Healthcare data has outgrown the value of credit card or social security numbers

Health data is wealth: Why hackers targetted Singapore

Singapore's high-profile data breach shows that hospitals need to step up their game in order to ward off potential attackers.

When database administrators detected unusual activity on SingHealth's IT systems in early July, little did they know that the episode would spiral into the most serious breach of personal data in Singapore's history. Soon enough, the country watched in growing horror as reports revealed that the records of 1.5 million SingHealth patients had been compromised, including those of Prime Minister Lee Hsien Loong and other government officials.

Forensic investigations later revealed that the hack had started eight days before the cyberattack was even reported. The data taken included the names, NRIC numbers, addresses, gender, race, and dates of birth of the patients. Information on the outpatient dispensed medicines of about 160,000 of these patients was also illegally accessed. The Cyber Security Agency of Singapore (CSA) and the Integrated Health Information System (IHiS) later confirmed that the breach was a deliberate, targeted, and well-planned cyberattack and was not the work of casual hackers or criminal gangs.

Medical information is expensive—it had a street value of around $50 as of 2015, compared to a measly $1 for credit cards and social security numbers.

Profitable healthcare data

For Singapore, one of the world's most connected and technologically sophisticated nations, the breach was a painful reminder that healthcare data has grown its value that hackers are now willing to go the extra mile to obtain it. "Healthcare data has outgrown the value of credit card or social security numbers," said **Olli Jarva**, managing consultant of software integrity group Synopsys.

Data from the World Privacy Forum revealed that cases of medical identity theft has ballooned globally in recent years. This is because medical information is expensive—it had a street value of around $50 as of 2015, compared to a measly $1 for credit cards and social security numbers. The average profit per medical record is a staggering $20,000, compared to just $2,000 for regular identity theft.

Sid Deshpande, research director at Gartner, warned that the most immediate threats which victims will face are that of identity fraud, financial fraud, and tax fraud. "Data contained in healthcare records is more permanent than credit card information, for example, so citizens need to be alert to scams resulting from social engineering efforts," he said. "This type of information likely fetches higher payouts on the dark web. It could also be sponsored by nation states that have interests inimical to Singapore's," he added.

He noted that the breach likely started when a front-end workstation was compromised, followed by privileged access credentials being used to access a database. "Attackers are usually after administrator credentials because these often enable direct access to sensitive data," Desphande noted.

Kenny Liew, telecommunications analyst at Fitch Solutions, further warned that the relatively lower number of servers could heighten cybersecurity risks. "We believe that Singapore could look at increasing secure server capacity to cope with the growing amount of data being collected and stored. This is especially as the volume of data in Singapore only grows by the day as the city state steps up the implementation of the government's digital economy blueprint and is seeking to establish itself as a leading fintech hub," Liew said.

Liew added that healthcare is not the only sector at risk from cyber attacks. Insurance companies, financial services, ride-hailing, and bike-sharing easily come to mind, but almost every single industry which collects data are suspect. "The state-built digital repository platform MyInfo, which allows Singaporeans to automatically key in information for e-forms also remains a key prey for malicious cyber identities," he added.

Are hospitals ready?

Over in the Farrer Park General Hospital, technology is such a crucial part of patient experience that even the meals that patients can order is linked to their digital medical records, so that any restrictions can be immediately applied. These services utilise a large volume of data, and the hospital uses artificial intelligence to protect this valuable information.

"We have been able to identify users surfing the dark web, as well as misuse of internet bandwidth. Our AI tools have a 90% detection rate of any malware or abnormal behaviour within its systems," said **James Woo**, chief information officer of Farrer Park Company.

"Based on my experience, there have been increasing zero-day attacks over the years, and I am not comfortable with that. Hackers change their attacking pattern nowadays, and detection and behaviour learning are more important to prevent an attack even before it happens," he noted.

Woo warned that attacks of the future will become more dynamic and is not going to be as structured as they are at present. "I believe that using artificial intelligence and machine learning allows us to tackle the dynamics of these changing trends. I also believe that attackers will eventually use AI to attack an organisation as well, so why not use AI to fight back and stay ahead of the curve?" he asked.

Singapore's cybersecurity frameworks are amongst the world's strongest, but healthcare organisations face a unique challenge when it comes to warding off cyberattacks. Jarva noted that from a security standpoint, the healthcare industry shares the same shortcomings as other enterprises, but with some added obstacles. Aside from the lack of resources, the industry also has to deal with an "extremely heterogeneous environment."

"Whilst healthcare organisations may standardise on laptops and IT servers, providers also manage multiple devices that are attached to the network. These can include drug infusion pumps, imaging devices like MRI and CT scanners, and treatment software, such as those used to manage implantable pacemakers," Woo said.

For instance, large computer systems are typically part of a bigger project developed and delivered by third-party system integrators, where the supply chains can get complicated. This compounds the challenge to manage security, as different parts of the system may have different third-party software components and inherent vulnerabilities, and often, may not be properly identified and patched early enough.

"This isn't a challenge that is unique to healthcare, it is a challenge that every large organisation goes through," Jarva added.

Moving forward

Although the government was lauded quickly for its swift action to contain the fallout after temporarily imposing internet surfing separation in SingHealth's IT systems and resetting user and system accounts, damaging security concerns have already started to weigh in on business sectors that handle a wealth of customer information on a daily basis.

Olli Jarva

Sid Deshpande

Kenny Liew

Tan Shong Ye

To address other vulnerabilities, the government could also look into separating parts of the IT infrastructure that are not heavily reliant on the internet to operate so that sensitive information could benefit from another layer of protection against attacks, noted **Joanne Wong,** senior regional director for Asia Pacific & Japan at LogRhythm.

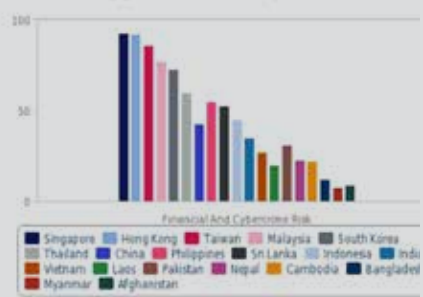
"Whilst this is not a be-all and end-all solution, it makes remote access into the network much harder for external parties and thus creates a defensive shield for these systems," she noted.

Deploying secured information gateways that scrutinise voluminous data passing through networks could also prevent restricted information from leaking out, whilst at the same time block unwanted data from passing through.

"Banks in Singapore and around the region frequently use secured information gateways as one of many deterrence measures," Wong added. "This is generally a good practice and add an additional layer of security without compromising on the benefits of the internet."

PwC Singapore digital trust leader **Tan Shong Ye** noted how an organisation's future investments can focus on strategy, process, technology, people, and culture. "With the increase in emphasis on digital and information comes the need for cyber risk assessments to keep personal data, client data, and intellectual property safe," he said.

Security apparatus most robust in Singapore



Sources BMI Research