ACICE
ADMM Cybersecurity and Information Centre of Excellence

UPDATE ON

THE CYBER DOMAIN

Issue 12/24 (December)

Cybersecurity in Healthcare: Protecting Patient Data and Medical Devices

INTRODUCTION

1. The healthcare sector has increasingly digitalised its operations as healthcare institutions seek to leverage information and communications technology (ICT) to raise operational efficiencies which could lead to better treatment outcomes for patients. Additionally, patient records have increasingly been digitalised, facilitating smoother flow of healthcare data that raises operational efficiencies in the entire healthcare sector.

2. Yet, this increased digitalisation has exposed the healthcare sector to cybersecurity threats and vulnerabilities. These cyber risks threaten to undermine the efficient operation of healthcare institutions, potentially adversely affecting patient trust and confidence in the healthcare system when sensitive and personal medical information are compromised. Furthermore, cyberattacks that impair the proper functioning of medical equipment have dangerous consequences on patient welfare, including loss of lives. Consequently, it is prudent for healthcare institutions to put in place cybersecurity contingency and preventative measures so as to minimise the risks of damaging cyberattacks.

OVERVIEW OF CYBERSECURITY CHALLENGES

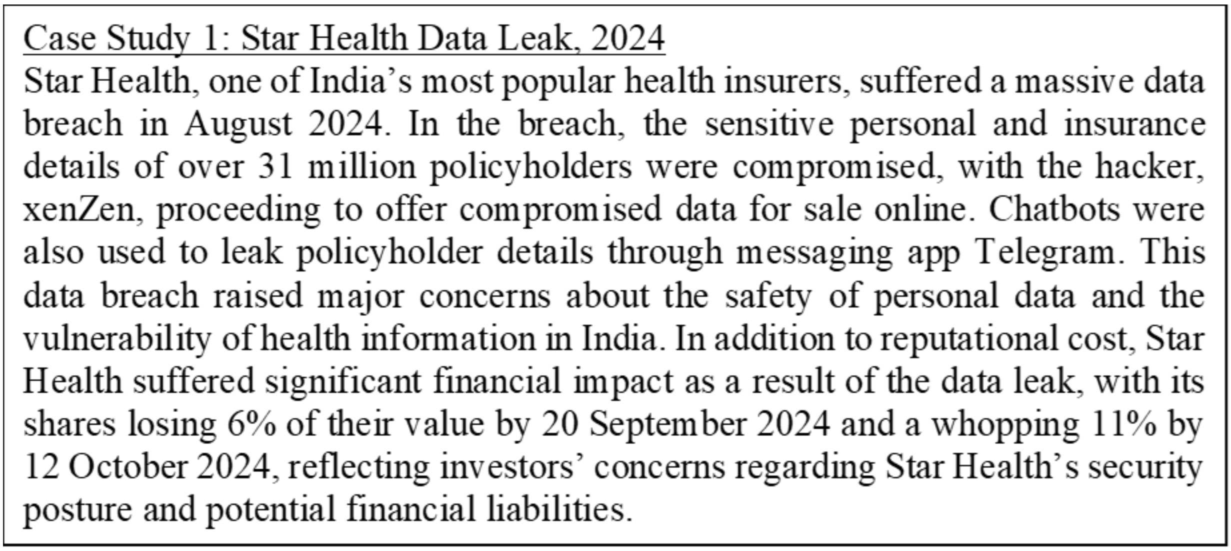
3. The healthcare sector faces a myriad of cybersecurity challenges that can impair their operations. Examples of such challenges include:

a. <u>Ransomware attacks</u>. This refers to cyberattacks where malicious software encrypts files and demands payment to restore access. This has significant consequences to the operations of hospitals and healthcare systems as they rely on continuous access to patient data and medical systems. As such, ransomware can disrupt services, delay treatments and jeopardise patient safety.

