Management Corporation Strata Title Plan No. 3400

[2020] SGPDPC 10

Yeong Zee Kin, Deputy Commissioner — Case No. DP-1909-B4797

Data Protection – Protection obligation – Unauthorised access to and disclosure of personal data – Insufficient security arrangements

17 March 2020

Introduction

1 On 2 September 2019, the Personal Data Protection Commission (the "**Commission**") was notified that a directory containing personal data belonging to Management Corporation Strata Title Plan No. 3400 (the "**Directory**") was accessible on the Internet by any member of the public (the "**Incident**").

Facts of the Case

2 In April 2012, Management Corporation Strata Title Plan No. 3400 (the "**Organisation**") purchased a Network Attached Storage Device (the "**NAS**") for the purposes of internal file sharing among its administrative staff over a local network. The Directory was one of the files stored on the NAS. The Organisation did not intend for the NAS to be connected to the Internet. Prior

to the Incident, the Organisation was unaware that the Directory could be accessed via an Internet Protocol address without the need for any login credentials.

3 The Directory contained personal data of 562 individuals collected for the purposes of complying with the Building Maintenance and Strata Management Act, the Building Maintenance (Strata Management) Regulations 2005, as well as to contact subsidiary proprietors of the Organisation.

4 The following types of personal data of the Affected Individuals were exposed to the risk of unauthorised disclosure (collectively, the "**Disclosed Data**"):

(a) 12 council members of the Organisation: Name; NRIC / Passport Number; Contact number; Email address; and

(b) 550 subsidiary proprietors of the Organisation: Name; Email address; Contact number; Block and Unit number; Change of property ownership details; Identity of resident; Statement of accounts; Car plate numbers; Figures in relation to share values/arrears.[1]

[1]The types of personal data collected from the 550 subsidiary proprietors varied. This was because apart from the mandatory requirement to provide their names, the other types of personal data were optional fields.

5 Upon being informed of the Incident by the Commission on 2 September 2019, the Organisation promptly disconnected the NAS from the Internet on the same day.

Findings and Basis for Determination

Whether the Organisation had contravened section 24 of the PDPA

6 In today's digital age, many organisations are moving towards paperless offices. Through digitisation, an increasing amount of information (including personal data) is stored electronically and online. This has resulted in a higher risk of data breaches involving IT security vulnerabilities. In the past few years, the Commission has investigated data breaches involving Insecure Direct Object References[2], SQL injection vulnerability[3], and absence of directory access controls[4]. Given the increasing number of cases involving IT security vulnerabilities, including the present one, I would like to take this opportunity to highlight some of the measures that organisations could implement in order

[2]See *Re InfoCorp Technologies Pte. Ltd.* [2019] SGPDPC 17 and *Re Singapore Telecommunications Limited* [2019] SGPDPC 36.

[3]See *Re Metro Pte Ltd* [2016] SGPDPC 7; *Re Ncode Consultant Pte Ltd* [2019] SGPDPC 11; and *Re Creative Technology Ltd* [2020] SGPDPC 1.

[4]See *Re Fu Kwee Kitchen Catering Services & anor* [2016] SGPDPC 14; *Re Tutor City* [2019] SGPDPC 5; *Re Advance Home Tutors* [2019] SGPDPC 35; *Re SearchAsia Consulting Pte. Ltd.* [2019] SGPDPC 40; and *Re Society of Tourist Guides (Singapore)* [2019] SGPDC 48.

to comply with their obligations under Section 24 of the Personal Data Protection Act 2012 (the "**PDPA**").

7 Section 24 of the 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 (the "**Protection Obligation**"). In my view, the Organisation failed to put in place reasonable security arrangements to protect the Disclosed Data and was in breach of the Protection Obligation for the reasons explained below.

8 In an IT security context, timely detection of risks to personal data is key to an organisation's compliance with the Protection Obligation. As explained and discussed below, there are two key measures that organisations should implement to detect IT security vulnerabilities.

9 First, organisations should conduct code reviews[5] and pre-launch testing[6] before new IT features or changes to IT systems are deployed. These processes allow organisations to pick up and rectify errors and/or flaws in the

[5] Depending on the complexity and scope of the new code/system, organisations may conduct the code reviews manually, or with the appropriate automated code review software and tools.

[6] This may include load testing, stress testing and/or integration testing.

new IT features and/or systems prior to deployment. There have been a number of cases where errors in the application code resulted in the unintended disclosure of personal data or unintended access to personal data: see, for example, *Re Singapore Telecommunications Limited* [2019] SGPDPC 36[7], and *Re Flight Raja Travels Singapore Pte Ltd* [2018] SGPDPC 16[8]. This is particularly important if the new IT feature is accessible from the Internet, and therefore exposed to a "*multitude of cyber threats that may compromise the website and expose any personal data [the organisation] collects*"[9].

