Nihal Pai
Comp 116

Professor Ming Chow
Final Paper

The State of Cyber Security in Singapore

I. Abstract

Once a fishing village serendipitously located in the centre of South East Asian maritime commerce, Singapore has since blossomed into a digitally-enabled nation that facilitates a large portion of global finance, commerce, and transport. However, the same prominence that brought Singapore to the world stage also puts it directly in the line of fire from well-orchestrated cyber threats. This paper focuses on how Singapore has developed its thorough cyber security legislation and infrastructure over time, and details how the most serious cyber threat in its history, 2018's SingHealth data breach, occurred despite these protective measures. The paper will also describe the countermeasures taken by digital administrators of SingHealth, and project a series of practices based on global industry standards that might prevent and mitigate the risks of such attacks. The paper also stresses the importance of investing in cyber hygiene education in local Singaporean communities to install longstanding resistance to cyber threats on a fundamental level.

II. Introduction

As a global banking, maritime, and aviation hub, Singapore plays a vital role in facilitating the transactions incurred within the digitised economies it operates in. The minuscule city-state is a conduit for a significant proportion of the world's freight, air traffic, and financial capital, putting it at the figurative crosshairs of cyber attacks that are likely to have radiating effects on digital systems beyond its borders. These risks necessitate an immense responsibility to actively secure the cyber infrastructure that forms the foundation of its economic activities. Over the past few years, Singapore has been in the process of developing a robust cyber security enhancement program, with one of its major initiatives being the founding of the Cyber Security Agency of Singapore (*CSA*). The CSA is a governmental branch charged with the centralised superintendence of national cyber matters within both the private and public sectors. In 2016, CSA released a briefing highlighting its plan to focus on the main pillars of operation that centre around building resilient infrastructure, developing robust policy frameworks, promoting collective responsibility amongst communities, combating cyber crime, investing in professional cyber security talent, and forging strong international legislative alliances. While the main aims of these pillars continue to remain highly relevant, recent infractions such as July 2018's severe breach of digital health records necessitate the need for evolving strategies and legislation, like the passing of 2018's *Cyber Security Act* omnibus bill. This paper will hence serve to a) provide a brief history of cyber security development in Singapore, b) summarise the basis of CSA's overarching strategic pillars and the omnibus bill, c) delineate the concerted SingHealth breach that prevailed despite these robust initiatives, and d) evaluate what went wrong in the case of SingHealth and suggest potential actionable steps to prevent future attacks.

III. To the Community

Singapore's thorough analysis of global cyber threats, implementation of its equally extensive strategies, and pivoting of pre-existing policies in response to new threats gives me immense confidence that its citizens and the economies it affiliates with are in ultimately good hands. The country, often referred to as the Switzerland of the East, is sometimes likened to a protective bubble that isolates its residents from the major conflicts of the world. However, such attitudes cannot remain unchanged, as conflict in the digital realm has become far easier to incite than in the past, even in peaceful countries like Singapore. I recently learned this the hard way, when this past summer, I received a harrowing letter from my own government informing me that my public health records, along with those of Singapore's Prime Minister Lee Hsien Loong and 1.5 million others' [2], had been hacked and stolen in the nation's most severe and professionally articulated cyber attack to date. The letter assured me that the government would be taking the required steps to mitigate the possibility of such attacks occurring again. The incident provoked me to think about several important things that are relevant to any digitally-enabled community, the first of which being that it is crucial to conduct proper post-mortems and understand how such attacks could still slip between the cracks despite the government's rigorous planning and execution of defence protocols. Secondly, it made me realise just how tremendous the impact on international commerce would have been, had this attack targeted other critical digital infrastructures related to Singapore's digitally-entangled economy. To many, the attack also served as a jarring reminder that online, safety absolutely cannot be taken for granted and that this stuff happens much too often to be taken lightly. For example, I found out that in 2016 and 2017 alone, cybercrime accounted for 16.6% of overall crime, with a multitude of global-scale data breaches that impacted Singaporean citizens. These included everything from phishing and 25 ransomware cases to Dark-Web crimes and Uber's 2016 breach that compromised 380000 Singaporean users [5]. It was hence clear that the best ways to develop true resilience within communities was to a) raise awareness and implement proper practices from grassroots levels i.e. within regular citizens and b) critically evaluate in-place policies and facilitate their subsequent restructuring in anticipation of threats rather than in response to them.