b. Data breaches. Healthcare organisations store a plethora of personally identifiable information (PII) of their patients, as well as their medical records, making them prime targets for hackers. A data breach can expose patients' personal, financial and medical information, leading to identity theft and fraud. There are also adverse consequences to patient trust, especially in sensitive areas where patient trust is of utmost importance. For instance, healthcare settings have had to put in place necessary safeguards to ensure anonymity of HIV/AIDS patients given the social stigma surrounding the disease. These safeguards are important to encourage vulnerable groups to come forward for testing, which is crucial in stemming the spread of the HIV virus. A data breach involving a HIV/AIDS patient repository is destructive to the trust established, and may discourage vulnerable groups from coming forward for testing and/or treatment.

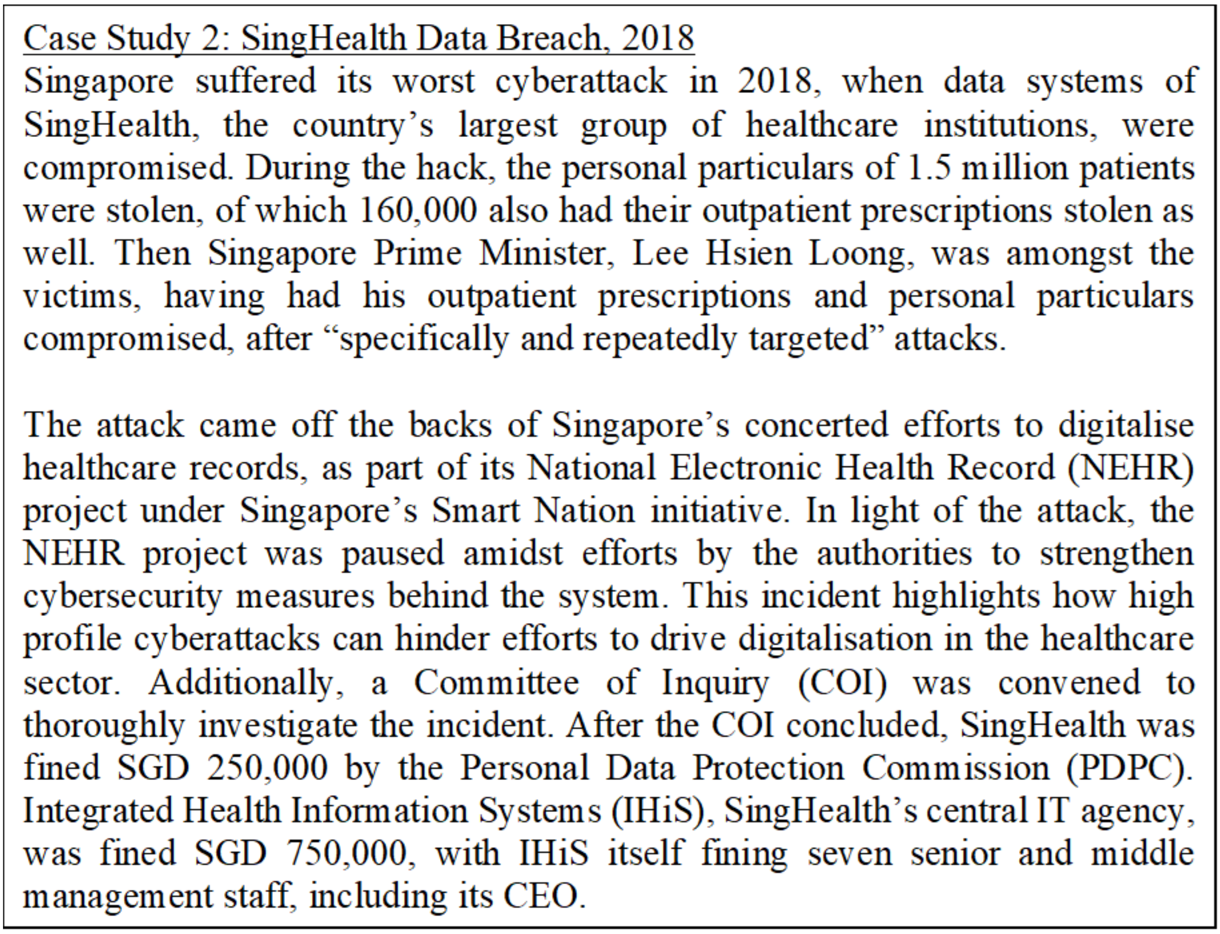
c. Distributed Denial of Service (DDoS) attacks. In such attacks, malicious actors flood healthcare networks with traffic, making systems slow or inoperable. This can severely disrupt healthcare operations, affecting everything from scheduling patient appointments to accessing medical records. There may also be severe consequences in emergency situations leading to patient death, such as if a DDoS attack compromised a hospital's Accident and Emergency (A&E) department, or if a DDoS attack came shortly after a mass casualty incident.

