PERSONAL DATA PROTECTION COMMISSION

[2020] SGPDPC 5

Case Nos.: DP-1904-B3721

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

And

Royal Caribbean Cruises (Asia) Pte. Ltd.

… *Organisation*

DECISION

Royal Caribbean Cruises (Asia) Pte. Ltd.

[2020] SGPDPC 5

Tan Kiat How, Commissioner — Case No. DP-1904-B3721

4 February 2020

Introduction

1 On 14 April 2019, Royal Caribbean Cruises (Asia) Pte. Ltd. (the "**Organisation**") notified the Personal Data Protection Commission (the "**Commission**") that the systems of one of the Organisation's vendors (the "**IT Vendor**") had been subject to a cyber-attack, resulting in the personal data of some of the Organisation's customers being exposed to unauthorised access (the "**Incident**").

Facts of the Case

2 In early 2017, the Organisation engaged the IT Vendor to develop and supply the Organisation with an electronic receipt system to generate and store electronic receipts with respect to payments made by the Organisation's customers for cruise and holiday bookings (the "**Receipt System**"). The initial plan was for the Receipt System to be hosted on the Organisation's internal server. However, after taking into consideration that the Receipt System would need to be accessed from external Internet Protocol ("**IP**") addresses during events and roadshows, the Organisation asked the IT Vendor to host the Receipt System on an Amazon Web Services ("**AWS**") server. The Receipt System was installed on an AWS Server in December 2017 and the Organisation started using the Receipt System at the end of January 2018.

3 On 11 April 2019, the Organisation encountered difficulties operating the Receipt System and reported the issue to the IT Vendor. On 12 April 2019, the IT Vendor informed the Organisation that the Receipt System had been subject to a cyber-attack. The cyber-attacker had deleted the database in the Receipt System, and replaced it with a ransom message demanding payment of 0.08 Bitcoins in order to recover the deleted data.

4 The following types of personal data belonging to 6,004 of the Organisation's customers ("**Affected Customers**") were affected by the Incident (collectively, "**Customer Data**"):

(a) Receipt Date and Number;

(b) Sailing Date;

(c) Name of Guest / Card Holder;

(d) Ship Name;

(e) Booking ID;

(f) Amount Paid;

(g) Payment Type;

(h) The first four and last four digits of credit / debit card number for payments made using credit / debit cards;

(i) Issuing bank and the 6 digit cheque numbers for payments made using cheques; and

(j) Voucher redemption numbers for payment made using vouchers.

5 In addition, 440 of the 6,004 Affected Customers had completed an online check-in process that required them to provide additional personal data. These 440 Affected Customers had the following types of additional personal data placed at risk of unauthorised access (collectively, "**Additional Customer Data**"):

(a) Name;

(b) Nationality;

(c) Marital status;

(d) Date of birth;

(e) Residential address;

(f) Mobile number;

(g) Email address;

(h) Emergency contact information;

(i) Last 4 characters of the passport numbers;

(j) Passport expiry date; and

(k) Customer credit card details including the cardholder's name, credit card issuer, last 4 digits, and expiry date.

6 There were 25 employees of the Organisation whose personal data was also affected by the Incident (collectively, "**Employee Data**"):

(a) Name;

(b) Receipt System Username;

(c) Receipt System User role;

(d) Receipt System Password;

(e) Email Address;

(f) Mobile number; and

(g) Location (i.e., office or roadshow).

7 Upon discovery of the Incident, the Organisation took the following remedial actions:

(a) On 12 April 2019, the Receipt System's phpMyAdmin[1] web application name was changed to obscure access. IP address restrictions were also added for access to the Receipt System;

[1] phpMyAdmin is an open source administration tool for MySQL and MariaDB data over the world wide web.

(b) On 16 April 2019, the Organisation engaged a cybersecurity consultant to conduct technical forensic investigations and identify vulnerabilities in the Receipt System;

(c) On 17 April 2019, the Organisation took the Receipt System offline permanently. The Organisation also blocked its online check-in portal to prevent information from the Receipt System from being used to access Additional Customer Data of the 440 Affected Customers; and

(d) On 1 May 2019, the Organisation notified the 440 Affected Customers of the Incident, on the basis that the Additional Customer Data that may have been accessed through the online check-in portal was likely to be sensitive and/or could materially impact them.

