BioSpectrum
the business of Bio & Health Sciences
ASIA EDITION

Cybersecurity: The Next Frontier for Protecting Patient Safety

May 18, 2023 | Opinion

By Vijay Vaidyanathan, Regional Vice-President, Solutions Engineering - Asia Pacific & Japan at Claroty



A successful cyber attack can have severe consequences in healthcare, ranging from financial loss due to data breaches to medical identity theft, and even physical harm to patients if their medical records are altered or inaccessible. While there were known and growing risks in our increasingly hyper-connected healthcare before 2020, the one-two punch of the ransomware revolution and the COVID-19 pandemic have many healthcare delivery organizations (HDOs) on the ropes and taking a beating.

The Singaporean Ministry of Health has highlighted reasons why cyber-attacks on the healthcare sector have such a high impact.

Firstly, ensuring the confidentiality and integrity of a patient's health records is paramount. Personal health information is reportedly 50 times more valuable on the black market than financial information. Additionally, while financial information such as credit card numbers can be changed, personal health information typically remains with an individual throughout their lifetime.

Perhaps even more crucially, cyber-attacks can disable healthcare and administrative services, which can disrupt healthcare institutions' ability to provide timely and appropriate patient care

Singaporeans have been victims of cyberattacks in the past. The most notable incident was the 2018 SingHealth data breach, where personal information of 1.5 million SingHealth patients and records of outpatient dispensed medicines for 160,000 patients were stolen, and Prime Minister Lee Hsien Loong's information was specifically targeted. In 2021, a ransomware attack on a private clinic resulted in the exposure of personal data and clinical information of over 73,000 patients, including their names, addresses, identity card numbers, contact details, and clinical information.

Where We Go From Here

In 2019 ransomware attack on a hospital in Germany, resulted in the death of a patient. The attack caused the hospital's systems to be offline, including its IT infrastructure, forcing staff to revert to paper-based systems. This, in turn, delayed treatment for the patient, who was in critical condition and needed to be transferred to another hospital. Unfortunately, the patient died before they could be transferred.

This unfortunate case clearly demonstrates that cybersecurity is ultimately about patient safety. Current policies and regulations around healthcare cybersecurity are being tested to the limit. Investment in cybersecurity solutions is rising, and the global healthcare cybersecurity market is projected to reach $61,832 million by 2031, driven by “the emergence of digital technologies in healthcare sector, the rising incidences and complexity of cyberattacks, (and) the growing concern on data privacy and safety”.

It is against this background that the Cyber Security Agency of Singapore (CSA) has emphasized the need for critical information infrastructures (CIIs) to enhance the cybersecurity of OT systems. Organizations in the region must continuously transform to keep up with the changing threat landscape and go beyond generic cybersecurity practices.

The Australian government has also announced plans to overhaul its cybersecurity rules and establish an agency to oversee government investment in the field and help coordinate responses to hacker attacks.

Meanwhile, The Australian government recently said it planned to overhaul its cybersecurity rules and set up an agency to oversee government investment in the field and help coordinate responses to hacker attacks, after recent attacks this and last year that included health insurer Medibank Private Ltd.

Closer to home, Singapore's Private Hospitals and Medical Clinics Regulations state that licensees must implement adequate safeguards to protect medical records. Additionally, the Ministry of Health’s Healthcare Cybersecurity Essentials (HCSE) sets out 12 recommendations to help healthcare providers improve the security of their systems and data.

However, the onus is still on healthcare providers to take responsibility for implementing necessary measures to protect patient safety. Today's practices were built for earlier times, and few healthcare players want additional regulations and requirements. But it is not about what they want; it is about what patients need, a more defensible, maintainable, and timely access to care.

There is a window of opportunity to reposition the industry towards more trustworthy, transparent, and resilient healthcare delivery. It is critical to prioritize cybersecurity in healthcare to ensure patient safety and maintain the quality of care in the face of evolving cyber threats.

***Authour*: Vijay Vaidyanathan, Regional Vice-President, Solutions Engineering - Asia Pacific & Japan at Claroty**