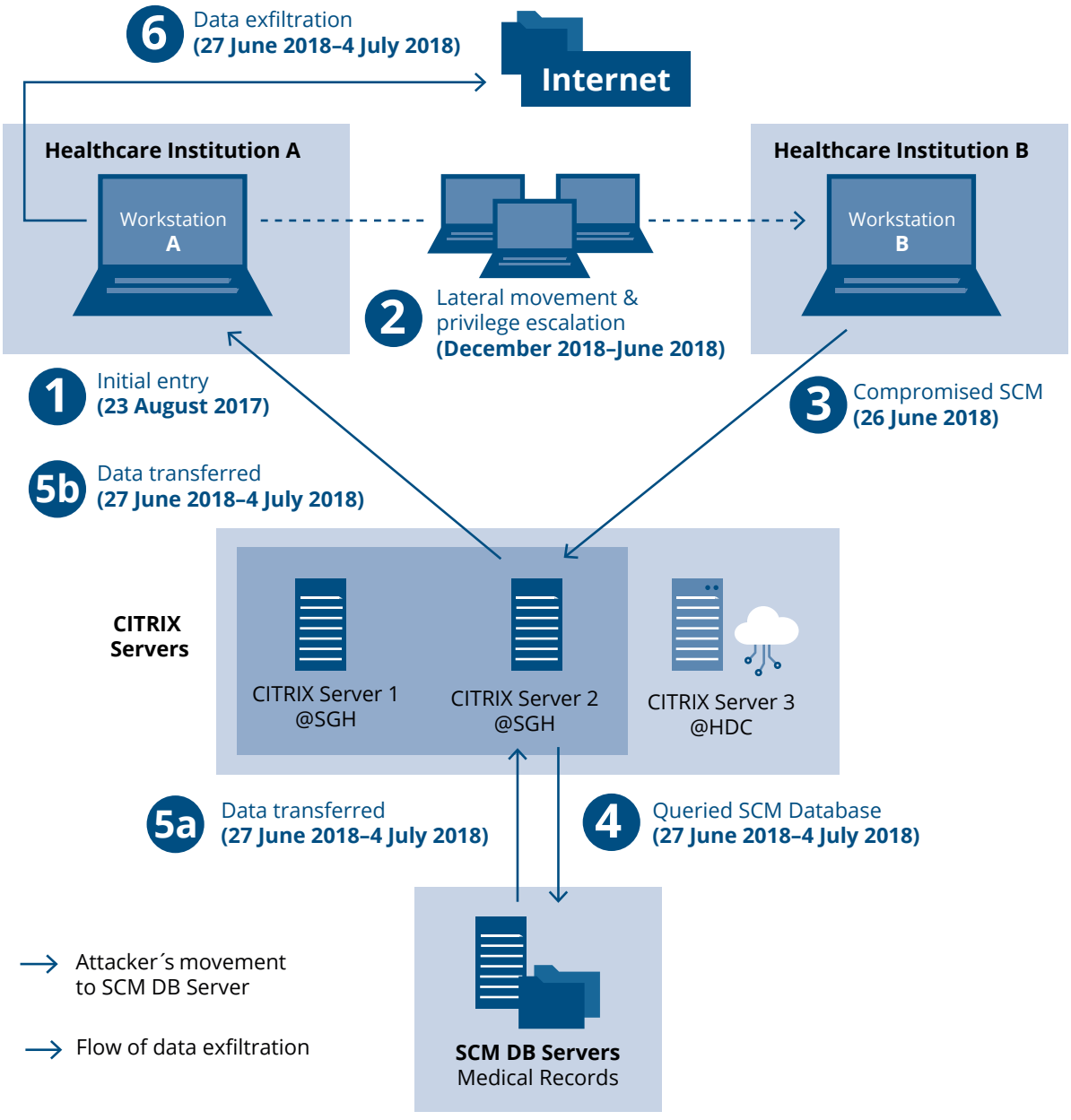
5 Morse, Susan. 2019. "Healthcare's Number One Financial Issue Is Cyber Security." Healthcare Finance News, 30 July. (https://www.healthcarefinancenews.com/news/healthcares-number-one-financial-issue-cybersecurity). According to one expert, only 4 to 7% of healthcare IT budgets go toward cybersecurity, compared to 15% in finance; this corroborates with a 2019 survey where the median healthcare IT budget allocation toward cybersecurity was 3 to 6%, though this survey noted that this allocation is generally increasing. See: Healthcare Information and Management Systems Society. 2019. "2019 HIMSS Healthcare Cybersecurity Survey." (https://www.himss.org/himss-cybersecurity-survey).

6 Alder, Steve. 2020. "Small-Sized and Medium-Sized Healthcare Providers Most Likely to Be Attacked with Ransomware." HIPAA Journal (blog). (https://www.hipaajournal.com/small-and-medium-sized-healthcare-providers-most-likely-to-be-attacked-with-ransomware/); IBM. 2020. "Cost of a Data Breach Report 2019." (https://www.ibm.com/security/data-breach). According to RiskIQ, ransomware attacks increased by 35% from 2016 to 2019. Such attacks make healthcare data and devices unusable through encryption. Meanwhile, the 2017 survey by Marsh & McLennan Companies indicated that malicious actors had targeted 27% of healthcare organisations surveyed in the past 12 months. See: Marsh & McLennan Companies. 2018. "Holding Healthcare to Ransom: Industry Perspectives on Cyber Risks." (https://www.marsh.com/sg/insights/research/holding-healthcare-to-ransom.html). The 2019 IBM report regarding data breaches should be viewed with the caveat that the healthcare companies it studied were located in the US, which had the highest per record cost. Nonetheless, this high figure should not be dismissed: according to the survey, data breaches in the healthcare industry have consistently ranked as the most expensive of any industry for the past nine years. The report also indicates that healthcare organisations took 329 days on average to identify and contain data breaches, the highest of any industry surveyed. In this context, the 2018 SingHealth breach – taking about a year from the first detected attack in August 2017 to detection and containment in July 2018 – looks surprisingly typical.

7 Magnus, Richard, et al. 2019. "COI Report." 13; Poon, Chian Hui. 2017. "Public Healthcare Sector to Be Reorganised into 3 Integrated Clusters, New Polyclinic Group to Be Formed." The Straits Times, 18 January. (https://www.straitstimes.com/singapore/health/public-healthcare-sector-to-be-reorganised-into-3-integrated-clusters-new).

8 Magnus, Richard, et al. "COI Report." 18. This figure (5.01 million) was correct as of July 2018, the time of the attack. It is worth noting that not all of Singapore's clusters use Allscripts' SCM solution, and some use products from Epic instead.

Figure 1. Timeline and attack route of the SingHealth breach.
(Source: Magnus et al., "COI Report," 53.)



In post-incident analysis, Singapore's Cyber Security Agency (CSA) divided the year-long attack into three broad phases.[9] Firstly, from August to December 2017, the attacker established a presence in SingHealth's network by compromising "Workstation A" using both customised and publicly available malware, likely delivered through a phishing attack. Secondly, from December 2017 to June 2018, the attacker engaged in lateral movement and privilege escalation, compromising other devices and administrator accounts in a series of unsuccessful attempts to access the SCM database. SingHealth and IHiS staff noted some of these, but treated them in isolation with limited action, missing several opportunities to report and repel the attack.

