PERSONAL DATA PROTECTION COMMISSION

[2023] SGPDPC 6

Case No. DP-2009-B7056

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

And

E-Commerce Enablers Pte. Ltd.

… *Organisation*

DECISION

E-Commerce Enablers Pte. Ltd.

Lew Chuen Hong, Commissioner — Case No. DP-2009-B7056

16 May 2023

Introduction

1 On 25 September 2020, E-Commerce Enablers Pte. Ltd. ("**Organisation**") notified the Personal Data Protection Commission ("**PDPC**") and its customers of an incident involving unauthorised access to its customer data servers (the "**Incident**"). PDPC subsequently received 2 complaints from the Organisation's customers in relation to the Incident. On 12 November 2020, the Organisation's customer database was offered for sale on an online forum indicating that personal data was exfiltrated during the Incident.

2 PDPC commenced investigations to determine the Organisation's compliance with the Personal Data Protection Act 2012 ("**PDPA**") in relation to the Incident.

Facts of the Case

3 The Organisation runs an online platform offering cashback for purchases made through affiliated merchant programs. The platform also provides coupons, voucher codes, and comparison features with discounts for users.

4 At the time of the Incident, the Organisation hosted its customer database on virtual servers in an Amazon Web Services ("**AWS**") cloud environment ("**Customer**

Storage Servers"). The Organisation employed a 12-man Site Reliability Engineering ("**SRE**") team whose responsibilities included maintaining the Organisation's infrastructure, providing, and managing the Organisation's cloud environment on AWS, and ensuring security of the AWS keys. The SRE team made use of an AWS access key with full administrative privileges (the **"AWS Key**") for the purposes of its work, including infrastructure deployment. Only SRE team members had access to, and were authorised to use, the AWS Key. On 4 June 2019, the AWS Key was inadvertently committed to software code in a private repository in GitHub, by a senior member of the SRE team. This was discovered by another SRE team member on 6 June 2019, and the AWS Key was removed from GitHub on the same day. However, it remained viewable in GitHub's 'commit history', which records all changes and previous versions of code uploaded on GitHub.

5 On 21 June 2019, the AWS Key was to be deleted and replaced by a new key as part of an out-of-cycle key rotation. The member of the SRE team in charge of the key rotation informed the SRE team (via email) that he had created a new key to replace the AWS Key, and that he would be deleting the AWS Key. However, after creating the replacement key, he failed to fully disable and remove the AWS Key.

6 As a result, the AWS Key continued to be usable to access the Organisation's AWS environment (and consequently the Customer Storage Servers) until shortly after the time of the Incident, about 15 months later.

The Incident

7 On 9 September 2020, a malicious threat actor accessed the Organisation's AWS environment utilizing the AWS Key. The AWS Key was likely found by the threat actor in the commit history of the GitHub private repository.

8 Having gained privileged access to the AWS environment, the threat actor (i) conducted reconnaissance to identify the Organisation's data repositories, (ii) modified security settings including to allow remote internet access to the Organisation's database instances (i.e. its virtual servers hosting data), and (iii) generated a fresh database instance to stage its data exfiltration.

9 The threat actor then proceeded to exfiltrate data from the Customer Storage Servers. The data items, and the corresponding number of individuals affected, are set out below:

Types of personal data	**Number of affected users**
Email Address	1,457,637
Name	840,210
Mobile number	447,076
Address	138,327
Gender	23,278
NRIC numbers	9,961
Date of birth	202,634
Bank Account number	299,381
Partial credit card information, including:	378,531

(i) partial credit card number (first 6 digits and last 4 digits) (ii) issuing bank (iii) country (iv) expiry month and year (v) Visa or Mastercard	

10 On 17 September 2020, the Organisation discovered during a routine security review that there had been unauthorised access to its AWS environment. Further investigations revealed that there had been unauthorised third-party access to the Organisation's AWS environment.

11 The Organisation subsequently engaged a private forensic expert, ("**PFE**") to investigate further. The PFE confirmed that the unauthorised access had been carried out using the AWS Key. The Organisation conjectured that it was likely that the threat actor had obtained the AWS Key from GitHub's commit history, where the AWS Key was still visible despite the removal of the wrongly committed code from the private repository in GitHub.

Remedial actions

12 Following the Incident, the Organisation implemented the following remedial measures:

<u>Immediate remedial steps to contain the Incident</u>

(a) Performed a full deletion of the AWS Key and rotated the other AWS keys;

(b) Reversed all changes made by the threat actor and triggered a forced logout and password reset of all customers' accounts;

To prevent recurrence or similar incidents

(c) Increased monitoring of logs to ensure heightened detection of any unauthorised access;

(d) Separated development and production accounts, resulting in a smaller subset of engineers having access to the production environment;

(e) Secured access to systems and data with several measures, including VPN and IP address whitelisting and database encryption; and

(f) Created a platform for employee security suggestions / breach reporting.