III. A Brief Timeline of Cyber Security in Singapore

Singapore's deep dive into cyber security development [1] of its thorough cyber security Masterplan, beginning with the Infocomm Security Masterplan (*ISMP*) from 2005 to 2008. This focused on building the public sector's foundation of basic defence and threat response protocol, as well as the security of the Critical Information Infrastructure (*CII*) that underlies defence, foreign relations, public health, public safety, national security, and general public order. Following this foundation, several iterations were made to the Masterplan from 2008 to 2015, such as the establishment of the Singapore Infocomm Technology Security Authority (*SITSA*) that deals with cyber-espionage, an augmented Masterplan that focused more on securing individuals and businesses within its info-comm network, the National Cybersecurity R&D Programme that aimed to foster cyber security expertise as well as fortify the integrity of cyber infrastructure, and the construction of the National Cyber Security Centre (*NCSC*), a hub to ensure the relevant organisations are aware of and coordinated in their response to national/global-scale cyber attacks across sectors. 2015 saw the birth of the Cyber Security Agency of Singapore (*CSA*) under the Prime Minister's Office. A definitive landmark in the nation's cyber development, the *CSA* essentially absorbed all organisations related to cyber security and currently spearheads Singapore's

cyber policy-making, master-planning, and coordination of efforts across governmental, industrial, and educational institutions, as well as businesses, individuals, and international entities. Following this, a cyber law-enforcement agency known as the Cybercrime Command was augmented to the Singapore Police Force. The Command marked a deliberate foray into investing in post-mortem analysis and investigation of cyber attacks. However, Singapore's cyber security ventures more saliently entered the public and international consciousness in 2016, when the Ministry of Home Affairs launched the National Cybercrime Action Plan (*NCAP*). The initiative emphasised the need for public education regarding online safety, reinforcing cybercrime laws, developing offensive cyber capabilities, and forging local and international alliances. Here, the pillars of the *CSA*'s strategy were established. However, in April 2017, the inevitable finally occurred when cyber criminals compromised the networks of Singapore's two leading universities (National University of Singapore and the Nanyang Technological Institute), seizing critical data regarding the transport sector, defence initiatives, and foreign affairs [3]. This sophisticated and impactful breach set a clear precedent for what the nation should expect from cyber threats, namely Advanced Persistent Threats *APT*'s) that directly target information regarding national security and could lead to loss of life if placed the wrong hands. In response to this, the government revealed the Cybersecurity Bill for public consideration, which granted the *CSA* the necessary powers to actively contain and neutralise cybersecurity threats. This greatly broadened the *CSA*'s operational scope, allowing them access not just CII but also the rights to investigate any personal computer or system and direct individuals to execute corrective measures during attacks [4]. In 2018, Singapore finds itself with a new Cyber Security Act omnibus bill, which details new roles that require enterprises to implement thorough incident response plans to ensure compliance in terms of timely reporting of security breaches [3].

IV. Summary of Singapore's Cyber Security Strategy

Despite the various attacks that have occurred in the past (and will occur in the future), Singapore's approach to enhancing cyber security preparedness involves exceptionally proactive measures [5] that could, if executed appropriately, reflect an ideal for other digital communities to aspire to. Its two major initiatives, the *CSA* Pillars and the recent *Cyber Security Act* omnibus bill are representative of this approach.

