**Publication: The Straits Times, pg A06**
**Date: 16 July 2019**
**Headline: Review panel identifies poor data-access practices**

The Public Sector Data Security Review Committee is also carrying out in-depth inspections of the IT systems of key government agencies, including the Central Provident Fund Board.
ST FILE PHOTO

# Review panel identifies poor data-access practices

## It also flags insufficient 3rd-party data-handling policies and varying levels of data-safety training

**Hariz Baharudin**

Public sector agencies have insufficient policies governing third parties handling data and inconsistent practices in managing data access, a high-level committee currently reviewing and strengthening data security practices across the entire public service has found.

The Public Sector Data Security Review Committee, which was convened by Prime Minister Lee Hsien Loong and is chaired by Senior Minister Teo Chee Hean, conducted a six-week-long governmentwide stock-take of data management practices after it was formed in April.

The committee, which includes four ministers and experts from the private sector, has until Nov 30 to submit its findings and recommendations to PM Lee.

In a briefing yesterday, the Smart Nation and Digital Government Office (SNDGO) said the committee also found varying levels of training in data protection in the public sector, and that many data incidents were the result of human error, where well-meaning staff had inadvertently compromised data.

An analysis of emerging trends by the committee also found that the increasing prevalence of data sharing and the growing availability of complex analytics tools heighten the chances of a data breach.

The SNDGO said in a statement: "There is a need to strengthen our data security regime for the future. This is in view of the increasing complexity of our systems, the greater demand for the use of data to provide convenient digital services to the public and the need to use data for better policymaking."

Besides the stock-take, SNDGO said the committee is also carrying out in-depth inspections of key government agencies' IT systems. It is doing this in waves, beginning with organisations in the finance and healthcare sectors.

These agencies are: the Inland Revenue Authority of Singapore, the Central Provident Fund Board, the Ministry of Health, the Health Promotion Board and the Health Sciences Authority.

The non-government members on the committee were chosen for their experience and expertise in technology and data security in their respective fields.

The committee is also supported by an expert group consisting of seven international experts and industry professionals. In addition, it is supported by an inter-agency task force formed by public officers across the Government.

The committee was announced following a spate of cyber and data security breaches and incidents over the past year.

The latest data breach involved the personal information of more than 800,000 blood donors which was improperly put online for more than two months.

Singapore's worst cyber attack was in June last year, when hackers got into the database of public healthcare cluster SingHealth and stole the personal data of 1.5 million patients and the outpatient prescription information of 160,000 people, including PM Lee.

harizbah@sph.com.sg

BEEFING UP SYSTEM CRUCIAL

**There is a need to strengthen our data security regime for the future. This is in view of the increasing complexity of our systems, the greater demand for the use of data to provide convenient digital services to the public and the need to use data for better policymaking.**

**SMART NATION AND DIGITAL GOVERNMENT OFFICE STATEMENT**

## Safeguarding personal data

13 new security measures will be rolled out across the entire public service to better protect citizens' personal data following a series of high-profile breaches over the past year. Here are some of them, according to the stage of a data lifecycle.

### STORAGE

**Tokenisation**
Reducing the risk of data being misused by replacing its identifiers with a different value known only to the agency.
**Would have minimised the impact of the SingHealth and HIV database leaks.**

**Masking**
Hiding the true value of the data by masking out portions of value, so that even if a hacker gets hold of the data, he cannot understand it.

**Partitioning**
Breaking a dataset into small sets by segmenting out sensitive entities to reduce the likelihood of highly sensitive data being compromised.

### DISTRIBUTION

**Password protection**
Strengthening password and encryption requirements across more types of data files, to prevent unauthorised distribution.

**Digital watermarking**
Add marking information to identify the originator of the dataset, which allows leaks to be traced to the source and aid investigation.

**Data loss protection tools**
Signal when unusual activities involving data happen, like large amounts of data being downloaded to an officer's laptop.
**Could have detected and stopped the unauthorised extraction of SingHealth patients' and HIV Registry data.**

### USAGE

**Volume-limited and time-limited data access**
Restricting data access to a set duration and volume, so that the impact and likelihood of a breach is limited.
**Could have stopped unauthorised access to SingHealth patients' data using dormant user accounts.**

**Automatic identity and access management (IAM) tools**
Having tools that automatically manage officers' identity and access rights, ensuring that only those authorised can get to the data.
**Dormant user accounts would have been deactivated to prevent abuse.**

Sources: PUBLIC SECTOR DATA SECURITY REVIEW COMMITTEE, SMART NATION AND DIGITAL GOVERNMENT OFFICE
STRAITS TIMES GRAPHICS

# Measures will limit scope of damage done by data breaches: Experts

The 13 technical measures recommended by the Public Sector Data Security Review Committee would have lessened the potential damage of recent data breaches, said experts.

Yesterday, a committee tasked with improving data management in the public sector unveiled the measures to better protect citizens' sensitive personal information, developed after a government-wide stock-take of practices and in-depth inspections of government agencies.

The Smart Nation and Digital Government Office said one of the measures recommended by the Public Sector Data Security Review Committee is to have in place tokenisation or encryption, the act of replacing identifiers in data sets with something that only the relevant agency would know.

Such encryption would limit the scope of damage that can be done by hackers who access and steal data, experts told The Straits Times.

For instance, a breach reported by a Health Sciences Authority vendor in March involving the personal information of more than 800,000 blood donors could have been very damaging. In the wrong hands, personal data could be used to commit identity fraud, blackmail or to impersonate the people affected.

Encryption adds levels of security to data so that even if stolen, hackers would not be able to use the information, said Mr Tony Jarvis, chief technology officer of Check Point Software Technologies.

Mr Grant Geyer, senior vice-president for products at cyber-security firm RSA, added: "If sensitive data is encrypted, even if you steal it, it will not have a value if you are unable to understand it."

Experts also said that limiting the volume and time of data access, and enhanced logging and active monitoring of data access, would help curtail the volume of data that can be improperly accessed.

Mr Bryan Tan, a lawyer with Pinsent Masons MPillay who specialises in technology law and data protection, said this could have curbed the amount of information gained by American Mikhy Farrera-Brochez who, in 2016, leaked online the confidential information of 14,200 people diagnosed with HIV.

He said the announcement of the measures was a "trust-building exercise", and represents a shift in how the Government is communicating its workings to the public.

"Before this, the Government has seldom revealed what kind of internal measures it has. But given the circumstances, they are seeing that there is a need to be more open about how it protects citizens' data now."

In announcing the concrete steps being taken, the Government is trying to instil confidence in its ability to handle data, said Singapore Management University law don Eugene Tan.

Professor Tan said: "It would be imperative to boost public confidence in the way the public sector protects data, particularly because they possess and collect a lot of sensitive data. Coming after about three months after being formed, it shows that the committee is eager to get its work done, but it does beg the question why these measures weren't implemented earlier."

**Hariz Baharudin**