Steps to better protect, secure Singaporeans' data

The Public Sector Data Security Review Committee has made recommendations in five key areas for adoption by entities that handle public sector data.

Protecting data
and preventing it from being compromised

- Entities to collect data only when necessary and limit their retention period.
- Minimise devices which hold data by letting files be accessed only on secured platforms. Use data only for tasks that require the data, and give selective access.
- Enhance how data use is monitored through digital watermarking and checking how data moves through the network.
- Detect suspicious activity, through e-mail and data loss protection tools.
- Protect stored data by making it unusable and unreadable even if stolen.
- Protect the data when it is being distributed.

Detecting and responding
to data incidents

- Establish a central contact point for the public to report government data incidents.
- Set up the Government Data Office to monitor and analyse security incidents.
- Have a standard process for post-incident inquiry for data incidents and share takeaways across all agencies.
- Install a framework for all public agencies to notify individuals affected by data incidents promptly.
- Designate the Government IT Management Committee as the central body to respond to large-scale incidents that involve multi-agencies.

Raising competencies
and improving the culture of data security

- Install organisational KPIs for data security.
- Hold top leadership of all public sector organisations accountable for installing strong organisational data security practices.
- Ensure accountability for third-party handling of government data by amending the Personal Data Protection Act to cover government vendors and non-public officers who mishandle personal data.
- Publish government policies and standards relating to data protection and update this annually.

Accountability
for data protection

- Specify roles for groups of officers involved in management of data security.
- Ensure all public officers are regularly updated on data security considerations through an annual training programme.
- Inculcate a culture of excellence around sharing and using data, and cultivate an environment conducive to open reporting of data incidents.

Sustainability

- Appoint the Digital Government Executive Committee to oversee public data security.
- Set up the Government Data Security unit to drive data security efforts in the public sector.
- Deepen the Government's expertise in data protection technologies.

Source: PUBLIC SECTOR DATA SECURITY REVIEW COMMITTEE PHOTO: ISTOCKPHOTO STRAITS TIMES GRAPHICS