d. Man-in-the-Middle (MitM) attacks. In these attacks, cybercriminals intercept communication between two parties to steal information or alter communications. This can happen during telemedicine sessions, which have grown in popularity ever since the COVID-19 pandemic, or during communication between healthcare providers. As a result, patient privacy is compromised and medical data can be manipulated, damaging patient trust in the healthcare system.



Case Study 1: Star Health Data Leak, 2024

Star Health, one of India's most popular health insurers, suffered a massive data breach in August 2024. In the breach, the sensitive personal and insurance details of over 31 million policyholders were compromised, with the hacker, xenZen, proceeding to offer compromised data for sale online. Chatbots were also used to leak policyholder details through messaging app Telegram. This data breach raised major concerns about the safety of personal data and the vulnerability of health information in India. In addition to reputational cost, Star Health suffered significant financial impact as a result of the data leak, with its shares losing 6% of their value by 20 September 2024 and a whopping 11% by 12 October 2024, reflecting investors' concerns regarding Star Health's security posture and potential financial liabilities.



Case Study 2: SingHealth Data Breach, 2018

Singapore suffered its worst cyberattack in 2018, when data systems of SingHealth, the country's largest group of healthcare institutions, were compromised. During the hack, the personal particulars of 1.5 million patients were stolen, of which 160,000 also had their outpatient prescriptions stolen as well. Then Singapore Prime Minister, Lee Hsien Loong, was amongst the victims, having had his outpatient prescriptions and personal particulars compromised, after "specifically and repeatedly targeted" attacks.

The attack came off the backs of Singapore's concerted efforts to digitalise healthcare records, as part of its National Electronic Health Record (NEHR) project under Singapore's Smart Nation initiative. In light of the attack, the NEHR project was paused amidst efforts by the authorities to strengthen cybersecurity measures behind the system. This incident highlights how high profile cyberattacks can hinder efforts to drive digitalisation in the healthcare sector. Additionally, a Committee of Inquiry (COI) was convened to thoroughly investigate the incident. After the COI concluded, SingHealth was fined SGD 250,000 by the Personal Data Protection Commission (PDPC). Integrated Health Information Systems (IHiS), SingHealth's central IT agency, was fined SGD 750,000, with IHiS itself fining seven senior and middle management staff, including its CEO.

4. Additionally, many medical devices, such as pacemakers, insulin pumps and imaging devices, are now connected to healthcare networks and the internet. This creates potential entry points for attackers. Should the functioning of these medical devices be compromised, the patient's life is endangered and critical treatments can be disrupted. For instance, a cyberattack on backend systems that ensure proper functioning of insulin pumps can result in pumps delivering

inaccurate readings and therefore pumping out too much insulin, leading to hypoglycaemia where patients face a range of symptoms such as heart palpitations, sweating and dizziness. Conversely, insulin pumps, in the face of a cyberattack, can also be in danger of pumping too little insulin, leading to hyperglycaemia, where patients face symptoms such as dehydration, fatigue and blurred vision.