In the final phase, the attacker successfully cracked the SCM database on 26 June 2018, and had unfettered access to SingHealth's EHRs till 4 July 2018, when an IHiS database administrator noticed unusual queries and shut them out.[10] To access and exfiltrate data, the attacker hijacked unsecured administrator accounts, hopped through SCM-database-adjacent servers for which vulnerability assessments had not been conducted, and finally, tapped a software vulnerability in Allscripts' SCM system to gain access to SingHealth's EHRs. The attacker specifically targeted information about Singapore's Prime Minister, but also made off with almost 1.5 million patients' personal particulars, as well as 159,000 patients' outpatient dispensed medication records.[11]

Dire as this incident was, several factors prevented it from being worse. Firstly, after noticing the queries in July 2018, IHiS staff rapidly escalated the incident to CSA, which quickly established the extent of the breach and curbed the attacker's access. Secondly, Singapore's government was prompt and transparent in notifying affected individuals, going public about the breach days later on 20 July 2018, whereas detection and disclosure by other companies can take weeks and months if it happens at all.[12]

To Singapore's government, the breach was inconvenient, coming just as it planned to mandate use of a National EHR (NEHR).[13] Officials reacted sternly, stepping up cybersecurity measures, reviewing NEHR security, and appointing a Committee of Inquiry (COI) to look into the breach. After investigations, Singapore's Personal Data Protection Commission (PDPC) fined SingHealth SGD 250,000 and IHiS SGD 750,000, while IHiS fined seven members of senior and middle management, including the CEO, demoted one employee, and fired two.[14] Though these

9 Magnus, Richard, et al. 2019. "COI Report." 53.
10 Magnus, Richard, et al. 2019. "COI Report." 154–55.
11 Magnus, Richard, et al. 2019. "COI Report."; Watts, Jake Maxwell, and P. R. Venkat. 2019. "State-Backed Hackers Sought and Stole Singapore Leader's Medical Data." Wall Street Journal, 10 January. (https://www.wsj.com/articles/state-backed-hackers-sought-and-stole-singapore-leaders-medical-data-11547109852). The stolen personal particulars were non-medical information such as names, addresses, dates of birth, national identification number, etc. Prime Minister Lee Hsien Loong had just been diagnosed in 2015 with prostate cancer, although he said on Facebook that the attackers would not have found any "dark state secret" in his records.
12 Lee, Justina. 2018. "Suspected China Cyberhack on Singapore Is a Wake-up Call for Asia." Nikkei Asian Review, 21 August. (https://asia.nikkei.com/Spotlight/Asia-Insight/Suspected-China-cyberhack-on-Singapore-is-a-wake-up-call-for-Asia).
13 Choo, Cynthia. 2018. "National E-Records System to Undergo 'Rigorous' Security Review before Proceeding with Mandatory Contribution." TODAYonline, 6 August. (https://www.todayonline.com/singapore/national-electronic-health-record-system-undergo-rigourous-security-review-proceeding).
14 Choo, Cynthia. 2019. "2 IHiS Staff Sacked, CEO among Those Fined for Role in SingHealth Cyber Attack." TODAYonline, 14 January. (https://www.todayonline.com/singapore/2-ihis-staff-sacked-ceo-among-those-fined-role-singhealth-cyber-attack); Mohan, Matthew. 2019. "PDPC Fines IHiS, SingHealth Combined S$1 Million for Data Breach Following Cyberattack." CNA, 15 January. (https://www.channelnewsasia.com/news/singapore/ihis-singhealth-fined-1-million-data-breach-cyberattack-11124156).

quick actions may have mollified some, the event damaged SingHealth's reputation, with commentators expressing anger over emerging reports of mismanagement.[15]

2.2. The 2018 SingHealth Breach as a Case Study

Published in January 2019 through Singapore's Ministry of Communications and Information, the COI's public report details 16 recommendations that cover all aspects of the breach.[16] This study does not seek to reiterate these recommendations. Rather, it evaluates them in global context, suggesting points of intervention for other healthcare organisations in four key areas: senior management oversight, security team response, intra-network cyber defences, and EHR-specific security measures. To further contextualise the COI report, several semi-structured interviews were conducted with US and German experts.[17] These interviews indicated that though the SingHealth breach remains a valuable case study, there are important considerations of its applicability elsewhere.

Despite the salience of the SingHealth breach, there are three caveats to using it as a case study. First, the healthcare organisation: as a large and well-resourced public organisation, SingHealth is uniquely equipped to outspend its smaller, cost-conscious counterparts. Second, the country: Singapore's small size makes regulation easier, and its government is unafraid to implement aggressive cybersecurity policies. Starting 2017, for example, it barred all civil servants from Internet access on their workstations, much to their ire.[18] Consequently, the COI recommendations are skewed towards being costly and heavy-handed, making some unsuited to other environments – for example, the US, which favours a lighter regulatory touch, and whose healthcare system includes numerous smaller, rural organisations.

Third and most distinctive is the threat actor. SingHealth's attacker was almost certainly an Advanced Persistent Threat (APT), a class of "sophisticated, usually state-linked" actors that – befitting their name – are usually singularly focused on specific national goals and unlikely to relinquish their targets.[19] Conversely, most threat actors in healthcare cybersecurity are financially motivated criminal groups, which are in theory disinclined to "bite into concrete" and more easily deterred by basic countermeasures.[20] (Cybercriminals also often favour quick-and-dirty ransomware as a money-grabbing tactic, suggesting that targets should emphasise backup and recovery, but this too is changing.)[21]

15 Henson, Bertha. 2018. "SingHealth COI: How Bo Chup Can You Get?" Bertha Harian (blog), 29 September. (https://berthahenson.wordpress.com/2018/09/29/singhealth-coi-how-bo-chup-can-you-get/).

16 Seven of these are high-priority, and nine additional. Besides the report, which includes an executive summary, they can be viewed here: (https://www.straitstimes.com/singapore/16-recommendations).

17 See first page for list of interviewees.

18 BBC News. 2016. "No Internet for Singapore Public Servants." 8 June. (https://www.bbc.com/news/world-asia-36476422); Lim, Benjamin. 2018. "What Is Life at Work Without the Internet? Civil Servants Tell All." Rice Media, 29 March. (https://www.ricemedia.co/current-affairs-features-life-at-work-without-internet-civil-servants-tell/).

19 Magnus, Richard, et al. 2019. "COI Report." 94.

20 Sven Herpig, Director for International Cybersecurity Policy, Stiftung Neue Verantwortung (SNV), in discussion with the author, July 23, 2020. Alexander Szanto, Cybersecurity Research Fellow at the Brandenburg Institute for Society and Security (BIGS), in discussion with the author, 24 July 2020.

21 Herpig, interview; Cohen, Jessica Kim. 2020. "Ransomware Targeting Health Systems in More 'Sophisticated' Ways." Modern Healthcare, 24 January. (https://www.modernhealthcare.com/cybersecurity/ransomware-targeting-health-systems-more-sophisticated-ways). Although a detailed examination of cybercriminal activity targeting the healthcare sector is beyond the scope of this article, both interviewees and other articles indicated that cybercriminal groups are using increasingly sophisticated ransomware tools, and sometimes not merely demanding ransoms, but selling obtained data. This blurs the line between the tactics of nation-states and financially motivated actors.

The COI recommendations hence apply best to organisations with a similar threat model to SingHealth – again, larger healthcare institutions, which are prime targets for APTs, by virtue of their VIP clients and their sheer number of EHRs.[22] Such target-rich institutions must brace for sophisticated assaults that will not stop until attackers get what they want – in SingHealth's case, the Prime Minister's information. Their superior resources make it easier and more appropriate for them to mimic the COI's aggressive, spare-no-expense approach to cybersecurity.

The picture for smaller institutions is more nuanced. Nominally, they are likelier to face financially motivated attackers rather than APTs, and in this sense may want to simply "raise the bar" to deter opportunistic attackers first, rather than worry about full fortification against sustained, targeted attack. But their lack of resources means greater difficulty bouncing back from disruption, with serious impacts on patient care. This matters for others too: sector-wide interconnectivity means that compromising a smaller institution's networks may permit an attack on a larger institution – for example, if a rural hospital were part of a larger telemedicine system. Effectively defending smaller institutions hence requires creative, collaborative, ecosystem-wide solutions that the COI report does not focus on. Ultimately, though, every institution must take responsibility for its own cybersecurity, and the SingHealth breach nevertheless provides smaller peers with a template with which to do so.

22 FireEye. 2019. "Beyond Compliance: Cyber Threats and Healthcare." (https://www.fireeye.com/blog/threat-research/2019/08/healthcare-research-data-pii-continuously-targeted-by-multiple-threat-actors.html).

3 Weak Point #1: Managerial Oversight

The breach's first lesson is that senior management must keep their eye on serious vulnerabilities and incidents by actively engaging middle management and critically assessing risks, rather than performing "checklist cybersecurity." By relegating cybersecurity to the sidelines as a technical issue, SingHealth and IHiS management allowed previously noticed network vulnerabilities to fester, paving the way for attackers. Over the final months of the year-long breach, their lack of situational awareness prevented them from escalating the issue to the national-level CSA in a timely fashion, which delayed incident response and deprived SingHealth of vital resources. To prevent crises, senior executives should ensure follow-through on identified vulnerabilities, but as total prevention of breaches is impossible, they must also keep abreast of ongoing incidents so they can react and request national resources if necessary.

