Parliament No:	14
Session No:	1
Volume No:	95
Sitting No:	75
Sitting Date:	9-11-2022
Section Name:	Oral Answers to Questions
Title:	Educating Businesses on Protection of Customers' Data and Enhancing Punishment Against Hacking
MPs Speaking:	The Senior Minister of State for Communications and Information (Mr Tan Kiat How),Mr Lim Biow Chuan,Mr Lim Biow Chuan (Mountbatten),Mr Tan Kiat How

EDUCATING BUSINESSES ON PROTECTION OF CUSTOMERS' DATA AND ENHANCING PUNISHMENT AGAINST HACKING

6 Mr Lim Biow Chuan asked the Minister for Communications and Information (a) whether IMDA can do more to educate businesses on the need to protect their customers' data from being hacked; and (b) whether the punishment against illegal hackers of such data can be enhanced.

The Senior Minister of State for Communications and Information (Mr Tan Kiat How) (for the Minister for Communications and Information): Mr Deputy Speaker, our laws make clear the obligations that businesses must meet when they collect and store customers' data. In addition, the Personal Data Protection Commission, or PDPC, and the Cyber Security Agency, or CSA, have published resources on their websites to educate organisations, including businesses, on the importance of data protection and cybersecurity.

The PDPC's "Guide to Data Protection Practices for ICT Systems" compiles a set of good data protection practices that organisations can implement. PDPC has also published the common causes of breaches for IT systems, cloud-based applications and other IT systems, so that businesses are aware of the risks they face. CSA's website also has cybersecurity toolkits available for free, to guide organisations on the cybersecurity practices to protect themselves from cyberattacks and data breaches.

The Government has gone beyond education and raising awareness and is doing more to encourage businesses to adopt good cybersecurity and data protection measures. SMEs may participate in the Infocomm Media Development Authority (IMDA) and PDPC's Data Protection Essentials programme (DPE). It helps them implement baseline data protection and cybersecurity practices, such as antivirus, firewall, data back-up and encryption, with support from a curated panel of service providers. CSA has

also launched the Cyber Trust and Cyber Essentials marks, which businesses can apply for and be recognised for good cybersecurity measures.

Unauthorised access to computer material is punishable under the Computer Misuse Act or CMA. Perpetrators are liable, upon conviction, for a fine not exceeding $5,000 or imprisonment for a term not exceeding two years, or both. Knowingly obtaining or dealing in personal information that has been obtained through unauthorised access is also punishable under the CMA, with a fine of up to $10,000 or imprisonment of up to three years, or both. Penalties are more severe for a second or subsequent conviction.

These two offences under CMA are also listed as serious offences under the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act. Persons who knowingly acquire, possess, use, conceal or transfer the benefits of such offences, or assist another to retain such benefits, are liable to a fine not exceeding $500,000 or to imprisonment for a term not exceeding 10 years, or to both. The Courts can also confiscate any benefit arising from both offences under this Act.

The Government takes illegal hacking very seriously and will ensure our laws remain effective in the development of a safe and secure cyberspace. Notwithstanding these penalties, it is, ultimately, the responsibility of businesses to be vigilant and adopt proper cybersecurity and data protection measures to keep their customers' data safe.

Mr Deputy Speaker: Mr Lim Biow Chuan.

Mr Lim Biow Chuan (Mountbatten): Sir, last year, it was reported that a total of $2.68 million was collected in fines for personal data protection breaches. And last month, it was reported that 2.6 million accounts of an online marketplace company were hacked and the data sold on the dark web. Is IMDA satisfied that enough has been done to encourage companies to protect the data, because it seems like this is going on and on?

For the second supplementary question, have any hackers been caught? If so, would IMDA be willing to publish more information so as to send the signal to hackers or hackers-to-be that there are serious consequences that they have to face for hacking into people's data?

Mr Tan Kiat How: Mr Deputy Speaker, I thank the Member for raising pertinent points and it is an appreciation of the context that we are operating in. More businesses, more industries and individuals are spending more time online; we are putting our personal data in different systems; we are transacting more online in terms of B2B transactions, B2B2C and across P2P as well. So, it is the nature of our times that we get more digital and more online. That is why we see an increased focus on the need for good cybersecurity and data protection measures.

In fact, the Personal Data Protection Act (PDPA) was updated and amended in 2020, a couple of years ago, to reflect this growing trend that we see. And one important update to the PDPA was the enhancement of the penalty framework, which took effect from 1 October 2022. Previously, the financial penalty cap which may be imposed on organisations for breaches under the PDPA was up to $1 million. With the amendment and update, which came into effect on 1 October 2022, it is up to 10% of an

organisation's annual turnover in Singapore or organisations with annual local turnover exceeding $10 million, whichever is higher.

This signals the Government's and I think our economy and society's focus on good data protection.

Having said that, I think going after the organisations after the data breach is almost like catching the horse after the barn door has opened and the horse has dashed out. What is more important is ex ante practices to even prevent the data from being exfiltrated or taken out of the organisation.

That is where the important philosophy and the fundamental principle of the amendment of the PDPA in 2020 put emphasis on that, which is about accountability. It is a fundamental principle of the PDPA – the organisations have to take responsibility for personal data under their possession or control. They have to be answerable to not just the regulatory authorities, their business partners, but, importantly, to the individuals and their clients and customers whose data is being entrusted to be kept under the control or possession of the organisation or business.

So, to Mr Lim's point on whether we are satisfied, I think this is something we have to continue working on. I call on all businesses and organisations – and I encourage them – to take this seriously. There are many resources and toolkits available on the website, including many different schemes, to help businesses start on their journey or enhance their cybersecurity or personal data protection.

In terms of transparency, as Mr Lim alluded to, we have the Personal Data Protection Commission (PDPC) that publishes all the different decisions on the data breaches investigations on their website. This is not just to have a salutary impact on other businesses and organisations to take this seriously, but also for other businesses and organisations to understand the good practices of where other organisations have come short and to incorporate some of these good practices into their operations and business environment.

I encourage all businesses to take a look at what has been published on PDPC's website on the breaches around the PDPC regulatory regime.

Mr Deputy Speaker: No supplementary questions? There is a supplementary question. Mr Lim Biow Chuan.

Mr Lim Biow Chuan: Sorry, Sir. I just wanted to ask the Senior Minister of State whether any hackers have been caught and will he say something about the punishment.

Mr Tan Kiat How: In terms of the hackers, I presume Mr Lim is asking in relation to the Computer Misuse Act – rather than the Personal Data Protection Act. Sorry, I thought he was referring to the PDPA and the PDPC.

The Computer Misuse Act was last amended in 2018 and we are consistently making sure it remains effective. It was already amended in 2017 to allow the authorities to handle the increasing scale and complexity of cybercrimes, which include hacking, as Mr Lim alluded to, as well as the evolving tactics of cybercriminals. One of the notable amendments was the criminalised act of dealing in hacked personal information.

On the specifics of the hackers being caught and some of the penalties that have been meted out, I do not have the specific information now because it is under the Computer Misuse Act. If Mr Lim is interested, do file a separate Parliamentary Question and we will take it up.