STRATEGIES TO SECURE HEALTHCARE INSTITUTIONS FROM CYBERATTACKS

5. Given that healthcare institutions take care of a large number of patients, there will be damaging consequences and disastrous fallouts should a cyberattack occur. Hence, it is of utmost importance that healthcare institutions take measures to protect themselves from cyberattacks. Listed below are some recommendations:

6. <u>Encrypt Patient Data</u>. Healthcare institutions should encrypt all patient data as this protects data by converting data into an unreadable coded format. The data can only be read with a decryption key. As such, even if patient data is compromised, intercepted, accessed or stolen by unauthorised parties, it remains secure and unusable to the malicious actors behind the attack. Additionally, it is important to ensure that there is secure backend key management, where only authorised parties have access to decryption keys and can decrypt data, so as to maintain data integrity. Beyond data, it is important for healthcare institutions to encrypt devices too, such as laptops and USB drives so that data leakage is prevented, even if these devices are lost or stolen.

7. <u>Implement Access Control and Authentication Mechanisms</u>. This will restrict access of patient data to authorised individuals who need the data and minimise the probability of a data leak. There are many ways to implement such strong access controls. Examples include role-based access control (RBAC), where access to patient data is restricted based on job roles, ensuring only authorised personnel can access sensitive information; multi-factor authentication (MFA), where additional authentication steps are required, such as a code sent to a mobile device, therefore preventing unauthorised access; and unique user IDs and passwords, where each employee is assigned a unique ID and employees are required to use strong passwords so as to prevent unauthorised access.

8. Data Integrity and Audit Trails. Audits play an important role in ensuring data integrity as they help in the prevention and response of cyber breaches. They encourage healthcare institutions to maintain a proactive and comprehensive approach to safeguarding sensitive data and systems, by identifying data vulnerabilities and weaknesses, and ensuring that healthcare institutions comply with relevant regulatory requirements. It is thus prudent for healthcare institutions to conduct regular internal and external audits of their data security practices. Furthermore, they should conduct vulnerability scanning and penetration testing, as these techniques stimulate attacks and can identify weaknesses in data systems before a breach occurs.

9. Regular software updates and patching. These updates are critical in ensuring that software in medical devices remain up to date and that any vulnerabilities that might expose medical devices to data breaches are addressed. As such, it is important to enable automatic updates for medical device software, so that the latest security patches can be downloaded. It is also important to have a process for regularly reviewing and applying patches to address known vulnerabilities in medical device firmware and operating systems.

10. Isolation of Critical Medical Devices. It may also be necessary to isolate critical medical devices by placing them on a separate network segment, so as to prevent unauthorised access from other parts of the network that can compromise the essential functioning of these medical devices. This can be done by using firewalls and intrusion detection systems (IDS) between medical device networks and other systems to monitor traffic and detect unusual activity. Medical device manufacturers can also consider limiting their devices' internet exposure, by avoiding connecting devices to the internet unless absolutely necessary, and configuring firewalls that can block unauthorised inbound and outbound traffic.

11. Security Awareness Training. Healthcare institutions should conduct security awareness training to educate staff on best practices for handling medical devices, such as recognising phishing attempts, avoiding unauthorised software installations and following password security protocols. Staff should also be aware of response procedures, including reporting protocols and isolation procedures, so that they know what to do if they suspect a device has been compromised.

12. Real-time Monitoring. Healthcare networks can conduct real-time monitoring of medical devices under their purview, as the continuous monitoring of device activity can detect unusual behaviour that could indicate a security threat. It is important to maintain audit logs of device access and use so as to track who has interacted with a device. This in turn is useful for detecting insider threats and for investigating incidents.

