| | |
|---|---|
| Parliament No: | 13 |
| Session No: | 2 |
| Volume No: | 94 |
| Sitting No: | 115 |
| Sitting Date: | 6-1-2020 |
| Section Name: | Written Answers to Questions for Oral Answer Not Answered by End of Question Time |
| Title: | Impact of and Preventive Measures Following Incidents of Personal Data Lost to Hackers |
| MPs Speaking: | [Mr Chong Kee Hiong, Mr S Iswaran] |

# IMPACT OF AND PREVENTIVE MEASURES FOLLOWING INCIDENTS OF PERSONAL DATA LOST TO HACKERS

45 Mr Chong Kee Hiong asked the Minister for Communications and Information regarding incidents of personal data lost to hackers due to data privacy law breaches (a) what is the number of incidents in the public and private sectors respectively in each of the last three years; (b) what is the number of persons affected annually; and (c) whether the Ministry will consider implementing a registration and licensing scheme for software services providers, similar to the requirements imposed on accounting and legal firms, financial institutions and medical services providers.

Mr S Iswaran: The Personal Data Protection Commission ("PDPC") investigated five cases in 2017, 13 cases in 2018 and 16 cases in 2019, involving private sector organisations due to hacking. In the public sector, four cases of data breaches due to hacking were reported in 2017 and three cases in 2018. No case was reported in 2019. These numbers include cases where malware was planted, and databases were held ransom or data was exfiltrated.

Of these reported cases, in some instances completed investigations have demonstrated that personal data was exfiltrated due to hacking and breach of the PDPA. These affected 48,000 individuals in 2017 and 1.5 million individuals in 2018. The number for 2018 comprises primarily the data breach involving Singapore Health Services Pte Ltd and its data intermediary, Integrated Health Information Systems Pte Ltd. For similar cases involving the public sector, 35,000 individuals were affected in 2017, and 900 individuals were affected in 2018.

Under the Personal Data Protection Act (PDPA), organisations are required to put in place security measures to safeguard the personal data in their possession or control. Data security requirements are also imposed on public agencies through the Public Sector (Governance) Act and the Government's Instruction Manual on ICT.

Both private and public sector organisations have to fulfil their respective obligations regardless of whether they decide to outsource any functions to software services providers. If they do so, they should carry out due diligence to assess the capability, track record and suitability of software services providers.

The PDPA requires each private sector organisation to appoint a Data Protection Officer (DPO) to ensure that the organisation complies with the PDPA. To better safeguard themselves against data breaches, organisations should firstly ensure that their DPOs are trained to develop and implement policies and practices for the organisations to meet their obligations under the PDPA. Secondly, they should register their DPOs with PDPC to keep abreast of relevant personal data protection developments. Thirdly, organisations can also apply for IMDA's Data Protection Trustmark, to verify that they conform to personal data protection standards and best practices.

---