PERSONAL DATA PROTECTION COMMISSION

[2021] SGPDPC 11

Case No. DP-2009-B7057

In the matter of an investigation under
section 50(1) of the Personal Data Protection Act 2012

And

Commeasure Pte Ltd

… *Organisation*

DECISION

Data Protection *– Protection obligation – Disclosure of personal data – Failure to implement reasonable security arrangements*

Data Protection *– Data intermediary – Obligations of data intermediary and organisation which engages a data intermediary*

Commeasure Pte Ltd.

[2021] SGPDPC 11

Lew Chuen Hong, Commissioner — Case No. DP-2009-B7057

15 September 2021

Introduction

1 On 25 September 2020, the Personal Data Protection Commission ("**the Commission**") received a data breach notification from Commeasure Pte Ltd ("**the Organisation**") that its database containing 5,892,843 customer records had been accessed and exfiltrated ("**the Incident**"). The Organisation first found out about the data breach on 19 September 2020 when a cybersecurity company based in Atlanta, United States of America, approached the Organisation with an offer to contain the breach and retrieve the data from the hackers. The Commission commenced investigations into the Incident thereafter.

Facts of the Case

Background

2 The Organisation was incorporated in Singapore in 2014, and operates a hotel booking platform www.reddoorz.com which serves customers in the Southeast Asian region, such as Indonesia, Singapore, Philippines, Vietnam and Thailand. The Singapore office is primarily engaged in sales, finance and administrative activities, while all IT functions (including the management of the affected application package in this case) were managed by the Organisation's subsidiary company, Commeasure Solutions India Pvt Ltd ("**CPL India**").

Cause of the Incident

3 Investigations revealed that the unknown threat actor(s) had most likely gained access and exfiltrated the Organisation's database of customer records hosted in an Amazon RDS cloud database, after they obtained an Amazon Web Services ("**AWS**") access key. The AWS

access key was embedded within an Android application package ("**the affected APK**") publicly available for download from the Google Play Store.

4 This affected APK was created sometime in 2015, when the Organisation was still a start-up, and was last updated in January 2018. Even though the AWS access key had access to a "live" or production database, the AWS access key was embedded in the APK, and erroneously marked as a "test" key by the then-developers. With the exception of one of the Organisation's co-founders and Chief Technology Officer, all the developers have since left the Organisation. Most unfortunately, even though the Organisation regarded this APK as "defunct", the APK remained publicly available for download on the Google Play Store until the Organisation became aware of the Incident and removed the affected APK.

5 The fact that the Organisation had treated the affected APK as a "defunct" APK meant that even though the Organisation had engaged a cybersecurity company to conduct a security review and penetration testing sometime from September 2019 to December 2019, it was not within the scope of the security review or penetration tests. Consequently, the vulnerability was left undetected and exposed until the Organisation found out about the Incident. Likewise, even though the Organisation used "Proguard" on its current Android apps to prevent reverse engineering of APKs, which may have prevented the unknown threat actors from retrieving the AWS access key, the Organisation failed to review and deploy "Proguard" on the affected APK which it regarded as "defunct".

6 As a result of the Incident, the Organisation's database containing 5,892,843 customer records which included the customer's name, contact number, email address, date of birth, a hashed password (encrypted with one-way BCrypt hash algorithm) used by the customer to access their "RedDoorz" account and their booking information was accessed and exfiltrated by unknown threat actor(s). Based on the Organisation's investigations, the unknown threat actor(s) did not gain access or download the customers' masked credit card numbers.

Remedial actions

7 Following the Incident, the Organisation took the following remedial actions:

a. CPL India immediately removed the affected APK from the Google Play Store;

b. The old access keys were invalidated and new access keys were created. The infrastructure and code repository access credentials were changed;

c. IP blocking of suspicious traffic was enabled; and

d. Informed all the affected customers via email on 26 September 2020 of the data breach, advising them to change their RedDoorz account password as an added precautionary measure, and to avoid using the same password on other digital platforms.

8 To prevent a recurrence of the Incident or similar incidents, the Organisation also took the following remedial actions:

a. The Organisation amended its credential policy to clearly prohibit developers from embedding access codes in any code base;

b. The Organisation upgraded their IT infrastructure to a private space for isolation of the customer database from the Internet. Only whitelisted IP addresses were allowed connection to 'live' databases;

c. The Organisation separated the accounts for production and staging environments for all AWS services. Two-factor authentication was enabled for all tools and accounts used by developers. VPN-based control was implemented to access infrastructure resources;

d. The Organisation configured alerts to capture mySQL dump query. Web application firewalls were set up. An audit of all user access to the AWS environment was conducted; and

e. The Organisation appointed a cybersecurity company to conduct vulnerability assessment and penetration testing of all its existing applications.

Findings and Basis for Determination

Whether the Organisation contravened the Protection Obligation

9 Section 24 of the Personal Data Protection Act 2012 ("**PDPA**") requires an organisation to protect personal data in its possession or under its control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks (the "**Protection Obligation**"). For the reasons set out below, the Organisation failed to implement reasonable security arrangements to protect the personal data in its control.

10 The Organisation collected the personal data of customers when they created a "RedDoorz" account through its hotel booking platform www.reddoorz.com. Even though the Organisation's customer database was hosted using Amazon RDS on cloud, on servers physically located in North Virginia, United States of America, the database remained under the Organisation's control throughout as the Organisation could access, use and remove the data.