13. Risk Assessment and Management Strategies. Risk assessment and management strategies are essential in controlling and preventing data breaches. They help healthcare institutions prioritise risks and establish measures that can mitigate potential threats. Risks can be categorised based on factors like severity, probability and potential impact on data security. Hence, vulnerabilities that pose high risks to sensitive patient data can be prioritised. By focusing on high-risk areas, healthcare institutions can allocate their resources more effectively, ensuring that critical systems and sensitive data are prioritised in their security strategies.

14. Incident response and recovery planning. Cyberattack incident response and recovery plans are critical components of cybersecurity that help healthcare institutions prepare for, manage, and recover from cyberattacks. These plans are essential in minimising damage, ensuring business continuity and maintaining trust with patients. With an incident response plan, healthcare institutions can minimise the impact of cyberattacks, such as through quick containment where healthcare institutions follow established protocol that can contain a cyberattack as soon as it is detected. Additionally, the incident response procedure should include steps to protect and recover compromised data, thereby limiting potential data loss and safeguarding sensitive information. Furthermore, recovery planning helps healthcare institutions quickly restore their essential systems and services, thus minimising downtime and associated costs in the face of an attack.

CONCLUSION

15. In conclusion, the increased digitalisation of the healthcare sector has made healthcare institutions and medical devices more vulnerable to cyberattacks by malicious actors. The impact of cyberattacks on healthcare institutions and medical devices are in turn wide-ranging and highly damaging.

16. Healthcare institutions should therefore implement robust measures that protect patient data and secure medical devices against cyberattacks. It is also important to implement cybersecurity strategies to deal with these threats.

Contact Details

All reports can be retrieved from our website at www.acice-asean.org/resource/.

For any queries and/or clarifications, please contact ACICE, at ACICE@defence.gov.sg.

Prepared by:
ADMM Cybersecurity and Information Centre of Excellence

• • • • •

REFERENCES

1. High blood sugar (hyperglycaemia) – NHS
https://www.nhs.uk/conditions/high-blood-sugar-hyperglycaemia/

2. Low blood sugar (hypoglycaemia) – NHS
https://www.nhs.uk/conditions/low-blood-sugar-hypoglycaemia/

3. Star Health insurance hack led to personal data of 31 million customers being compromised: Story in 5 points – India Today
https://www.indiatoday.in/technology/features/story/star-health-insurance-hack-led-to-personal-data-of-31-million-customers-being-compromised-story-in-5-points-2615354-2024-10-11

4. India's Star Health probes alleged role of security chief in data leak – Reuters
https://www.reuters.com/technology/cybersecurity/indias-star-health-probes-alleged-role-security-chief-data-leak-2024-10-10/

5. Insulin Pumps – Diabetes U.K.
https://www.diabetes.org.uk/about-diabetes/looking-after-diabetes/treatments/insulin/insulin-pumps

6. Star Health takes Telegram and hacker to court over massive data leak – Insurance Business
https://www.insurancebusinessmag.com/asia/news/cyber/star-health-takes-telegram-and-hacker-to-court-over-massive-data-leak-507778.aspx

7. India's Star Health says it received $68,000 ransom demand after data leak – Reuters
https://www.reuters.com/world/india/indias-star-health-says-it-received-68k-ransom-demand-after-data-leak-2024-10-12/

8. Personal info of 1.5m SingHealth patients, including PM Lee, stolen in Singapore's worst cyber attack – Straits Times
https://www.straitstimes.com/singapore/personal-info-of-15m-singhealth-patients-including-pm-lee-stolen-in-singapores-most

9. Doctors raise concerns again over national e-records system after data breach at SingHealth – Today
https://www.todayonline.com/singapore/doctors-raise-concerns-again-over-national-e-records-system-after-data-breach-singhealth

10. Prevention Is No Cure: A Case Study of the 2018 SingHealth Breach – Konrad-Adenauer Stiftung
https://www.kas.de/documents/288143/14393910/4.1+Prevention+is+No+Cure.pdf/