3.1. Lack of Follow-Through

Though IHiS management tasked staff and external parties to evaluate SingHealth's systems for vulnerabilities, they did not follow through to verify fixes. As such, serious vulnerabilities were left unaddressed, allowing their exploitation during the 2018 breach.[23] For vulnerability assessment and penetration testing to work, organisations must commit resources and attention to fixing the problems revealed.[24] Because IHiS management merely "checked the box" by performing assessments with-

23 Magnus, Richard, et al. 2019. "COI Report." 45–46, 76–80, 91–92, 368–71. Here, the greatest offender was the "FY16 H-Cloud Pen-Test," a penetration test following a major server migration that found several "high-risk weaknesses." IHiS learned of these vulnerabilities by March 2017, well before the attack, but its "remediation process… was mismanaged and inadequate." Multiple vulnerabilities were not rectified, and some were even marked as resolved despite being unfixed. Ministry of Health Holdings (MOHH), the holding company of SingHealth and the two other healthcare clusters, was responsible for conducting the FY16 H-Cloud Pen-Test through its Group Internal Audit (GIA) unit. This penetration test followed a server migration to the new "H-Cloud Data Centre," discussed further under Section 6.2. Noted vulnerabilities included weak administrator account passwords and the ability to access the Citrix servers remotely without authorisation.

24 Trey Herr, Director of the Cyber Statecraft Initiative, Scowcroft Centre for Strategy and Security, Atlantic Council, in discussion with the author, 7 July 2020.

out addressing the problems they revealed, these exercises did not meaningfully improve SingHealth's cybersecurity posture.

But more than just hampering SingHealth's preparedness, managerial inattention to operational matters allowed the breach to spiral out of control when IHiS could have requested CSA assistance. Here, significant blame rested with two middle managers who resisted escalating the breach to senior management even while under pressure from their subordinates to do so.[25] Yet despite censuring them, the report also underscored "deeper cultural issues within the organisation" for this lapse in the reporting pipeline.[26] SingHealth and IHiS placed undue emphasis on "confirming" security incidents before they could be reported, with one middle manager's reporting officer suggesting that declaring a security incident that turned out to be a non-event would "look bad on the person who made the declaration."[27] In other words, cybersecurity was treated as something for IT staff to address and fully resolve *before* notifying senior management.

This should not have been the case. As the report itself notes, cybersecurity is "a risk management issue, and not merely a technical issue," and can directly impact patient safety and privacy.[28] Like other countries, Singapore considers healthcare infrastructure to be Critical Information Infrastructure (CII), and requires that cybersecurity incidents be reported to national authorities.[29] Governments can even exempt directors' and officers' (D&O) insurance from coverage when certain basic cybersecurity principles are neglected, removing individual executives' protection from liability, but this is rather more contentious.[30] Senior executives hence not only have an operational, but also a legal reason to keep their finger on the pulse of their organisation's cybersecurity status.

3.2. Looking Beyond Liability

Liability is certainly one strategy to promote cybersecurity, but it is not enough. If merely threatening penalties was a sure-fire guarantee of appropriate action, Singapore's PDPC would not have needed to apply fines in the first place. Mandating basic healthcare cybersecurity requirements is necessary, as most interviewees agreed.[31] But healthcare executives face competing priorities and trade-offs that can literally be life-and-death issues. Punishing their distraction is not always sufficient to guarantee the correct cybersecurity response, as additional regulatory variables can lead executives to prioritise compliance over risk management.[32]

More targeted mechanisms may hence complement regulatory requirements by letting managers price the cost of various cybersecurity deficiencies into their decisions.[33] Cyber risk insurance is the most prominent of these: poor cybersecurity practices precipitate steeper premiums, incentivising organisations to improve.[34] Insurers Aon and Allianz, for example, teamed up with Apple and Cisco to offer discounted policies for organisations

25 Discussed further under second failure point.
26 Magnus, Richard, et al. 2019. "COI Report." 144.
27 Magnus, Richard, et al. 2019. "COI Report." 143.
28 Magnus, Richard, et al. 2019. "COI Report." 242.
29 Magnus, Richard, et al. 2019. "COI Report." 32–34.
30 Herr, interview.
31 Herpig, interview; Todd Rosenblum, former senior US defence and homeland security official from 2009–16, in discussion with the author, 14 July 2020; SingHealth doctor wishing to remain anonymous, in discussion with the author, 29 July 2020.
32 Szanto, interview; Health Care Industry Cybersecurity Task Force. 2017. "Report on Improving Cybersecurity in the Health Care Industry." US Department of Health & Human Services (https://www.phe.gov/preparedness/planning/cybertf/documents/report2017.pdf).
33 Herr, interview.
34 Rosenblum, interview; Szanto, interview.

that adopt good security practices.[35] Some US interviewees suggested a variant on this, with an entity assessing healthcare companies on their cybersecurity practices, either through annual exercises or specific criteria, and publicly grading their performance to inform those doing business with them.[36] Theoretically, this would be more flexible than strict government mandates, allowing companies to make decisions appropriate to their situation. However, some other interviewees indicated that simply mandating a technical baseline would still be the most effective approach; the preferred approach may depend partly on national context.[37]

Most of all, senior management must not just integrate cybersecurity into their decision-making, but also develop their own capacity to understand cybersecurity risk.[38] They can do so by streamlining communication between themselves and middle-management experts. The COI report proposes a "management dashboard" to capture incidents both above and below the threshold for national-level reporting.[39] In theory, this would improve management visibility, but improperly executed, it could burden staff administratively and still be ignored by senior management. Hence, dashboard or not, organisations must have subject-matter experts on staff to "translate" technology risks into patient privacy and safety concerns for senior management. The COI also recommends regular tabletop exercises to engage incident response staff and senior management in potential crisis situations.[40] Tabletop exercises incorporating employees at multiple levels of seniority would inculcate better reporting practices, making it more natural for more junior employees to escalate issues when necessary.

35 Szanto, interview; Kirk, Jeremy. 2018. "Apple, Cisco Strike Partnerships for Cyber Insurance." BankInfoSecurity, 6 February. (https://www.bankinfosecurity.com/apple-cisco-strike-partnerships-for-cyber-insurance-a-10632).

36 Herr, interview; Rosenblum, interview. These two interviewees suggested similar concepts, but did so independently: Rosenblum suggested an independent third party scoring healthcare providers with letter grades (A/B/C), using a list of attributes for scoring developed either by government entities (e.g., the National Institute of Standards and Technology in the US) or a consortium of private-sector cybersecurity companies. Herr suggested sector-based annual exercises, with companies scoring in, e.g., the lowest third having their negative performance publicised. Both approaches would rely on public information to inform parties doing business with the healthcare providers (e.g., insurance companies), allowing them to price in cybersecurity information.

37 Herpig, interview; Szanto, interview; SingHealth doctor, interview. Some interviewees, when discussing this topic, suggested that the third-party approach might be prompted partly by national differences in regulatory tactics, since the US generally favours more market-based approaches in contrast to the EU or Singapore. Given the small sample size of interviewees, it is not possible to make a comprehensive generalisation, but it is worth considering this potential difference.

38 Anca Agachi, Assistant Director of the Foresight, Strategy, and Risks Initiative, Scowcroft Centre for Strategy and Security, Atlantic Council, in discussion with the author, 11 May 2020. Thanks to Anca Agachi for emphasising the distinction between these two.

39 Magnus, Richard, et al. 2019. "COI Report." 244–45.

40 Magnus, Richard, et al. 2019. "COI Report." 236, 313–18.

4 Weak Point #2: Security Team Response

The COI report's second lesson is the manpower element: security personnel must focus proactively on detection and response, and even general IT staff must play an active role in detecting cybersecurity incidents. But these recommendations must be considered in light of the larger cybersecurity ecosystem. Healthcare cybersecurity, even more than general cybersecurity, is marked by a shortage of trained personnel. Hence, the "ideal world" of the report, where SingHealth and its peers can all hire an army of defenders, stands in contrast to the difficult reality that the world as a whole is far short of the defenders it needs. Supporting smaller institutions requires going beyond the COI report to examine other collaborative approaches.