Subsequent sale of personal data on Raidforums

13 On 12 November 2020, the Organisation's database was offered for sale on Raidforums, an online cybersecurity forum commonly used for trading and selling of stolen databases. Raidforums' domain name and content was independently seized by authorities from the United States in April 2022.

Findings and Basis for Determination

14 Based on the circumstances of the Incident, the Commission's investigation centred on whether the Organisation had breached its obligations under section 24 of the PDPA 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**"). The Organisation was determined to have breached the Protection Obligation in two respects.

Lack of sufficiently robust processes for AWS key management

15 First, the Organisation failed to ensure that processes to manage the AWS keys that granted access to the Customer Storage Servers were sufficiently robust.

16 While the Organisation admitted that it could have done more to ensure that its employees were performing their AWS key rotation duties properly, the Organisation claimed that the compromise of the AWS Key arose from human error, and not because of any systemic issue with the Organisation's security practices. According to the Organisation, there was no reason to doubt the capabilities of the SRE team member in question, because (i) he was a senior member of the SRE team, (ii) his responsibilities included key security and rotation, and (iii) he had dutifully rotated / deleted all other keys assigned to him in the out-of-cycle key rotation. The SRE team member's inadvertent commit, and an incomplete rotation/deletion were in direct contravention of the Organisation's security practices. The Organisation accordingly sought to frame the Incident as a one-off case of human error.

17 This position is not accepted. As explained in *Re DataPost Pte Ltd*, Organisations cannot place sole reliance on their employees to perform their duties properly as a security arrangement to protect personal data. There must be some

processes to ensure that the step required from the employee is taken, such as independent verification by another checker[1].

18 For example, a precaution the Organisation could have taken to ensure that the out-of-cycle key rotation was complete would have been to have a supervisor or another SRE team member test either all or a reasonable sample of the old keys (depending on the number of keys being rotated) to verify that they had been disabled. There was no such verification or testing practice put in place by the Organisation; the Organisation relied wholly on the SRE team member's seniority and experience.

19 When a high-risk task (e.g. rotation of an AWS key that gives access to the whole of the AWS environment) is concerned, it is all the more important that there must be additional verifications and checks.

Failure to conduct periodic security review

20 Second, specific security review by the Organisation on AWS keys could have covered and detected whether the AWS Key remained active or had been used after the out-of-cycle key rotation, and during the 15 months preceding the Incident. The Organisation failed to conduct regular security review on whether the AWS keys had been properly rotated/deleted. In the course of investigations, the Organisation acknowledged that it could have done more to ensure that the SRE team was performing their AWS key rotation duties properly. Following the Incident, the

[1] *Re DataPost Pte Ltd* [2017] SGPDPC 10, at [13] – [16]

Organisation implemented a more secure process for temporary, time-limited keys to be issued to SRE team members whenever access to the AWS environment was required. The Organisation also developed a specific IT security policy concerning the secure sharing of keys internally.

Observation on the incident management processes

21 Following discovery of the inadvertent committal of the AWS Key to GitHub, the Organisation took 15 days to conduct a key rotation. Regardless of whether this had been an out-of-cycle rotation, the Organisation should review its incident management processes to determine whether it was reasonable to have taken 15 days to remediate compromise of a full administrative privilege AWS access key.

The Commissioner's Decision

22 In determining whether to impose a financial penalty on the Organisation pursuant to section 48J(1) of the PDPA, and the amount of any such financial penalty, the matters set out at section 48J(1) and the factors listed at section 48J(6) of the PDPA were taken into account, including the following aggravating and mitigating factors:

Aggravating Factors

(a) The Organisation lacked sufficiently robust processes to monitor its incident management response to ensure reasonable remediation speed, which led to 15 days passing before the Organisation responded to the exposure of the AWS Key;

(b) The AWS Key was exposed for a long period of 15 months;

Mitigating Factors

(a) The Organisation took prompt remedial actions, including notifying the affected individuals;

(b) The Organisation was cooperative during investigations; and

(c) The Organisation voluntarily acknowledged that its failure to ensure proper rotation and deletion of the AWS Key constituted a breach of the Protection Obligation.

23 The Organisation was notified of the preliminary decision by way of the Commission's letter dated 15 February 2023 and was invited to make representations on the same. The Organisation made representations on 22 March 2023, albeit not on its liability for breaches of the Protection Obligation or on the proposed financial penalty. Where accepted by the Commission, these representations have been incorporated into this decision.

24 Having considered all the relevant circumstances of this case, the Commissioner hereby requires the Organisation to pay a financial penalty of $74,400 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 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.

25 No further directions are necessary on account of the remedial measures already taken by the Organisation.