Healthcare Cybersecurity:

Advancing and Innovating Safely

As the profession increasingly taps on the powers of technology and data, there needs to be vigilance in protecting the healthcare information entrusted to us by patients. In this Feature piece, we invite three authors to share their perspectives and insights into cybersecurity within their respective sectors.

Text by Chua Kim Chuan

I have been a cybersecurity practitioner for over 30 years, long before it was called cybersecurity. As a Chief Information Security Officer of a Singapore healthcare cluster, some of the questions I get asked regularly include "**What keeps you awake at night?**" and "**What can I do to protect my computer from viruses?**" These questions underscore the vital importance of cybersecurity in our daily lives.

Clearly, cybersecurity challenges have become much more threatening over the last decade.

It has been four years since cybercriminals accessed SingHealth patient data in one of the worst cyberattacks in Singapore. Cyberattacks in healthcare surged globally last year, with an all-time high of data breaches in 2021 exposing 45.67 million patient records in the United States alone. In Singapore, two private healthcare providers reported customer data theft incidents in the same year.

We should not feel discouraged as there are many things we can do to protect ourselves. I have compiled some cybersecurity practices that can help us all stay cyber-safe, or at least cyber-safer. These measures are evergreen, relevant, critically important and by no means exhaustive.

Keep your IT "house" in order

As a consumer of digital services, we have no control over the actions of "bad actors" – ie, the cybercriminals. But what we can do is to keep our "house in order". By that, I mean keeping the software on our personal computers, smartphones, network routers and webcams up-to-date. Many vendors that take cybersecurity seriously provide automatic updates for their software and it would be a good idea to enable such services, where available.

Keeping our house in order also means removing obsolete applications and utility software that you no longer need or use and, most importantly, ensuring that antivirus software and virus signatures are updated. Make sure you purchase products from trustworthy vendors and install applications from trusted application stores to avoid unwanted "backdoors" into your "house". Remember to change the default password on all IT devices, including routers and your Internet Protocol television cameras to prevent unwanted voyeurs.

Protect your digital identity

We interact with most of cyberspace through our "digital identity", like our Apple ID, Google or Microsoft accounts. If we are not careful, these identities can be hijacked and taken over by cybercriminals. We all know the importance of using strong passwords, and it is important to not stop there; you should proceed to activate Two-Factor Authentication (2FA) services for your online accounts. Most of the popular Internet cloud services support multiple 2FA services including SMS One-Time Passwords (OTP), and this should be a default practice whenever we sign up for an Internet service.

Keep your cyber guard up

Cyberspace is an inherently unsafe place, and it is best to be cautious and suspicious when online. Remember that while we protect our digital identities, cyber fraudsters are highly proficient at impersonating friends, colleagues or technical support personnel. Some will make up false identities for the purpose of committing fraud.

So be on your guard when online, and if you receive an unusual or odd request through social media application from a "friend", it would be prudent to take a pause, and not respond immediately. Try to contact the person using SMS or telephone to verify if the request is genuine. Be careful and refrain from clicking on suspicious links from emails which came out of the blue, "too good to be true" offers such as super cheap mobile phones and cryptocurrency, or other offers or emails with a sense of urgency pressing you for immediate action.