Findings and Basis for Determination

Whether the Organisation had contravened section 24 of the PDPA

8 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 taking reasonable security steps or arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks.

9 As a preliminary point, the Organisation owned the Receipt System and had possession and control over the Customer Data, Additional Customer Data and Employee Data at all material times. While the IT Vendor was engaged to develop the Receipt System, the Commission's investigations revealed that the IT Vendor had not processed, nor were they engaged to process, the Customer Data, Additional Customer Data and Employee Data on the Organisation's behalf. The IT Vendor was accordingly not a data intermediary and the Organisation was solely responsible for the protection of the Customer Data, Additional Customer Data and Employee Data.

10 The Receipt System had vulnerabilities and gaps that the cyber-attacker could easily have exploited, resulting in the Incident:

(a) The administrative credentials (i.e., administrator username and password) to log into the Receipt System were stored in files within the same server with no access controls and were therefore publicly accessible; and

(b) The version of the phpMyAdmin tool in use with the Receipt System at the material time was not patched and contained known security vulnerabilities.[2]

11 In relation to (a), given that the administrative credentials would allow and enable access to Customer Data, Additional Customer Data and Employee Data of a significant number of individuals stored in the Receipt System, it clearly should not have been stored in files without access controls, especially so when the files were in the same server. In relation to (b), and as mentioned in previous decisions,[3] regular security testing and patching as security measures is absolutely crucial. Patching is one of the common tasks that all system owners are required to perform in order to keep their security measures current against external threats. The Organisation clearly did not have any process in place to ensure regular patching in the present case.

12 According to the Organisation, it was the IT Vendor's responsibility to put in place the appropriate security measures for the Receipt System. In contrast, the IT Vendor asserted that it was the Organisation's network security team that was in charge of security. The Commission's investigations revealed that the Organisation had not in fact engaged the IT Vendor to provide services in relation to security maintenance or patching of the Receipt System. As the data controller and customer, the Organisation ought to be clear about the scope of services that it is procuring from the IT Vendor, and document the scope properly in contract or other project documentation. In this case, the Organisation was not able to produce anything in writing to corroborate its assertions. The absence of documentation, on the contrary, buttresses the IT Vendor's assertion that it was not engaged to provide services in relation to security measures for the Receipt System. Without clarity, the risks of any omissions will fall on the Organisation, which as data controller is ultimately responsible. In the circumstances, the Commissioner finds that it was the Organisation and not the IT Vendor that had the obligation to ensure that the Receipt System had up-to-date security maintenance and patching.

[2] The security vulnerabilities were listed in Common Vulnerabilities and Exposures, which is a list of publicly disclosed information security vulnerabilities and exposures.
[3] See for example *Re The Cellar Door Pte Ltd and Global Interactive Works Pte Ltd* [2016] SGPDPC 22 at [26]; *Re Singapore Health Services Pte. Ltd. & others* [2019] SGPDPC 3 at [124]; *Re Tutor City* [2019] SGPDPC 5 at [23]; *Re Genki Sushi* [2019] SGPDPC 26 at [20]-[21].

13 The Organisation's failure to implement security measures, including software patches to ensure that vulnerabilities the Receipt System were properly patched, resulted in a standard of protection that fell far short of what was required for the Receipt System. As such, the Organisation failed to put in place reasonable security arrangements to protect the Customer Data, Additional Customer Data and Employee Data. Accordingly, the Commissioner finds the Organisation in breach of section 24 of the PDPA.

The Commissioner's Directions

14 In determining the directions, if any, to be imposed on the Organisation under section 29 of the PDPA, the Commissioner took into account the following mitigating factors:

(a) The Organisation cooperated with the Commission in its investigations; and

(b) The Organisation took prompt remedial actions in respect of the Incident.

15 Having considered all the relevant factors of this case, the Commissioner hereby directs the Organisation to pay a financial penalty of $16,000 within 30 days from the date of this direction, 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 it is paid in full. The Commissioner has not set out any further directions given the remediation measures already put in place.

YEONG ZEE KIN
DEPUTY COMMISSIONER
FOR COMMISSIONER FOR PERSONAL DATA PROTECTION