4.1. COI Suggestions for Staffing Improvements

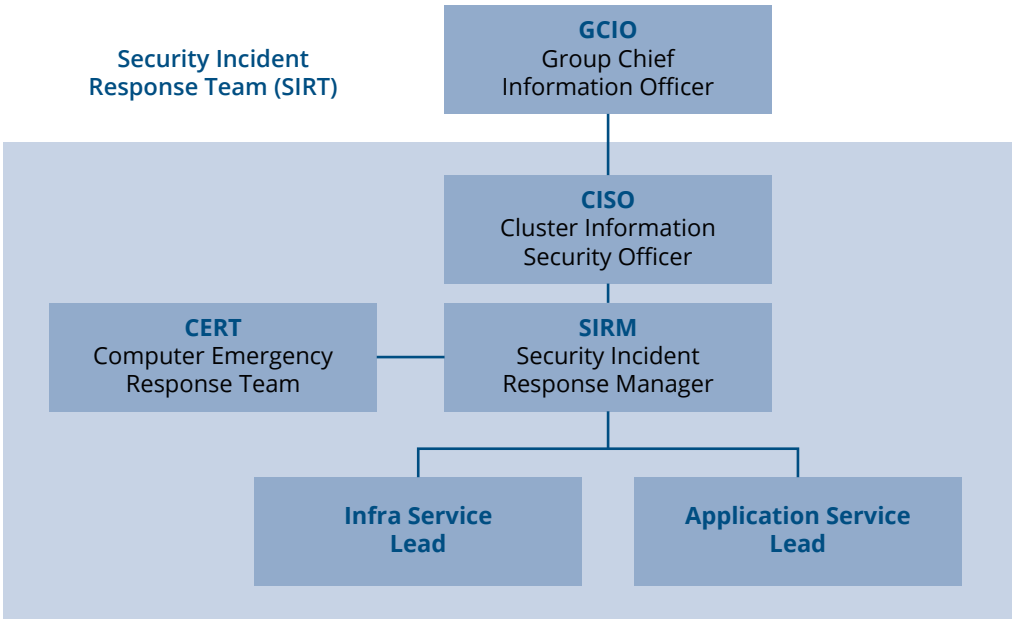
In some measure, the COI's recommendations are a response to one individual's failure – the Security Incident Response Team (SIRT) leader – but the impact of his negligence on SingHealth's response also suggests structural problems with the training and organisation of technical experts. Still, his role should not be understated; he failed to activate the SIRT despite seeing suspicious activity over several months, leaving the smaller and untrained Computer Emergency Response Team (CERT) to fend for itself.[41] The COI excoriated him for having "smothered" his subordinates' initiative with "a blanket of middle management mistakes," and after the breach, he was fired.[42] The COI recommends

41 Magnus, Richard, et al. 2019. "COI Report." 136, 417; Tan and Yeong, Breach of the Protection Obligation, 46. The SIRT leader was seriously wanting in his response, ignoring a series of callbacks to foreign IP addresses in January 2018, several months before data exfiltration, and then telling subordinates to delay incident reporting in June 2018 due to concerns about the potential workload generated. His superior, the cluster information security officer (cluster ISO), was also at fault, as he took an apathetic, laissez faire approach to his subordinates' reports, and "passively waited for updates" even during time-sensitive parts of the investigation. Nonetheless, IHiS apparently found the SIRT leader to be the worse offender; the cluster ISO was merely demoted by IHiS, while the SIRT leader was fired. It appears that the COI report largely agreed with this general assessment, as the SIRT leader's performance – in particular, his claim that his team would have "no day, no night" if he reported the incident – was one of the largest subjects of COI criticism in the breach's aftermath.

42 Choo, Cynthia. 2019. "2 IHiS Staff Sacked, CEO among Those Fined for Role in SingHealth Cyber Attack."; Magnus, Richard, et al. 2019. "COI Report." 164.

appointing a competent SIRT leader, but also goes beyond to suggest three staffing changes that would empower employees other than the SIRT leader.

Figure 2. SIRT reporting structure.
(Source: Magnus et al., "COI Report," 416.)



Firstly, per these recommendations, IHiS should train all IT staff, even non-security staff, to identify suspicious activity.[43] Though non-security IT staff noticed signs of intrusion, they interpreted these as operational issues. One database administrator noticed failed logins to the SCM database a month before EHRs were exfiltrated, but assumed that her colleagues were "testing the system." In actuality, signs like these – unusual database activity, account abuse, and suspicious network behaviour – should have tipped staff off.[44]

Secondly, SingHealth should strengthen its dedicated incident response team with additional drills and encourage adherence to an incident response plan. This plan should emphasise usage of predefined communication channels (possibly linked to the "management dashboard") and appropriately balance evidence gathering and threat containment.[45] Even despite not having strong leadership, SingHealth's three-person CERT displayed admirable initiative during the crisis, but only one member had received formal incident response training, and the existing incident response plan did not address

43 Magnus, Richard, et al. 2019. "COI Report." 269–78. Recommendation #3, "Staff awareness on cyber-security must be improved to enhance capacity to prevent, detect, and respond to security incidents," deals with this topic at length.
44 Magnus, Richard, et al. 2019. "COI Report." 276–78.
45 Magnus, Richard, et al. 2019. "COI Report.", 313–30, 408–20. Recommendation #6, "Incident response processes must be improved for more effective response to cyber attacks," and Recommendation #15, "Competence of computer security incident response personnel must be significantly improved," deal with these topics at length.

APTs.[46] They hence committed several missteps, such as reformatting rather than quarantining infected workstations, which erased potential evidence.[47]

Thirdly, IHiS should establish its own in-house Security Operations Centre (SOC), emphasising proactive defence. At the time of the breach, IHiS outsourced its detection capabilities, relying on a managed security service provider to provide alerts, which IHiS staff had to investigate before responding, creating delays and confusion.[48] The COI report hence recommends that IHiS bring all these capabilities in-house, equipping the Security Operations Centre to analyse large and heterogeneous data inputs so that it can conduct round-the-clock monitoring and full-lifecycle management of incidents.[49] It emphasises that this would be an "advanced" SOC, with analysts proactively searching for malicious actors within the network ("threat hunting") rather than waiting for them to be detected, but recognises that this level of maturity may take time to achieve.[50]

4.2. An Ecosystem-Level Approach

However, SingHealth's manpower issues also underscore a larger healthcare-sector-wide deficiency in trained cybersecurity professionals. If SingHealth, a public institution in a wealthy, tech-savvy country, struggled to find qualified cybersecurity personnel, what does that mean for the sector at large? Many small organisations live below the "cyber poverty line," with one study citing 85% of small- and medium-sized hospitals as having no qualified cybersecurity staff on hand.[51] How can one discuss intensive incident response team training, let alone an SOC, when these institutions do not even have dedicated cybersecurity personnel? Juxtaposed to the harsh reality of budget limitations and the existing global, cross-industry cybersecurity skills gap, the COI's elaborate recommendations seem far from universally applicable. A hiring frenzy might help secure the largest networks, but the shortage of qualified personnel would still leave some institutions out in the cold.

46 Magnus, Richard, et al. 2019. "COI Report." 40.
47 Magnus, Richard, et al. 2019. "COI Report." 135–36, 142, 162–64, 321–22.
48 Magnus, Richard, et al. 2019. "COI Report." 325–26; Hamilton, Michael K. n. d. "MDR vs. MSSP vs. SIEM – InfoSec Acronyms Explained." CI Security (blog). (https://ci.security/resources/news/article/mdr-vs-mssp-vs-siem-infosec-acronyms-explained); "Why Choose MDR over MSSP or SIEM?" n. d. Arctic Wolf (blog). (https://arcticwolf.com/resources/briefs-2/why-choose-mdr-over-mssp-or-siem). The COI report skips several intermediate levels of organisational maturity; several contemporary sources suggest that outsourced Managed Detection and Response (MDR) or SOC-as-a-service solutions can serve as an intermediate step between MSSPs and in-house SOCs, providing improved integration of detection and response without incurring the full cost of in-house SOCs.
49 Magnus, Richard, et al. 2019. "COI Report."
50 Magnus, Richard, et al. 2019. "COI Report." 296–97, 329–30; "Three Elements That Every Advanced Security Operations Center Needs." n. d. CSO (blog). (https://www2.cso.com.au/article/563871/three-elements-every-advanced-security-operations-center-needs/); "What Is Cyber Threat Hunting?" Crowdstrike (blog), 21 June 2019. (https://www.crowdstrike.com/epp-101/threat-hunting/). The COI report refers repeatedly to this proposal as creating an Advanced Security Operations Centre (ASOC), but there does not appear to be a canonical definition of such. It appears that this emphasis is primarily in light of a shift to proactive threat hunting, although again, it seems this might require substantially more organisational maturity than SingHealth/IHiS displayed based on their performance in the breach. A publication by the US Department of Health & Human Services does contrast between an SOC for medium-sized healthcare institutions, and an ASOC for large healthcare institutions, with the primary point of difference being the move to a 24x7x365 model. Unlike the COI report, this publication does indicate that fully outsourcing an ASOC is one possibility. See: US Cybersecurity Act of 2015, Section 405(d) Task Group. 2018. "Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients, Technical Volume 2: Cybersecurity Practices for Medium and Large Health Care Organizations." US Department of Health & Human Services (https://www.phe.gov/Preparedness/planning/405d/Documents/tech-vol2-508.pdf).
51 Sullivan, Tom. 2017. "75% of Health Orgs Live below Cybersecurity Poverty Line." Healthcare IT News, 11 May. (https://www.healthcareitnews.com/news/75-health-orgs-live-below-cybersecurity-poverty-line).