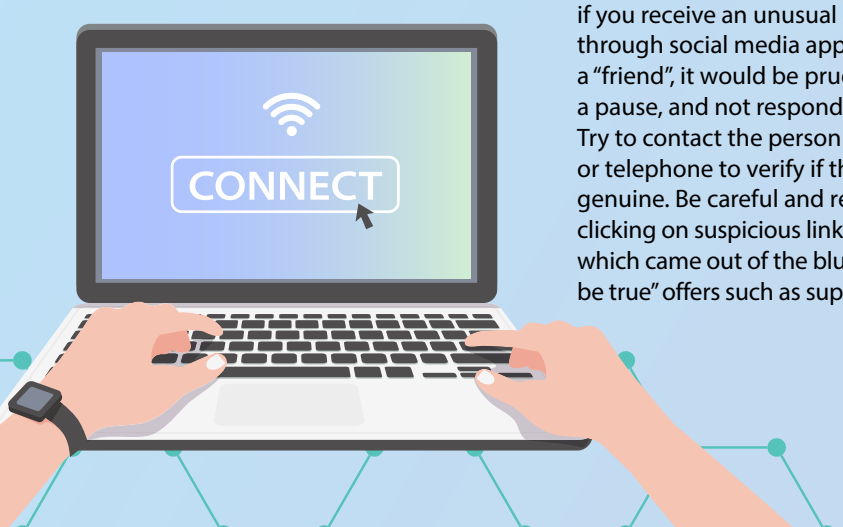
Prepare for the worst

Despite our best efforts to protect ourselves, there are still many things in cyberspace that are beyond our control, and the unforeseen can happen. It is prudent to take measures now to prepare for the unfortunate event that your data becomes corrupted or your digital identity is stolen, so that the consequences will not be catastrophic.

The most practical way to do this is to regularly perform backups of your personal data. Ask yourself what emails, legal documents, photos and videos in your personal devices are important to you, and would need to be protected. Make that list, backup those files in a removable storage device and keep them away in a safe location. Make it a habit, and do it regularly. With some luck, you will never need to use it, but it is there for your peace of mind. For those who may find the backup process to be a chore, consider subscribing to online backup solutions offered by major service providers that will automatically backup these data for a small monthly fee.

Summary

Modern digital technologies are part of our daily routine and modern lifestyle. Digital services, with the pervasive use of smartphones have offered us much ease and convenience. However, technology is also a double-edged sword and we need to stay vigilant and be on constant guard against cybercriminals. It does not really require much to be cyber-safe, and following some basic principles can go very far in protecting our personal devices and data.



Kim Chuan is the Group Chief Information Security Officer at SingHealth and has had a front row seat in the evolution of cybersecurity over the past 30 years. He has held senior IT security leadership role in the Ministry of Health Holdings and Integrated Health Information Systems Pte Ltd.

Text by MAJ (Dr) Lim Jia Chen

Prior to 2018, the Ministry of Defence (MINDEF) and the Singapore Armed Forces (SAF) had already implemented a multi-tier system of cybersecurity measures to protect our medical systems and data. The SAF takes a "zero-trust" approach on cybersecurity, with the Defence Cyber Organisation (DCO) set up in 2017 to lead and drive cybersecurity efforts across the defence sector.[1] In particular, we recognise the reputational risk of data loss and service disruption to the SAF.

Safeguarding practices

At an application and connectivity level, our SAF Electronic Medical Records (EMR) resides within hardened SAF networks.[2] Even though it is connected to the National Electronic Health Records and other healthcare infrastructure and interfaces in real time, the SAF EMR terminals are internet-separated as an added layer of security.[3] At a database level, our data is encrypted at rest and subjected to cybersecurity protection measures stipulated by DCO. Beyond organisational internal audits and checks, the MINDEF Bug Bounty Programmes invited white-hat hackers to test the SAF's major internet-facing systems, including our personnel's medical health information portal, eHealth, for vulnerabilities and bugs.[4] This is to strengthen our defences against the increasing number and sophistication of cyberattacks.

The SAF is cognisant that the last mile of our cybersecurity defence is maintained by our people, who must be the strongest link.[5,6] Prior to accessing our EMR system, our personnel are put through dedicated training programmes on cybersecurity and data protection. MINDEF and SAF also emphasises educating users on protecting themselves against malicious cyber activities, as well as adhering to proper security protocols.

Responses following the data breach

The 2018 Healthcare Data Breach was unprecedented; it took the nation by surprise and left us with many lessons. These existing systems have served us well, as we were able to comply with the measures recommended by the Public Sector Data Security Review Committee (PSDSRC) in 2019,[7] following its review of the data security policies and data governance practices across the public sector in the aftermath of the healthcare data breach.

Evolving threats

Cybersecurity threats continue to increase in volume and complexity. The recent OCBC phishing scams[8] and the Solarwinds hack[9] have shown that malicious actors are constantly devising new methods to exploit vulnerabilities in our cybersecurity defences, regardless of industry. The SAF and its defence partners cannot assume that our current posture will be sufficient in the years ahead.