10 Second, organisations should conduct periodic security reviews of its IT systems[10]. The comprehensiveness of such security reviews should be scoped based on the organisation's assessment of its data protection needs. For example, periodic security reviews would not typically include penetration tests for most systems that are within the internal corporate network. However,

---

[7]There was unauthorised disclosure of personal data of the organisation's customers due to a direct object reference vulnerability (which was a design issue in the organisation's mobile app's application programming interface).

[8]The organisation introduced a new mobile application that allowed access to the online booking system through mobile devices without login. This resulted in some of the organisation's customers having unauthorised access to booking records (containing personal data) of other customers.

[9] See *Re Horizon Fast Ferry Pte. Ltd.* [2019] SGPDPC 27 at [26].

[10]As set out by the Commissioner in a number of previous decisions, including *Re WTS Automotive Services Pte. Ltd.* [2018] SGPDPC 26 at [18], *Re Bud Cosmetics* [2019] SGPDPC 1 at [24] and *Re Chizzle Pte. Ltd.* [2019] SGPDPC 44 at [6] to [8].

organisations with Internet-facing IT systems that contain personal data that is sensitive in nature should consider conducting penetration testing as part of their periodic security reviews.

11 Generally, as part of the periodic security review of its IT systems, organisations should avail themselves of up-to-date online vulnerability scanning tools, and are expected to acquire reasonable proficiency in their use or seek assistance by engaging vendors with the appropriate expertise[11]. The use of such tools provides organisations a reasonable chance of detecting common security vulnerabilities in their IT systems[12].

12 As a complement to the use of up-to-date online vulnerability scanning tools, the periodic security review of an organisation's IT systems should also include a manual component. This would include review of password management policies[13], archival of personal data that no longer needs to be stored online to near-line or off-line storage[14], and purging of personal data that no longer serves any legal or business purpose for the organisation.

---

[11]See *Re WTS Automotive Services Pte Ltd* [2018] SGPDPC 26 at [24], and *Re DS Human Resources Pte Ltd* [2019] SGPDPC 16 at [15(a)].

[12] For example, see the OWASP Top Ten at: https://owasp.org/www-project-top-ten/.

[13] See *Re GlogbalSign.in Pte Ltd* [2019] SGPDPC 43.

[14] See *Re Orchard Turn Developments Pte. Ltd.* [2017] SGPDPC 12.

13 In addition, it is important for an organisation to be aware of and track its personal data assets. The creation and maintenance of a personal data asset register (*i.e.* a record identifying all personal data in the organisation's possession or control) is a good practice that would assist organisations to comply with the Protection Obligation. An up-to-date personal data asset register provides the organisation with an accurate record of all the personal data in its possession or control, and enables the organisation to ensure its periodic security reviews covers the personal data assets. It also enables the organisation to more effectively review the implementation of its data protection policies, for example, the access control list setting out the employees who have access to the IT systems the personal data asset is stored in, whether the internal business owner of the personal data asset has reviewed it for data quality issues[15], and initiating the process for disposing personal data that have reached the end of its life cycle within the organisation.

14 In the present case, the Organisation admitted that it had not conducted any security reviews of its IT systems, including the NAS and the Directory. Consequently, it was unaware of their configuration which allowed access from

[15]This includes aspects like whether the personal data is accurate and how recently it was updated: see The Commission's Model ArtificiaI Intelligence Governance Framework (Second Edition) at page 38.

the Internet without any form of access control. The Organisation ought to have formulated a policy for the NAS and the Directory, implemented the IT security practices that gives effect to the policy and conducted periodic security reviews to ensure that the practices are adequate. For example, if the intention was to permit access to the NAS and the Directory from the Internet, then the policy should establish who should have access and the level of sensitivity of the personal data; the IT security practices would then implement the right level of security measures to control access to the personal data and protect the personal data during its transmission. On the contrary, if the intention was to restrict the NAS and the Directory to the internal corporate network, then the practices to implement this policy would include considerations like whether the NAS and the Directory was connected to the right segment of the corporate network and whether their configuration was effective in limiting access to users from within the corporate network. In view of the Organisation's admission, and the lack of any security measures to protect the Disclosed Data stored in the Directory, I find the Organisation in breach of section 24 of the PDPA.

Conclusion

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

(a) The majority of the Affected Individual's Disclosed Data exposed to risk of unauthorised access, use and/or disclosure related only to contact information;

(b) The Organisation's took prompt remedial action to disconnect the NAS from the Internet; and

(c) There was no evidence of actual misuse or exfiltration of the Disclosed Data.

16 Having considered all the relevant factors of this case, I have decided to issue a warning to the Organisation for the breach of its obligations under section 24 of the PDPA. No directions are required in view of the prompt remedial action implemented by the Organisation.

———————————