Hence, healthcare IT personnel shortages require an ecosystem-level approach, in which all institutions, but especially smaller ones, lean on other parties for support. Most prominently, they can outsource IT needs to third-party cloud providers and cybersecurity firms, which provide security at a lower cost than in-house solutions and, from a policy perspective, are more consolidated and hence easier to regulate.[52] They can also work with peers: membership in Information Sharing and Analysis Centres (ISACs) such as the international Health ISAC (H-ISAC) grants access to both public- and private-sector information on threats.[53] Some regional players are even moving beyond mere information sharing to implement truly collaborative defence: the Michigan Healthcare SOC covers multiple districts across the US state of Michigan, allowing smaller institutions to enjoy the benefits of an SOC without operating one themselves.[54]

Large institutions may be better funded, but will still struggle when faced with even mid-sized APTs, with one interviewee terming it "improbable" that they could mount a successful defence.[55] They will find government support essential during APT-level breaches, and should prioritise detection and prompt reporting, aiming to delay attackers and maximise the chance of detection so they can summon national-level support in time.

52 Herr, interview.
53 "About Health Information Sharing and Analysis Center." n. d. Health Information Sharing and Analysis Center. (https://h-isac.org/about-h-isac/).
54 Herr, interview; Cyberforce|Q (https://www.cyberforceq.com/mi-hsoc); Michigan Healthcare Security Operations Center (https://events.esd.org/wp-content/uploads/2019/10/Lessons-Learned-from-Operating-a-Collective-Cybersecurity-Operations-Center.pdf).
55 Herpig, interview.

5 Weak Point #3: Network Defenses

The third lesson: from a technical standpoint, healthcare organisations must layer "defence-in-depth" throughout their network, rather than take a "castle moat" approach that relies primarily on perimeter defences.[56] SingHealth focused too narrowly on guarding a defined network perimeter, and so left itself defenceless once this was bypassed. Healthcare organisations should operate under the expectation that their outermost defences will be breached, so they should (1) implement measures that limit an attacker's movement through their network, such as privileged access management (PAM) and network segmentation, and (2) complement preventative measures in their cyber stack with detection and response capabilities that permit remote analysis and control of endpoints, and real-time monitoring of their EHR databases.

"Defence-in-depth" is not a new cybersecurity concept, having existed since the 2000s.[57] By layering multiple cybersecurity defences on top of each other, attackers will struggle to overcome them in combination, even if these defences are individually conquerable. This strategy is particularly effective for protecting critical assets – like EHRs – which should be placed behind multiple defensive layers.[58] Though logical in principle, the success of a defence-in-depth strategy rests heavily on its execution. Selecting a grab bag of incompatible solutions can produce unintentional holes in an organisation's defence or overwhelm analysts with mismatched streams of information.[59]

56 Magnus, Richard, et al. 2019. "COI Report." 249–68. Recommendation #2, "The cyber stack must be reviewed to assess if it is adequate to defend and respond to advanced threats," deals with this topic at length.

57 May, Christopher, Joshua Hammerstein, Jeffrey Mattson, and Kristopher Rush. 2006. "Defence in Depth: Foundations for Secure and Resilient IT Enterprises." Pittsburgh: Carnegie Mellon University. (https://resources.sei.cmu.edu/asset_files/Handbook/2006_002_001_14633.pdf).

58 Magnus, Richard et al. 2019. "COI Report." 237.

59 Cullivan, Julie. 2018. "Why Defense in Depth Is Failing Us." SC Media, 4 September. (https://www.scmagazine.com/home/security-news/why-defense-in-depth-is-failing-us/).

5.1. Gaps in Preventative Measures

Though SingHealth's systems were not undefended, it was exactly this lack of overlap that resulted in their compromise. Across the trinity of prevention, detection, and response, its defences displayed two prominent weaknesses.

Firstly, in prevention, SingHealth's weak internal safeguards allowed the attacker free rein within the network once they had established a foothold. SingHealth's cyber stack was in fact strongest in its prevention-focused capabilities, with signature-based anti-malware systems, network firewalls, and intrusion detection and prevention systems that could be used to inspect and block traffic in real-time.[60] But because these solutions relied on known signatures to identify malicious files, the attacker's bespoke malware – some of which was fileless, anyway – was able to bypass this perimeter.[61] Once established, the attacker enjoyed remarkable freedom of movement, especially because the administrator accounts they commandeered in May 2018 allowed them to masquerade for 1.5 months as legitimate users with broad access.

This suggests a larger need for healthcare organisations to limit network access even for apparently legitimate users. Protecting EHRs is paramount, and no matter the quality of their perimeter defences, large organisations cannot fully guarantee that they are impregnable. Certainly, the use of fileless malware partly indicates that organisations should upgrade defences from signature-based solutions to anomaly-based solutions, which identify suspicious deviations from the norm rather than look for rigid identifiers.[62] And as discussed in failure point #4, organisations should conduct regular vulnerability scanning and patching. But software solutions will inevitably have more vulnerabilities than can be addressed, and no defence is impregnable. Organisations should implement network segmentation, a tried-and-tested method of slowing attackers' progress by limiting their lateral movement across internal networks.[63]

But most critically, the COI report identifies Privileged Access Management, a method of restricting privileged users' access to critical systems, as essential to defending EHRs, with unused administrator accounts disabled in regular inventories, and accounts in use secured with strong passwords and two-factor authentication (2FA).[64] Strict adherence to this is non-negotiable: PAM and 2FA were theoretically in place for SingHealth, but administrators bypassed it for "operational convenience," defeating its purpose.[65] Organisations can consider going a step further than 2FA and implementing just-in-time credentials. By restricting privileged access to a certain timeframe, just-in-time credentials reduce the need for standing access and hence the exposure time in the event of a breach.[66]

60 Magnus, Richard, et al. 2019. "COI Report." 256–57, 261.
61 Magnus, Richard, et al. 2019. "COI Report." 256–57.
62 Magnus, Richard, et al. 2019. "COI Report." 258.
63 Magnus, Richard, et al. 2019. "COI Report." 264–66.
64 Magnus, Richard, et al. 2019. "COI Report." 76, 298–312. Recommendation #5, "Privileged administrator accounts must be subject to tighter control and greater monitoring," deals with this topic at length.
65 Magnus, Richard, et al. 2019. "COI Report." 76–77.
66 Herr, interview; Kelley, Michael, and Felix Gaehtgens. 2019. "Best Practices for Privileged Access Management Through the Four Pillars of PAM." Gartner. (https://www.gartner.com/en/documents/3899567/best-practices-for-privileged-access-management-through-).