The COVID-19 pandemic demonstrated the need for a faster pace of healthcare innovation, workflow integration and interoperability between connected ecosystems to benefit the patient.[10] Healthcare organisations worldwide typically lag behind other industries in their ability to handle cyberattacks.[11,12] The increase in connectivity between organisations and the number of connected devices to the cloud mean that cybersecurity and medical data protection measures will need to adapt and keep pace to protect the healthcare community from cyberattacks. These attacks not only pose risks to the healthcare business, but also translate to other risks such as patient care becoming compromised due to healthcare operations being disrupted.

It is not a matter of if, but when and how extensive.

Acknowledgement

The author thanks COL (Dr) Tan Nan Guang for his guidance and input while preparing this article.

References

1. MINDEF Singapore. Fact Sheet: A Restructured SAF to Better Meet New Security Threats. Available at: https://bit.ly/3blPXns. Accessed 14 June 2022.

2. MINDEF Singapore. Patient Care Enhancement System (PACES) The SAF's Electronic Medical Records System. Available at: https://bit.ly/3tU6gOs. Accessed 14 June 2022.

3. Ministry of Health Singapore. Temporary Internet Surfacing Separation Implemented at all Public Healthcare Clusters. Available at: https://bit.ly/3bmHoIJ. Accessed 14 June 2022.

4. MINDEF Singapore. Fact sheet: Ministry of Defence (MINDEF) Bug Bounty Programme. Available at: https://bit.ly/3zZAio8. Accessed 14 June 2022.

5. MINDEF Singapore. Cyber Defence. Available at: https://bit.ly/3NdQpRY. Accessed 14 June 2022.

6. Martin G, Ghafur S, Kinross J, Hankin C, Darzi A. WannaCry—a year on. BMJ 2018; 361:k2381.

7. Smart Nation Singapore. Completion Of Public Sector Data Security Review To Secure And Protect Citizen's Data. Available at: https://bit.ly/3OyOrg2. Accessed 14 June 2022.

8. Chelvan VP. OCBC says S$13.7 million lost in phishing scams, up from S$8.5 million. CNA [Internet]. 30 January 2022. Available at: https://bit.ly/3HKOqTM.

9. Temple-Raston D. A 'Worst Nightmare' Cyberattack: The Untold Story Of The SolarWinds Hack. NPR [Internet]. 16 April 2021. Available at: https://n.pr/3xQYGW4.

10. Sheikh A, Anderson M, Albala S, et al. Health Information Technology and digital innovation for national learning and health systems. Lancet Digit Health 2021; 3(6):e383-96.

11. Kruse CS, Frederick B, Jacobson T, Monticone DK. Cybersecurity in Healthcare: A systematic review of modern threats and trends. Technol Health Care 2017; 25(1):1-10.

12. Abraham C, Chatterjee D, Sims RR. Muddling through cybersecurity: Insights from the U.S. Healthcare Industry. Business Horizons 2019; 62(4):539-48.

MAJ (Dr) Lim is a Division Medical Officer in HQ Army Medical Services, and the Assistant Chief Medical Informatics Officer (Army) for the SAF Medical Corps. He is currently a Resident in Emergency Medicine.

Text by Linus Tham

Many IT practitioners in Singapore, and indeed across the world, remember the SingHealth data breach in 2018, where the personal information of 1.5 million patients and the prescription information of 160,000 were stolen by unknown attackers. Some believe that the attack was state-sponsored, given the complexity and the duration of it.

As painful as that attack was, especially to the team at Integrated Health Information Systems (IHiS) who were tasked to operate and protect SingHealth's IT systems, I must register gratitude to them and others in the Ministry of Health (MOH) who openly shared valuable cyber intelligence information and inputs that helped IHH ensure that we were not also victims. Even more significant was how our partner doctors accepted the inconvenience when we quickly imposed controls such as internet separation at all IHH facilities in Singapore, while we checked to ensure that there were no copycat attack or collateral damage that IHH was unknowingly suffering.