The firs tenet of *CSA*'s Pillars revolves around *Enhancing Cyber Preparedness Against Cyber Threats* and *Building Resilient Infrastructure*. This is accomplished by regularly tasking organisations from different sectors with rigorous cyber exercises, with the aim of giving them the expertise to anticipate cyber attacks by effectively reviewing and adapting incident response strategies and cooperating seamlessly across sectors. Exercises range from industry-specific such as *Exercise CyberArk* [6], which is focused on the finance/banking industry, to national-level such as the holistic *Exercise Cyber Star*, which involves a whole swathe of organisations from multiple CII sectors such as aviation, land transport, maritime, media, energy, government, info-comm, healthcare, water, and security & emergency [7]. These exercises are key to uncovering and remediating weaknesses in their defence capabilities. Part of this Pillar involves the *Cyber Security Act* omnibus bill [5], which is primarily focused on augmenting existing policies to include the capacity for greater inspection and maintenance of systems. The Act details four main legislative features, the first of which designates a framework to ensure CII owners are well-versed on their duty to safeguard CII's and report incidents directly to the CSA. This aims to expedite internal processing of attacks and deal out the necessary remedies in a timely fashion. The second gives the

Commissioner of the *CSA* full power to launch investigations of threats and incidents based on their severity. This includes the power to examine individuals as well as procure and impound evidence. Assistant Commissioners may also be added to reduce bureaucracy faced by CII owners [8]. The third focuses on building a preventative system of information exchange, allowing the *CSA* to request information, hence ensuring the government is notified of potential vulnerabilities early. The system enables regulated protection and sharing of this information. Finally, the Act enforces a licensing framework for providers of cybersecurity services such as penetration testers, whose job scope often involves them obtaining sensitive information of vulnerabilities in clients' systems [9]. This aims to assure clients that their information is being accessed only by qualified providers, encouraging them to invest more heavily in these protective measures.

The second tenet of the *CSA*'s approach aims to *i*. As an internationally-oriented nation, Singapore annually hosts its Singapore International Cyber Week (*SICW*), which attracts thousands of policy-makers, industry veterans, and NGO's from over 50 regional and international partners [5]. The week's events range from cyber leadership symposiums to IoT conversations on industry standards and cooperative measures. Singapore invests heavily in in establishing initiatives with countries such as Australia, Germany, the UK, and Japan in the Memoranda of Understanding (*MOU*) as well as its ASEAN allies in the ASEAN Cyber Capacity Programme. These initiatives involve workshops and detailed discussions to facilitate the development cyber norms, thereby mitigating the potential for cyber conflict by allowing nations to work in tandem to secure their shared future in the digital world.

The third tenet of the *CSA* is concerned with *Developing a Professional Cybersecurity Workforce*. By engaging with educational institutions and industry partners, the government has developed highly-specialised programmes to enhance cyber security fluency of Singapore's youth. Some effective examples include the SkillsFuture Work-Study Degree / Earn & Learn initiatives [5], which allows students to gain practical work skills while working towards official cyber security qualifications, and the Cyber NSF Vocation [5], which allows appropriately-vetted National Servicemen to serve in advanced cyber roles such as forensics and penetration testing in association with technical institutes like Singapore Institute of Technology. As someone who has been through the 2-year National Service program, I believe this is a much-needed utilisation of latent talent that often goes wasted. This tenet also facilities Professional Conversion Programmes [5], affording people the training to switch into cyber security-related fields mid-career. These measures implant cyber security education in several aspects of society, directly involving the community and building a vibrant cyber ecosystem.