5.2. Lack of Response Capabilities

Secondly, in detection and response, SingHealth lacked visibility over its endpoints, networks, and the SCM database, obscuring the ongoing attack. Slowing attackers down is futile if defenders do nothing with the time they buy. Although IHiS had limited oversight over internal network traffic, it lacked analytical tools to make sense of the large network traffic volume.[67] Crucially, it lacked enterprise-wide endpoint forensics tools, with the COI report noting that a key witness's "silence" on IHiS's response capabilities was "telling."[68] This debilitated its response. One CERT member turned to an online service to inspect malware in January 2018, and through June to July 2018, had to lead investigations using open-source forensics software on his own personal laptop.[69] The result was a process that took days and weeks if it progressed at all, despite time being of the essence. Moreover, SingHealth lacked tools to monitor the SCM database, so administrators did not immediately notice that bulk queries were being conducted.[70]

To address these issues, the COI primarily recommends adoption of an Endpoint Detection and Response solution, and secondarily a Database Activity Monitoring solution. An Endpoint Detection and Response solution would have permitted IHiS to isolate, contain, and analyse the various afflicted workstations within hours instead of days.[71] The COI report stresses that this should be a centralised endpoint security management system that permits not just endpoint analysis, but also remote containment and remediation, as the need to physically travel to affected workstations further slowed IHiS's response during the attack.[72] In addition to Endpoint Detection and Response, the COI report suggests adopting a Database Activity Monitoring solution allowing for real-time monitoring of the SCM database. Though such solutions are established in other sectors like finance, they are not in healthcare, and if implemented could provide real-time monitoring and retrospective auditing, and even block suspicious activity.[73] Given the importance of securing EHRs, large healthcare organisations should strongly consider implementing Database Activity Monitoring, though they should ensure that doing so does not compromise the timely retrieval of patient information nor impact patient safety.

67 Magnus, Richard, et al. 2019. "COI Report." 252, 254–55. According to the COI report, SingHealth had "continuous, real time monitoring" through a security information and event management (SIEM) system and Cisco NetFlow data, which allowed it to capture network traffic information.
68 Magnus, Richard, et al. 2019. "COI Report." 252.
69 Magnus, Richard, et al. 2019. "COI Report." 112–15, 138–39, 142, 165–68, 252–53. Note especially Paragraph 418, p. 138: "Although the CERT had been set-up in March 2018, they had not yet been provided with workstations that were suitable for forensic investigations. The forensic tools were in fact installed on [the CERT member's] personal laptop, and forensic investigations could only be done on this one computer." Despite, or possibly in light of, his relative inexperience, the COI report specifically commended his resourcefulness and sense of initiative.
70 Magnus, Richard, et al. 2019. "COI Report." 74–75.
71 Magnus, Richard, et al. 2019. "COI Report." 253–54.
72 Magnus, Richard, et al. 2019. "COI Report." 255–60.
73 Magnus, Richard, et al. 2019. "COI Report." 74–75, 359–61.

6 Weak Point #4: EHR Security

Lastly, as third-party cloud providers become essential to healthcare data management, governments and healthcare organisations must work with them closely to protect patient records. Third-party cloud and EHR providers promise improved efficiency, scalability, and in some cases, even security. But without rigorous assessment by regulators and users, these outcomes are not guaranteed. Complacency and uncritical trust can lead users to miss vulnerabilities that, ultimately, only hurt their patients the most.

6.1. Flaws in Third-Party Solutions

The attacker's "last leap" to access patient data rested not purely on SingHealth's own network configuration, but on a software vulnerability in Allscripts' SCM solution.[74] In an apparent coincidence and missed opportunity, a disgruntled IHiS employee had discovered this vulnerability years earlier in 2014, only for it to go uncorrected. Rather than log his discovery with Allscripts, the employee emailed Allscripts' rival, Epic, suggesting that they could use it to "gain more market share."[75] On learning of this, IHiS terminated the employee, but assuming that this was primarily a disciplinary issue and Allscripts would rectify any existing flaws, did not investigate further.[76]

74 Details of this vulnerability are, however, not provided in the publicly released COI report. The COI report version released for the public has been redacted of sensitive information, such as technical details of vulnerabilities; a separate Top Secret version was submitted to the government.

75 Magnus, Richard, et al. 2019. "COI Report." 86–89.; Tham, Irene, and Min Zhang Lim. 2018. "IT Vendor Employee Found Alleged Flaw in System in 2014." The Straits Times, 29 September. (https://www.straitstimes.com/singapore/it-vendor-employee-found-alleged-flaw-in-system-in-2014).

76 Magnus, Richard, et al. 2019. "COI Report." 88–89; Tan and Yeong, Breach of the Protection Obligation, 45. The COI report identified this as a "missed opportunity," though the PDPC accepted that it was "not unreasonable" to assume that Allscripts would have patched the vulnerability.

This example makes clear that healthcare organisations cannot take third-party EHR software security for granted. Though acknowledging the unusual circumstances around this vulnerability, the report indicates SingHealth should have done more extensive penetration testing during, as well as after, SCM system adoption.[77] It also recommends periodic "red team" exercises, which occur over a longer period and hence provide a more accurate emulation of APT attacks.[78]

Coordinating this is not trivial: EHR systems are large legacy systems, and healthcare organisations have limited leverage with providers as switching away is difficult.[79] But to pre-empt future difficulties, they can write cybersecurity requirements into their procurement process, e.g., using service-level objectives to specify that providers must meet well-defined metrics when fixing security issues (e.g., rectifying certain types of vulnerabilities within a particular timeframe).[80] They should work together to hold vendors responsible: in the US, group purchasing organisations provide greater purchasing power, and the Mayo Clinic, a large healthcare institution, has voluntarily shared its cybersecurity procurement language.[81]

77 Magnus, Richard, et al. 2019. "COI Report." 283–88. The report suggests that before signing any contract with Allscripts, SingHealth could have requested to review source code, asked the government to do so and provide national certification, or, if unable to review the source code, conducted its own penetration testing. It also recommends requiring certification with recognised standards like ISO/IEC 15408. The report does not make clear, however, whether these checks were or were not applied during SCM system adoption, but it does state that the SCM system was not penetration tested in the lead-up to the breach.

78 Magnus, Richard, et al. 2019. "COI Report." 288–96.

79 SingHealth doctor, interview.

80 Herr, interview; Luna, Jesus, Neeraj Suri, Michaela Iorga, and Anil Karmel. 2015. "Leveraging the Potential of Cloud Security Service-Level Agreements through Standards." IEEE Cloud Computing 2, 3: 32–40. Many thanks to Trey Herr for this particular suggestion.

81 Healthcare Supply Chain Association (https://www.supplychainassociation.org/about-us/what-is-gpo/); Boyens, Jon M., Celia Paulsen, Nadya Bartol, Kris Winkler, and James Gimbi. 2020. "Case Studies in Cyber Supply Chain Risk Management: Mayo Clinic." Gaithersburg, MD: National Institute of Standards and Technology (https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.02042020-5.pdf).

6.2. Inappropriate Network Configurations

Third-party vendors aside, healthcare organisations' own network setups can also compromise EHR security, as SingHealth's did. Though the SCM database servers were located behind a firewall, IHiS maintained an open connection with less secure servers for efficiency.[82] The COI report hence also calls for regular vulnerability assessments on assets and systems that are connected to "Critical Information Infrastructure" (in this case the SCM system), which would include the Citrix servers.[83] Yet this also raises the question of follow-through – even if a vulnerability assessment had been conducted, would corrective action have been taken?[84]

The impossibility of perfect protection should therefore make one ask if there are EHRs that are simply too valuable to risk. Stopping healthcare digitisation wholesale is unfeasible, but because VIP records (e.g., high-level political or military officials') are prime targets for APTs, it may be worth keeping them offline.[85] Digital firewalls are not enough; SingHealth did in fact restrict and log access to VIP records, but this was primarily designed to counter insider threats, and did nothing to stop the attackers.[86] Physically airgapping VIP records may hence be the best way to protect them.

82 Magnus, Richard, et al. 2019. "COI Report." 18–21, 72–79. Normally, to access the SCM database, SingHealth users cannot access data from their workstations; they must use Citrix servers, which host the SCM client application, as an intermediary. Most Citrix servers had been moved to a new H-Cloud Data Centre (HDC) behind a firewall, but several remained at the Singapore General Hospital (SGH), some outside of a firewall. Critically, IHiS maintained an open connection between the SGH and HDC Citrix servers for reasons including operational efficiency and support of legacy applications, enabling the attacker to leap into the SCM database. Barring this open connection, the SCM database was "adequately protected" within the HDC, and the attacker would not have had access otherwise.

83 Magnus, Richard, et al. 2019. "COI Report." 82–83, 281–82, 291; Cyber Security Agency, Singapore (https://www.ifaq.gov.sg/csa/apps/fcd_faqmain.aspx). The "critical infrastructure" framework is used globally to designate assets, systems, and networks that are critical to national functions. In Singapore's case, "Critical Information Infrastructure" is a specific term with legal meaning under the country's Cybersecurity Act. Regarding vulnerability assessments, no such vulnerability assessments were conducted on the Citrix servers, but if done, they ostensibly would have revealed the vulnerability and broken the attacker's final route to the EHRs.

