Publication: The Business Times, p 01_02
Date: 29 January 2019
Headline: 2nd major breach may further dent Singapore's data hub push

2nd major breach may further dent

By Claudia Chong
chongkmc@sph.com.sg
@ClaudiaChongBT

Singapore

A SECOND high-profile data breach in the healthcare sector may put a dent in Singapore's positioning as a data hub, say some experts.

More than 14,200 people with HIV (human immunodeficiency virus) had their confidential information, including their contact details and medical information, stolen and leaked online by an American fraudster, the Ministry of Health (MOH) revealed on Monday.

The records leaked include those of 5,400 Singaporeans diagnosed with HIV up to January 2013, and 8,800 foreigners diagnosed up to December 2011, MOH said at a press conference.

This included each person's name, identification number, phone number and address, HIV test results and related medical information. The name, identification number, phone number and address of 2,400 people identified through contact tracing up to May 2007 was also included, reported *The Straits Times*.

The man behind the leak, Mikhy Farrera-Brochez, had gotten hold of information illegally from the HIV registry that his partner had access to. His partner was Ler Teck Siang, a Singaporean doctor who was head of MOH's National Public Health Unit (NPHU) from March 2012 to May 2013. He was charged in 2016 under the Official Secrets Act for failing to take reasonable care of confidential information regarding HIV-positive patients.

A lawyer who declined to be named was surprised that MOH was making public the breach only now.

He also noted that the data protection obligations of the Personal Data Protection Act do not apply to public agencies – ie they may not be penalised for breaches for which private entities would be punished.

The information in the latest breach is still in the hands of Farrera-Brochez, who was deported after he had served his jail term for another offence. He currently remains outside Singapore.

"Although both this incident and the recent cyber attack at SingHealth database concern data privacy in Singapore, they are very different in the way in which private data is leaked. This incident is a classical insider attack in which private data is

Publication: The Business Times, p 01_02
Date: 29 January 2019
Headline: 2nd major breach may further dent Singapore's data hub push

Singapore's data hub push

mishandled by an insider who is authorised to access the data, assuming that the sharing of data with Farrera-Brochez was intentional," said Prof Gao Debin from Singapore Management University's School of Information Systems.

Last year, Singapore experienced its worst cyber attack when, from June 27 to July 4, hackers infiltrated the computers of SingHealth and stole the personal particulars of 1.5 million patients, including Prime Minister Lee Hsien Loong.

Although these high-profile data breaches have been confined to the healthcare sector, they could very well have some spillover impact on public confidence in data security for other sectors too, the lawyer said.

"In Singapore, people look toward the government to set the standard and take the lead," he said.

Singapore has been in the spotlight as more companies eye the city as a location for data storage and cloud leasing. Last year, Facebook and Google announced investments into new data centres here.

But cybersecurity needs to grow in tandem with this burgeoning sector.

"Singapore excels in digital infrastructure, in stable policies and regulation, and in digital talent. But cybersecurity requires an additional leap in terms of innovation, which only a few countries such as Switzerland, China, the USA are ready to make today. Singapore has focused on other aspects of technology, such as artificial intelligence and fintech," said Arturo Bris, professor of finance at IMD Business School.

Continued on Page 2

2nd big breach could hurt Singapore's data hub push

Continued from Page 1

If the two incidents have taught us anything, it is that information governance is key – and this has to include taking a hard look at how people behave and react in everyday situations, said Prof Lawrence Loh, director of the Centre for Governance, Institutions & Organisations at the National University of Singapore.

Unfortunately, organisations across all sectors do not put enough focus on training their staff in cyber awareness, he added. "They think there is a trade-off. If you are too strict, you might hamper operational efficiency."

Tech firm Acronis' director of information security and compliance Oleg Ishanov said that in cases like this, each piece of personal data record should be individually encrypted, and ideally, access to this record should be approved by the data owner – for example, using their smartphone – or the system should provide access to the record only when there's a clear need, like only during the time of appointment between doctor and the patient.

While the incident might spark some scepticism over the security of the Singapore health system, it brings more attention and pressure on what exactly MOH is doing to prevent such cases in the future, all to help Singapore become a data and cybersecurity hub faster, said Mr Ishanov.

For instance, since 2016, additional safeguards against mishandling of information by authorised staff have been put in place, including a two-person approval process to download and decrypt information.

"The more organisations will be transparent and open about how information is protected – by publishing their detailed security practices – the more trust they will build among people of Singapore," said Mr Ishanov.