The fourth tenet primarily concentrates on investment in *Research and Development* in tandem with a Security-by-Design approach. This area homes in on using blockchain technology and Cyber-Physical Systems to secure in the logistics sectors as well as evaluation frameworks to better asses and verify cyber security and IoT products, which pose significant threats in terms of vulnerabilities [5]. Start-ups and incubators that develop cyber security solutions are also enjoying heavy investment, while the Proof-of-Concept (*POC*) scheme provides funding of up to $500000 for up to 12 months for developing promising and innovative cyber security solutions with the end goal of commercial use [10]. This Pillar also involves an extensive bug bounty program posed by the Ministry of Defence, which has seen global white-hat participation from the likes of 57 of HackerOne's top 100 hackers and payouts of up to US$14750 [11]. These methods make for a holistic structure of predictive, defensive, and detective strategies that enhance overall vigilance [5].

Lastly, the *CSA* places heavy emphasis on cultivating cyber-awareness within civilian communities. The aim is to start by improving cyber hygiene to protect personal devices, through outreach methods such as the National Cybersecurity Awareness Campaign, the inclusion of Cyber Safety activity books in elementary school classrooms, and helping businesses and individuals stay up to date on cyber issues and official announcements through social media outlets and the GoSafeOnline website [5].

V. The Big One: 2018 SingHealth Data Breach

While Singapore remained generally unharmed from major global cyber attacks such as WannaCry and the Equifax breach in 2017, June 2018 brought the most severe data breach the nation had ever seen through extensive intrusions of Electronic Medical Records (*EMR*'s) via the digital SingHealth platform. The *EMR*'s, containing personal (non-medical) information, belonged to 1.5 million patients who visited specialist outpatient clinics from May 1st, 2015 to July 4th, 2018 [12].The attack took the form of unauthorised queries to the SingHealth database; the attackers first attempted to remotely log in to servers linked to the *EMR* database by compromising inactive administrator accounts, and then made an effort to access close to 100000 *EMR*'s [13]. While the former attempt failed, the head of the cyber security organisation in charge of digital health records, Mr. Wee of the Integrated Health Information Systems (*IHiS*), did not link the two events despite the reports from subordinate system engineers. This was primarily due to miscommunication between divisions regarding the operating procedure for the speed at which risks are to be reported and expunged, and lack of upper-management diligence, which caused significant bottlenecks in threat detection and subsequent defensive measures. In terms of the technical details, investigations revealed that attackers were able to gain access by injecting one of SingHealth's front-end workstations with malware between June 27th and July 4th [14] . In the wake of the attack, immediate security measures were set in motion. *IHiS* administrators got to work changing server and admin passwords, restricting domain administration access, blocking connections to halt additional access, and closely monitoring database and system logs [14]. The *IHiS* also temporarily sanctioned internet separation to isolate their databases from further attacks [15]. In terms of subsequent communication procedure between organisations and with the public, *IHiS* informed the Ministry of Health, SingHealth, and the *CSA* of the attack on July 10th once forensics confirmed the incident. On July 20th, SingHealth began contacting all the affected patients to inform them of the data breach. Authorities stated that they would refrain from adding new information and communication technology systems until they finish implementing the appropriate remedial measures [14]. While additional data was not stolen and patient care unscathed, the attack represented the fact that just a single vulnerability in an otherwise robust security system can cause an unprecedented amount of damage.