84 This echoes the issue with the H-Cloud Pen Test. See first failure point for more on this: again, senior leadership must realistically appraise cybersecurity risks rather than merely tick off a checklist, as going through the motions alone does not guarantee improved cybersecurity.

85 Herpig, interview. Many thanks to Sven Herpig for this extremely valuable suggestion.

86 Magnus, Richard, et al. 2019. "COI Report." 20, 191–92.

7 Conclusion

Just like in healthcare itself, preventing "infection" is the ideal, but total prevention is impossible, and organisations must hence give careful thought to mitigation and treatment. Network incursions are inevitable for healthcare organisations, but the compromise of their EHRs is not, and can be prevented with these recommendations:[87]

87 Following the passage of the Cybersecurity Act of 2015, the US Department of Health & Human Services convened a task group to examine healthcare cybersecurity, and published a series of recommendations, including two separate volumes with technical recommendations, targeting small healthcare institutions and medium and large healthcare institutions, respectively. This full list of recommendations is worth referencing as well. See: US Department of Health & Human Services. 2018. "Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients." (https://www.phe.gov/Preparedness/planning/405d/Pages/hic-practices.aspx). Additionally, the DC-based think tank New America has also released a report on healthcare cybersecurity that contains informative recommendations, although it is relatively US-centric. See: Lord, Robert, and Dillon Roseen. 2019. "Do No Harm 2.0." Washington, DC: New America (http://newamerica.org/cybersecurity-initiative/reports/do-no-harm-20/).

	For Policy Makers	For Large Healthcare Institutions	For Small Healthcare Institutions
To improve senior management oversight	■ Enforce liability for cybersecurity lapses, while streamlining legislation to encourage risk management, not just compliance ■ Develop national cyber risk insurance industry ■ Consider creating/supporting an independent entity that publicly grades healthcare companies' cybersecurity ■ Consider exempting D&O insurance from coverage during basic cybersecurity lapses	■ Follow through to ensure vulnerabilities/risks are not just discovered, but fixed ■ Encourage active reporting of on-going incidents, not "fix it, then tell me" ■ Purchase cyber risk insurance ■ Conduct regular table-top exercises incorporating multiple levels of seniority ■ Hire subject-matter experts to "translate" technology risks into patient concerns for senior management ■ Consider management dashboard to capture security incidents	■ See large institution recommendations
To strengthen team response	■ Develop the healthcare cybersecurity workforce through expanding educational opportunities and organising sector-focused hackathons ■ Incentivise adoption of secure cloud-based solutions in healthcare sector, particularly among smaller institutions (e.g., through subsidising adoption) ■ Push government healthcare institutions to join information-sharing organisations, e.g., H-ISAC, and encourage other institutions to do likewise ■ Develop collective defence organisations, e.g., regional SOCs	■ Train all IT staff to identify suspicious activity ■ Strengthen incident response team with drills, predefined communication channels, and counter-APT response plan ■ Establish in-house SOC focusing proactively on threat hunting ■ Prioritise intrusion detection and national-level reporting to expedite counter-APT response ■ See other small institution recommendations	■ Train all IT staff to identify suspicious activity ■ Outsource IT needs to third-party cloud providers and cybersecurity firms to enhance security posture ■ Join H-ISAC (or other local ISACs) ■ Consider pooling resources with peer institutions to develop collective defence, e.g., regional SOCs

	For Policy Makers	For Large Healthcare Institutions	For Small Healthcare Institutions
To bolster intra-network cyber defences		■ Adopt anomaly-/behaviour-based, not signature-based, solutions ■ Enforce PAM, particularly 2FA, to limit network access even for legitimate users ■ Implement network segmentation ■ Adopt centralised EDR solution allowing remote containment and remediation of compromised endpoints ■ Consider use of just-in-time credentials ■ Consider adopting DAM for real-time EHR database monitoring	■ Enforce PAM, particularly 2FA, to limit network access even for legitimate users ■ Consider other large institution recommendations
To tighten EHR-specific security measures	■ Support healthcare institutions in assessing EHR cybersecurity through review of source code and certification against existing international standards ■ Consider mandating non-digital VIP records	■ Conduct penetration testing/source code review during EHR system adoption ■ Conduct periodic "red team" exercises emulating APT attacks ■ Procure EHR systems jointly with peer institutions, emphasising cybersecurity requirements ■ Include cybersecurity requirements in procurement process, e.g., well-defined SLOs specifying vulnerability rectification timeframe ■ Conduct regular vulnerability assessments on assets/systems connected to EHR database ■ Restrict VIP records to paper ■ Consider sharing procurement language with peer institutions	■ Procure EHR systems jointly with peer institutions, emphasising cybersecurity requirements ■ Conduct regular vulnerability assessments on assets/systems connected to EHR database

The Author

Shaun Kai Ern Ee

Shaun Ee is a nonresident fellow in the Atlantic Council's Scowcroft Center for Strategy and Security and a Yenching Scholar at Peking University, working at the nexus of international security, tech policy, and US-China relations. He also writes for TechNode, a Beijing- and Shanghai-based publication covering China's tech ecosystem, and supports Georgetown University's CSET Foretell, a "crowd forecasting" project to predict future trends in emerging tech and AI for policymakers.

Previously, Shaun worked in the Atlantic Council's Scowcroft Center across multiple initiatives. As assistant director of the Cyber Statecraft Initiative, he focused on the intersection of geopolitics, national security, and cyber policy, with publications such as "Defining Russian Election Interference: An Analysis of Select 2014 to 2018 Cyber Enabled Incidents." On the Asia Security Initiative, he focused on maritime defence in the Indo-Pacific and US-ROK-DPRK relations.

Originally from Singapore, Shaun speaks Mandarin, and served in the Singapore Armed Forces as a signals operator in an artillery unit. He holds a BA from Washington University in St. Louis, where he studied cognitive neuroscience and East African history.

References:

A "About Health Information Sharing and Analysis Center." n. d. Health Information Sharing and Analysis Center. (https://h-isac.org/about-h-isac/).

Alder, Steve. 2020. "Small-Sized and Medium-Sized Healthcare Providers Most Likely to Be Attacked with Ransomware." HIPAA Journal (blog), 16 April. (https://www.hipaajournal.com/small-and-medium-sized-healthcare-providers-most-likely-to-be-attacked-with-ransomware/).

B BBC News. 2016. "No Internet for Singapore Public Servants," 8 June. (https://www.bbc.com/news/world-asia-36476422).

"Beyond Compliance: Cyber Threats and Healthcare." FireEye, 2019. (https://www.fireeye.com/blog/threat-research/2019/08/healthcare-research-data-pii-continuously-targeted-by-multiple-threat-actors.html).

Boyens, Jon M., Celia Paulsen, Nadya Bartol, Kris Winkler, and James Gimbi. 2020. "Case Studies in Cyber Supply Chain Risk Management: Mayo Clinic." Gaithersburg, MD: National Institute of Standards and Technology. (https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.02042020-5.pdf).

C Choo, Cynthia. 2018. "National E-Records System to Undergo 'Rigorous' Security Review before Proceeding with Mandatory Contribution." TODAYonline, 6 August. (https://www.todayonline.com/singapore/national-electronic-health-record-system-undergo-rigourous-security-review-proceeding).

Choo, Cynthia. 2019. "2 IHiS Staff Sacked, CEO among Those Fined for Role in SingHealth Cyber Attack." TODAYonline, 14 January. (https://www.todayonline.com/singapore/2-ihis-staff-sacked-ceo-among-those-fined-role-singhealth-cyber-attack).

Cohen, Jessica Kim. 2020. "Ransomware Targeting Health Systems in More 'Sophisticated' Ways." Modern Healthcare, 24 January. (https://www.modernhealthcare.com/cybersecurity/ransomware-targeting-health-systems-more-sophisticated-ways).

Cullivan, Julie. 2018. "Why Defense in Depth Is Failing Us." SC Media, 4 September. (https://www.scmagazine.com/home/security-news/why-defense-in-depth-is-failing-us/).