11 In *Re The Cellar Door Pte Ltd*,[1] we found that even though the organisation was not in direct possession of the personal data that was held in the data intermediary's servers, it was still obliged to implement reasonable security arrangements to protect the personal data as it had control over such data. Likewise, even though AWS was responsible for the security of the

[1] [2017] PDP Digest 160.

cloud infrastructure that it provided to the Organisation, the Organisation bore ultimate responsibility under section 24 of the PDPA for making reasonable security arrangements to protect all the customers' data under its control.

12 The data breach occurred because the Organisation embedded the AWS access key, which allowed access to the "live" or production database, in the APK. The root cause was therefore in the application, which was clearly within the Organisation's responsibility. This presented a clear security risk. The AWS access key comprises of two parts, first, the access key ID, and second, the secret access key, and was effectively the Organisation's username and password. In a webpage titled "Best practices for managing AWS access keys", AWS advised users to protect the access keys as "anyone who has the access keys for your AWS account root user has unrestricted access to all resources in your AWS account" [2]. AWS also cautioned users not to "embed access keys directly into code", which was exactly what the Organisation had done in the present case. We therefore find the Organisation in breach of section 24 of the PDPA for reflecting the AWS access key in the affected APK.

13 In the course of investigations, the Organisation explained that its failure to implement sufficiently robust processes to manage its inventory of infrastructure access keys was attributable to the high turnover of its employees from the time of its inception to the discovery of the Incident. This explanation is unacceptable, however sympathetic one might be to the human resource issues that the Organisation had to manage. The Organisation's responsibility to protect personal data in its control or possession commences ought not to have been subjected to staff movement or appointment.

14 In *Re WTS Automotive Services Pte Ltd*,[3] we highlighted the importance of conducting a "regular review to ensure that the website collecting personal data and the electronic database storing the personal data has reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks" as the "personal

[2] https://docs.aws.amazon.com (last accessed on 6 August 2021).
[3] [2019] PDP Digest 317.

data of individuals may be exposed if the website or database in which it is stored contains vulnerabilities".[4] The Commission reiterates that it is necessary for an organisation to "[c]onduct regular ICT security audits, scans and tests to detect vulnerabilities".[5]

15 In this case, the Organisation conducted internal security testing and application architecture reviews every quarter and had engaged a cybersecurity company to conduct a security review and penetration testing sometime from September 2019 to December 2019. The Organisation admitted however, that it "overlooked" including the affected APK in the security review as it was "old". In addition, the Organisation admitted that the AWS access key had been mistakenly marked as a "test key". This resulted in its omission from the security review as well as from the Organisation's periodic review of accounts and login credentials.

16 It is important to highlight that the Organisation remained responsible for the affected APK. The Organisation's failure to include the affected APK and the AWS access key within the scope of the security review arose because of the Organisation's negligence to include them in its inventory of IT assets in production after the Organisation had wrongly labelled the affected APK as "defunct" and the AWS access key as a "test" key.

17 Accordingly, we are not satisfied that the IT security reviews that the Organisation conducted were sufficiently rigorous, and met the standard required under section 24 of the PDPA. We are therefore of the view that the Organisation has breached section 24 of the PDPA for failing to include the affected APK and AWS access key in the Organisation's security reviews. If a security review had examined the affected APK or the AWS access key, the vulnerability exposed by the embedded AWS access key would have been discovered, and the Incident could have been prevented.

---

[4] Personal Data Protection Commission, *Guide to Data Protection Impact Assessments* (1 November 2017) at para. 8.3.
[5] Personal Data Protection Commission, *Guide to Securing Personal Data in Electronic Medium* (revised 20 January 2017) at para. 6.1.

The Commission's Directions

18 In determining whether to impose a financial penalty on the Organisation pursuant to section 48J(1) of the PDPA, and if so, the amount of such financial penalty, we took into account the factors listed at section 48(6) of the PDPA. The Commission notes that the data breach affected 5,892,843 individuals whose personal data was exfiltrated. This is the largest data breach that has occurred since the PDPA came into effect. Further, prior to the exfiltration of the data in September 2020, the affected APK with the embedded AWS access key had remained publicly available for download on the Google Play Store for a significant duration of time. A lengthy period of 2 years and 9 months passed from the time the Organisation made its last update to the affected APK in January 2018 to 19 September 2020, when the Organisation finally found out about the data breach.

19 Having said that, the Commission also took into account the following mitigating factors:

(a) The Organisation was cooperative in the course of investigations and had provided prompt responses to PDPC's requests for information;

(b) The Organisation implemented remedial actions to address the Incident; and

(c) The Organisation had conducted periodic security reviews which promised to offer some data protection, albeit their efforts were ultimately futile as these security reviews did not include the affected APK.

20 In deciding the amount of financial penalty to be imposed, we also considered that the Organisation, which operates in the hospitality industry, had been severely impacted by the COVID-19 pandemic. Having considered all the relevant factors of this case, the Commissioner hereby requires the Organisation to pay a financial penalty of $74,000 within 30 days from the date of the relevant notice accompanying this decision, failing which interest

at the rate specified in the Rules of Court[6] in respect of judgment debts shall accrue and be payable on the outstanding amount of such financial penalty until the financial penalty is paid in full.

YEONG ZEE KIN
DEPUTY COMMISSIONER
FOR COMMISSIONER FOR PERSONAL DATA PROTECTION

[6] Cap 322, R5, 2014 Rev Ed.