VI. Action Items: Suggestions for Protecting User Data

The *IHiS*'s temporary solution of enforcing internet separation is not ideal in the long-run and does not complement the nature of all institutions. Even in this case, implementing this in hospitals would severely hinder progress for doctors in life-saving situations [16]. Several countermeasures can be taken to prevent this sort of attack form occurring, or at least minimise their impact. While I am not a cyber security expert, my research [17] yielded several tips for organisations that would shield user data from similar attacks. For one, companies that collect private user data have a responsibility to safeguard it. This could be accomplished by encrypting the data, limiting employee access to reduce the number of 'entry points', as well as conduct thorough evaluations of existing data containment policies - how much non-medical information did SingHealth really need here? Irrelevant data should be subsequently deleted from systems to prevent exposure as even if the user's account becomes inactive, their personal information still remains the same. Companies that find themselves in similar situations of personal data storage can implement several protocols to detract from SingHealth's fate. For one, several institutions make use of PowerShell scripting tools within workstations. These are highly exploitable, allowing malicious users to easily inject undesired scripting/commands, and should be deactivated if not being used actively. Organisations should also continue to invest in monitoring tools for SQL queries seeking unauthorised remote access to databases. Remote access especially should fortify access points with strong passwords and limit access to certain personnel. Administrators, who have full access to domains, should have their accounts regularly purged for inactivity i.e. restrict access to the keys to the kingdom. Organisations can also engage in whitelisting authorised lists of applications for non-administrative users, thereby disallowing potentially malicious software that goes undetected by traditional antivirus programs from running in the background. All associated systems should also be regularly patched and updated with security improvements as soon as they are made available. Endpoints that are known to run for long periods of time should be regularly checked for malware injection, while inactive endpoints containing old and vulnerable software should still be treated as potential entry points and be promptly deleted. Lastly, as we have seen in the SingHealth case, communication between subordinate security engineers and supervisors who actually have the authority to administer changes should be less bureaucratic and streamlined, especially with regards to the proper expectations for following incident management protocol. Authoritative burdens for team leaders can also be shared to reduce the chance of lapses in detection (think pair programming). For further inspiration, the Singaporean government may look to international industry standards [16] such as ISO 27001, IEC 27033, and the cloud computing security standard of the US National Institute of Standards and Technology. These frameworks would enable organisations to expedite the process of risk detection and mediation, enable the construction of secure network architecture in daily activities like communications through gateways and firewalls [16], and ensure that the necessary architecture to support cloud operations is designed sufficiently. The best part about these strategies, as my research suggests, is that they would not require organisations to limit internet access or hamper productivity.

VII. Conclusion

While these measures are extensive and would provide adequate protection against future attacks, I believe that the key to propagating true resilience to digital threats is to invest in the entire cyber ecosystem. In a country as small and well-governed as Singapore, focusing on arming the community with knowledge of the necessary cyber hygiene, and forming social attitudes around them that translate directly into business settings, would not be the most ridiculous venture. By deeply ingraining cyber hygiene into society, inconsistencies and lapses in awareness, detection, and defensive measures might be less likely. I believe that the *CSA*'s pillars, the Cyber Security Act, and investment in the wider Singaporean community definitely put the nation on the right track to achieving this vision, especially considering its overarching SmartNation objective. While these changes may take time to inculcate and require substantial investment on the grassroots level, it is better to sacrifice temporary short-term benefits for the continuous pursuit of a potential long-term panacea.

IV. References:

[1] Singapore, Cyber Security Agency of Singapore, Multiple Contributors. “Singapore's Cyber Security Strategy.” *Singapore's Cyber Security Strategy*, Cyber Security Agency of Singapore , 2016, pp. 1–27.

[2] Tham, Irene. “Personal Info of 1.5m SingHealth Patients, Including PM Lee, Stolen in Singapore's Worst Cyber Attack.” *Straits Times*, Singapore Press Holdings, 20 July 2018, www.straitstimes.com/singapore/personal-info-of-15m-singhealth-patients-including-pm-lee-stolen-in-singapores-most.

[3] Resolve Systems. The Definitive Guide to Cybersecurity in Singapore. The Definitive Guide to Cybersecurity in Singapore, Resolve Systems, 2018.

[4] Song, Daniel. “What You Need to Know about Singapore's New Cybersecurity Bill.” *Bird & Bird*, Bird & Bird, July 2017, www.twobirds.com/en/news/articles/2017/singapore/what-you-need-to-know-about-singapores-new-cybersecurity-bill.

[5] Cyber Security Agency of Singapore, Singapore Police Force. *Singapore Cyber Landscape 2017*. *Singapore Cyber Landscape 2017*, Cyber Security Agency of Singapore, 2017, pp. 1-28

[6] Multiple Contributors. “CSA Conducts First Cyber Security Table-Top Exercise.” *Cyber Security Agency of Singapore*, Cyber Cyber Security Agency of Singapore, 26 May 2015, www.csa.gov.sg/news/news-articles/cyber-security-table-top-exercise.