Cyber Security Agency, Singapore. n. d. "What Is a Critical Information Infrastructure?" FAQ – Protection of Critical Information Infrastructure. (https://www.ifaq.gov.sg/csa/apps/fcd_faqmain.aspx).

H Hamilton, Michael K. n. d. “MDR vs. MSSP vs. SIEM – InfoSec Acronyms Explained.” CI Security (blog). (https://ci.security/resources/news/article/mdr-vs-mssp-vs-siem-infosec-acronyms-explained).

Health Care Industry Cybersecurity Task Force. 2017. “Report on Improving Cybersecurity in the Health Care Industry.” US Department of Health & Human Services. (https://www.phe.gov/preparedness/planning/cybertf/documents/report2017.pdf).

Healthcare Information and Management Systems Society. 2019. “2019 HIMSS Healthcare Cybersecurity Survey.” (https://www.himss.org/himss-cybersecurity-survey).

Henson, Bertha. 2018. “SingHealth COI: How Bo Chup Can You Get?” Bertha Harian (blog), 29 September. (https://berthahenson.wordpress.com/2018/09/29/singhealth-coi-how-bo-chup-can-you-get/).

I IBM. 2020. “Cost of a Data Breach Report 2019.” (https://www.ibm.com/security/data-breach).

K Kelley, Michael, and Felix Gaehtgens. 2019. “Best Practices for Privileged Access Management Through the Four Pillars of PAM.” Gartner. (https://www.gartner.com/en/documents/3899567/best-practices-for-privileged-access-management-through-).

Kirk, Jeremy. 2018. “Apple, Cisco Strike Partnerships for Cyber Insurance.” BankInfoSecurity, 6 February. (https://www.bankinfosecurity.com/apple-cisco-strike-partnerships-for-cyber-insurance-a-10632).

Kufahl, Jack, and Eric Eder. 2019. “Michigan Healthcare Security Operations Center.” (https://events.esd.org/wp-content/uploads/2019/10/Lessons-Learned-from-Operating-a-Collective-Cybersecurity-Operations-Center.pdf).

L Lee, Justina. 2018. “Suspected China Cyberhack on Singapore Is a Wake-up Call for Asia.” Nikkei Asian Review, 21 August. (https://asia.nikkei.com/Spotlight/Asia-Insight/Suspected-China-cyberhack-on-Singapore-is-a-wake-up-call-for-Asia).

Lim, Benjamin. 2018. “What Is Life at Work Without the Internet? Civil Servants Tell All.” Rice Media, 29 March. (https://www.ricemedia.co/current-affairs-features-life-at-work-without-internet-civil-servants-tell/).

Lord, Robert, and Dillon Roseen. 2019. “Do No Harm 2.0.” Washington, DC: New America. (http://newamerica.org/cybersecurity-initiative/reports/do-no-harm-20/).

Luna, Jesus, Neeraj Suri, Michaela Iorga, and Anil Karmel. 2015. “Leveraging the Potential of Cloud Security Service-Level Agreements through Standards.” IEEE Cloud Computing 2, 3: 32–40. (https://doi.org/10.1109/MCC.2015.52).

M

Magnus, Richard, Fook Sun Lee, T. K. Udairam, and Hui Fong Cham. 2019. “Public Report of the Committee of Inquiry into the Cyber Attack on Singapore Health Services Private Limited’s Patient Database on or around 27 June 2018.” Singapore: Committee of Inquiry. (https://www.mci.gov.sg/coireport).

Marsh & McLennan Companies. 2018. “Holding Healthcare to Ransom: Industry Perspectives on Cyber Risks.” (https://www.marsh.com/sg/insights/research/holding-healthcare-to-ransom.html).

May, Christopher, Joshua Hammerstein, Jeffrey Mattson, and Kristopher Rush. 2006. “Defence in Depth: Foundations for Secure and Resilient IT Enterprises.” Pittsburgh: Carnegie Mellon University. (https://resources.sei.cmu.edu/asset_files/Handbook/2006_002_001_14633.pdf).

“Mi|HSOC – Michigan Healthcare Security Operations Center.” n. d. CyberForce|Q. (https://www.cyberforceq.com/mi-hsoc).

Mohan, Matthew. 2019. “PDPC Fines IHiS, SingHealth Combined S$1 Million for Data Breach Following Cyberattack.” CNA, 15 January. (https://www.channelnewsasia.com/news/singapore/ihis-singhealth-fined-1-million-data-breach-cyberattack-11124156).

Morse, Susan. 2019. “Healthcare’s Number One Financial Issue Is Cyber Security.” Healthcare Finance News, 30 July. (https://www.healthcarefinancenews.com/news/healthcares-number-one-financial-issue-cybersecurity).

P

Poon, Chian Hui. 2017. “Public Healthcare Sector to Be Reorganised into 3 Integrated Clusters, New Polyclinic Group to Be Formed.” The Straits Times, 18 January. (https://www.straitstimes.com/singapore/health/public-healthcare-sector-to-be-reorganised-into-3-integrated-clusters-new).

S

Sullivan, Tom. 2017. “75% of Health Orgs Live below Cybersecurity Poverty Line.” Healthcare IT News, 11 May. (https://www.healthcareitnews.com/news/75-health-orgs-live-below-cybersecurity-poverty-line).

T Tan, Kiat How, and Zee Kin Yeong. 2019. “Breach of the Protection Obligation by SingHealth and IHiS.” Singapore: Personal Data Protection Commission. (https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Commissions-Decisions/Grounds-of-Decision---SingHealth-IHiS---150119.pdf).

Tham, Irene. 2018. “Top-Secret Report on SingHealth Attack Submitted to Minister-in-Charge of Cyber Security.” The Straits Times, 31 December. (https://www.straitstimes.com/singapore/top-secret-report-on-singhealth-attack-submitted-to-minister-in-charge-of-cyber-security).

Tham, Irene, and Min Zhang Lim. 2018. “IT Vendor Employee Found Alleged Flaw in System in 2014.” The Straits Times, 29 September. (https://www.straitstimes.com/singapore/it-vendor-employee-found-alleged-flaw-in-system-in-2014).

“Three Elements That Every Advanced Security Operations Center Needs.” n. d. CSO (blog). (https://www2.cso.com.au/article/563871/three-elements-every-advanced-security-operations-center-needs/).

U US Department of Health & Health Services. 2018. “Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients, Technical Volume 2: Cybersecurity Practices for Medium and Large Health Care Organizations.” US Cybersecurity Act of 2015, Section 405(d) Task Group. (https://www.phe.gov/Preparedness/planning/405d/Documents/tech-vol2-508.pdf).

US Department of Health & Human Services. 2018. “Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients.” Public Health Emergency, 28 December. (https://www.phe.gov/Preparedness/planning/405d/Pages/hic-practices.aspx).

W Watts, Jake Maxwell, and P. R. Venkat. 2019. “State-Backed Hackers Sought and Stole Singapore Leader’s Medical Data.” Wall Street Journal, 10 January. (https://www.wsj.com/articles/state-backed-hackers-sought-and-stole-singapore-leaders-medical-data-11547109852).

“What Is a GPO?” n. d. Healthcare Supply Chain Association. (https://www.supplychainassociation.org/about-us/what-is-gpo/).

“What Is Cyber Threat Hunting?” Crowdstrike (blog), 21 June 2019. (https://www.crowdstrike.com/epp-101/threat-hunting/).

“Why Choose MDR over MSSP or SIEM?” n. d. Arctic Wolf (blog). (https://arcticwolf.com/resources/briefs-2/why-choose-mdr-over-mssp-or-siem).

Interviews:

A Agachi, Anca. 2020. Assistant Director of the Foresight, Strategy, and Risks Initiative, Scowcroft Centre for Strategy and Security, Atlantic Council, in discussion with the author.

H Herr, Trey. 2020. Director of the Cyber Statecraft Initiative, Scowcroft Center for Strategy and Security, Atlantic Council, in discussion with the author.

Herpig, Sven. 2020. Project Director for International Cybersecurity Policy, Stiftung Neue Verantwortung (SNV), in discussion with the author.

M MITRE staff, in discussion with the author. 2020.

R Rosenblum, Todd. 2020. Former senior US defence and homeland security official from 2009–16, in discussion with the author.

S Singapore doctor wishing to remain anonymous, in discussion with the author. 2020.

Szanto, Alexander. 2020. Cybersecurity Junior Research Fellow at the Brandenburg Institute for Society and Security (BIGS), in discussion with the author.