Parliament No:	14
Session No:	1
Volume No:	95
Sitting No:	60
Sitting Date:	4-4-2022
Section Name:	Written Answers to Questions
Title:	Reasons for Recent Data Breach of Local Retail Website and Measures to Ensure Security and Protection of Customer Data
MPs Speaking:	Ms Joan Pereira,Mrs Josephine Teo

REASONS FOR RECENT DATA BREACH OF LOCAL RETAIL WEBSITE AND MEASURES TO ENSURE SECURITY AND PROTECTION OF CUSTOMER DATA

39 Ms Joan Pereira asked the Minister for Communications and Information with regard to the recent data breach of a local retail website (a) what are the reasons for such incidents to occur despite previous repeated warnings by the authorities of such breaches; and (b) what are the measures which the Ministry will consider implementing to ensure that organisations secure their databases and protect their customers' information.

Mrs Josephine Teo: Over the last three years, the Personal Data Protection Commission (PDPC) investigated over 70 data breaches involving retail businesses.

Under the Personal Data Protection Act (PDPA), organisations have an obligation to protect their customers' personal data to prevent unauthorised access, collection, use or disclosure. Based on the cases that were brought to the PDPC's attention, the root cause of data breaches is often the lack of basic data protection practices and cybersecurity measures. Some examples include:

(a) Human errors, such as sending emails to the wrong recipient addresses or attaching the wrong documents; and

(b) Cyber incidents and IT-related errors, such as (i) coding issues, (ii) configuration issues, such as the improper configuration of third-party systems, (iii) malware and phishing related incidents, (iv) inadequate security practices, and (v) weakly secured accounts and passwords.

To help organisations strengthen their cybersecurity posture, the Cyber Security Agency (CSA) has developed various resources, such as cybersecurity toolkits, to guide enterprise leaders and their employees strengthen their cyber defences and prevent data breaches. In addition, enterprises can also

apply for the recently launched Cyber Trust and Cyber Essentials mark and be certified for sound cybersecurity practices.

The PDPC also makes various data protection resources available. Last year, the PDPC published the "Guide to Data Protection Practices for ICT Systems", which recommended solutions to prevent common issues that cause data breaches. To help Small and Medium Enterprises (SMEs) recover quickly and ensure compromised data is protected even after a breach, PDPC and the Infocomm Media Development Authority launched the Data Protection Essentials programme (DPE) on 1 April 2022 so that they can acquire baseline data protection and security practices. The DPE offers (a) enhanced security solutions that include backup and encryption, in addition to anti-virus and firewall; and (b) a one-stop professional service where SMEs can tap on a curated panel of providers to put in place baseline data protection and security standards.

In addition to the measures above, organisations are also encouraged to provide proper training and resources to their Data Protection Officers (DPOs) to level up their capabilities. The PDPC's DPO Competency Framework and Training Roadmap helps to guide the DPOs' progression.

While the Government provides the necessary support and guidance to help organisations strengthen their cybersecurity and data protection capabilities, organisations are, ultimately, responsible for safeguarding their customers' personal data. Organisations which breach the PDPA may be subject to financial penalties of up to $1 million. From 1 October 2022, the maximum cap of financial penalties will be increased to 10% of an organisation's annual turnover in Singapore or $1 million, whichever is higher.