[7] Multiple Contributors. “CSA Leads Whole-of-Government Exercise to Respond to Cyber Attacks.” *Cyber Security Agency of Singapore*, Cyber Cyber Security Agency of Singapore, 18 July 2017, www.csa.gov.sg/news/press-releases/csa-leads-wog-exercise-to-respond-to-cyber-attacks.

[8] Cramer, Stella, et al. “Singapore's New Cybersecurity Act Comes into Force: Here's What You Need to Know.” *DataProtectionReport.com*, Norton Rose Fullbright LLP, 10 Sept. 2018, www.dataprotectionreport.com/2018/09/singapores-new-cybersecurity-act-come-into-force-heres-what-you-need-to-know/.

[9] Multiple Contributors. “Cybersecurity Act.” *Cyber Security Agency of Singapore*, Cyber Cyber Security Agency of Singapore, 5 Feb. 2018, www.csa.gov.sg/legislation/cybersecurity-act.

[10] Multiple Contributors. “Co-innovation and Development Proof-of-Concept Funding Scheme.” *Cyber Security Agency of Singapore*, Cyber Cyber Security Agency of Singapore, 30 Nov. 2018, https://www.csa.gov.sg/programmes/proof-of-concept-scheme.

[11] Cyber Security Agency of Singapore, Singapore Police Force. *Singapore Cyber Landscape 2017*. *Singapore Cyber Landscape 2017*, Cyber Security Agency of Singapore, 2017, pp. 1-28

[12] Multiple Contributors. “SingHealth Cyber Attack: How It Unfolded.” *Straits Times*, Singapore Press Holdings Digital News , 20 July 2018, graphics.straitstimes.com/STI/STIMEDIA/Interactives/2018/07/sg-cyber-breach/index.html.

[13] Tham, Irene. “COI on SingHealth Cyber Attack: Failings in Judgment, Organisation Exposed.” *The Straits Times*, Singapore Press Holdings Digital News , 27 Sept. 2018, www.straitstimes.com/singapore/failings-in-judgement-organisation-exposed-as-cyber-attack-coi-grills-singhealth-risk-man.

[14] Multiple Contributors. “SingHealth Cyber Attack: How It Unfolded.” *Straits Times*, Singapore Press Holdings Digital News , 20 July 2018, graphics.straitstimes.com/STI/STIMEDIA/Interactives/2018/07/sg-cyber-breach/index.html.

[15] Multiple Contributors. “[SingCERT] Technical Advisory on Measures For Protecting Customers' Personal Data.” *Cyber Security Agency of Singapore*, Cyber Cyber Security Agency of Singapore, 20 July 2018, www.csa.gov.sg/singcert/news/advisories-alerts/measures-for-protecting-customers-personal-data.

[16] Goh, Benjamin. “Commentary: Implement Internet Separation? Let's Learn from Industry Best Practices.” *Channel NewsAsia*, Mediacorp Pte Ltd, 27 July 2018, www.channelnewsasia.com/news/commentary/singhealth-healthcare-serious-cyberattack-internet-separation-10565018.

[17] Multiple Contributors. “[SingCERT] Technical Advisory on Measures For Protecting Customers' Personal Data.” *Cyber Security Agency of Singapore*, Cyber Cyber Security Agency of Singapore, 20 July 2018, www.csa.gov.sg/singcert/news/advisories-alerts/measures-for-protecting-customers-personal-data.

[18] Ghosh, Nirmal. “Cyber Security Essential to Singapore's Survival: CSA Chief David Koh.” *The Straits Times*, Singapore Press Holdings Digital News , 21 Mar. 2018, www.straitstimes.com/world/united-states/cyber-security-essential-to-singapores-survival-says-csa-chief-david-koh.