Threats to cybersecurity

The threat landscape has evolved and the dangers continue to lurk and increase. The spike in cyberattacks just prior to and during the "special military operation" Russia initiated against Ukraine was a stark reminder that the world is not going to get safer, cyber-wise. To counter that, cyber awareness and readiness across the entire sector have been heightened. Investments to ensure data protection have and continue to increase. Laws are being introduced or revised to further enforce data protection.

Yet, there's no turning back from technological innovation. The COVID-19 pandemic accelerated the adoption of various forms of telemedicine across the world. The insatiable demand for healthcare will only increase with ageing populations, mandating the need to find new ways to apply technology in maximising the productivity of the limited healthcare resources worldwide. This demand will draw in more investments to support further innovation. In turn, such wider adoption attracts cybercriminals or even mere cyber pranksters to the healthcare sector, and their actions heighten the risk of major disruptions and potential patient harm in a cyberattack.

How then do we support plans for the Healthier SG project – where each individual is registered to a family GP, who is in turn part of a network of specialists, nurses and allied health professionals from the three public sector clusters paid to look after the Singapore population? Such a capitated model works only when there is a seamless data flow across all the care settings, including when citizens are reminded about their health screenings or follow-up appointments; where AI models are used to identify at-risk individuals and pre-emptively engage them to avoid an expensive hospital admission; and where a mechanism is in place to move data and funding between clusters, should the individual seek care "off cluster" (or "off network", as the US calls it), or when he or she decides to move from one cluster to the other.

Building in security

The only way to support this "care model innovation" is to ensure that security is part of the entire design from the onset. It must meet all the required best practices, standards and regulations (eg, Virtual Private Networks, encryption, two-factor authentication, biometrics, ISO/IEC 27001, HIPAA, PDPA, Computer Misuse Acts)[a, b, c] – yet it must still be "easy to use" for all – *including the 90-year-old* who can no longer see the text on the smartphone screen even if he or she is fortunate enough to be literate. The folks in MOH working on the entire funding concept, the administrators and clinicians in the clusters (and private sector personnel who would join the project teams), the technology teams (IHiS and the many system integration and consulting firms who would invariably be involved) and the security experts from the Cyber Security Agency of Singapore must all work together and focus on the outcome of good population care.

It will require them to step out of their comfort zones (particularly the security experts and auditors in the midst), but they must remember the goal. "The operation was successful but the patient died". To all, it must be the final outcome that matters.

While IHH Singapore, and indeed the rest of IHH, is focused on digital advancement as one of our key growth pillars, we remain steadfast in our aspiration to "Care. For Good." Singapore is one country in the group that has adopted digital technologies early on, Turkey being another. We have come together even more in the past two years to build greater synergies across the entire organisation through deployment of our core IT platform Cerebral Plus across our markets. We are also pushing to engage digitally with our patients and the larger population more, to empower them in their health (and not just healthcare) journey.

This would generate copious amounts of data which we intend to harness to improve our care (through our adoption of the Value Driven Outcomes model as a program worldwide); reduce costs (through improved procurement and equipment use advised by data); and enhance productivity and access (using computerised symptom checkers to help with triage or applying AI to filter diagnostic image reads, freeing specialists to focus on complex cases). We would have to do all these with security and privacy frameworks built-in from the onset, so that we will always be able to retain the trust our patients have vested in us as we continue to pursue our vision to be "The World's Most Trusted Healthcare Services Network". ◆

Notes

a. ISO/IEC 27001 is an international information security standard, jointly published by the International Organisation for Standardisation (ISO) and the International Electrotechnical Commission (IEC).

b. The Health Insurance Portability and Accountability Act (HIPAA) is a US federal statute that, creates a standard of healthcare information between healthcare providers and ensures the privacy of confidential information.

c. The Personal Data Protection Act (PDPA) is a Singaporean act that details the law on data protection, especially that of personal data.

Linus is Group Chief Information Officer of IHH Healthcare, one of the world's largest healthcare networks, and oversees the Group's IT strategy across ten countries. He joined IHH five years ago, bringing with him over 20 years' experience in IT across several industries and healthcare operations, including serving as Group Chief Operating Officer of Singapore's National Healthcare Group.