Genki Sushi Singapore Pte. Ltd.

[2019] SGPDPC 26

Tan Kiat How, Commissioner — Case No DP-1809-B2684

Data protection – Protection obligation – Disclosure of personal data – Insufficient security arrangements

Data protection – Personal obligation – Higher standard of protection needed to protect sensitive personal data

22 July 2019.

Background

1 On 7 September 2018, Genki Sushi Singapore Pte. Ltd. (the "**Organisation**") notified the Personal Data Protection Commission (the "**Commission**") that a server on the Organisation's network which stored the personal data of its employees, among other information, had been the target of a ransomware attack. This attack resulted in the unauthorised encryption of the employee personal data hosted on that server and the Organisation being subjected to a ransom demand (the "**Incident**"). The Commission commenced an investigation in order to determine whether the Organisation had failed to comply with its obligations under the Personal Data Protection Act 2012 (the "**PDPA**").

Material Facts

2 The Organisation is a sushi chain restaurant. As part of its internal operations, it used an off-the-shelf payroll software application, "TimeSoft", which was developed and licensed to it by Times Software Pte Ltd ("**Times**"). The TimeSoft application included a web portal and a database. The web portal was used by (a) employees to view their electronic payslips and (b) supervisors at the various restaurants to confirm the attendance of their employees during the designated hours. The database contained the personal data of the Organisation's former and current employees ("**Employee Data Files**"). The TimeSoft application was hosted on a local server belonging to the Organisation (the "**Server**"). The Server also contained financial data files (*e.g.* financial statements and details on the Organisation's dealings with its vendors).

3 On 30 August 2018, the Organisation's IT personnel discovered that the Server was unresponsive. Following internal investigations, the Organisation confirmed that the Server had been subjected to a ransomware attack, resulting in most of its hosted files (including the Employee Data Files) being encrypted with a ".bip" extension and their contents being inaccessible to the Organisation. A ransom payment was demanded from the Organisation in exchange for the decryption key. Based on its investigations, the Organisation suspected that the Server was infected by the "Dharma" variant of ransomware that had been installed on the Server through its internet link.

4 The Incident resulted in the unauthorised modification of the Organisation's data (including the Employee Data Files) as the encryption by

the ransomware replaced the original plaintext with ciphertext (which was unreadable without the proper cipher to decrypt it). The following types of personal data belonging to approximately 360 current and former employees of the Organisation were affected by the unauthorised modification:

(a) name;

(b) NRIC number, if the employee was a Singaporean;

(c) Foreign Identity Number ("**FIN**") and application date, if the employee was a foreigner;

(d) bank account information, i.e., bank and branch information;

(e) gender;

(f) marital status;

(g) date of hire;

(h) date of birth; and

(i) salary details.

5 The Incident also affected the following types of personal data for some of the Organisation's current or former employees (who had these types of data stored in the Server):

(a) passport number;

(b) address;

(c) telephone number;

(d) mobile phone number;

(e) names of relatives;

(f) emergency contact person's name and relationship with the employee; and

(g) country of birth.

6 There was no evidence of the encrypted personal data files being subjected to exfiltration or unauthorised disclosure.

7 Upon discovery of the Incident, the Organisation immediately took the following steps to contain and mitigate the effects of the Incident:

(a) isolated the Server from its larger IT network;

(b) performed anti-virus scans on each computer in the Organisation's office and restaurants;

(c) attempted, albeit unsuccessfully, to remove the ransomware and decrypt the infected data files using third party security tools; and

(d) to the best of its ability, notified its affected employees of the Incident. In this regard, all full-time employees and most part-time employees were notified by 7 September 2018. The Organisation was unable to notify its affected former employees due to their contact details being encrypted by the ransomware.

8 The Organisation subsequently also took the following steps to prevent the recurrence of the Incident:

(a) replaced the Server with a new server that was isolated in a "de-militarised zone" within the Organisation's IT network;

(b) introduced the following safeguards to protect the personal data in the new server:

(i) encrypting the TimeSoft application's database;

(ii) setting the server's firewall security policy to allow traffic only via Hyper Text Transfer Protocol Secure or through required service ports;

(iii) enabling an intrusion prevention system on the firewall;

(iv) installing TrendMicro OfficeScan XS anti-virus software on the new server, with the intent of subsequently upgrading this software to TrendMicro Deep Security after improvements to the Organisation's overall enterprise IT structure are completed;

(v) enabling audit logging on the new server;

(c) engaged an external vendor to provide security operation centre services, whereby the vendor would monitor the network and

server logs and look out for any potential malicious activities on the new server; and

(d) engaged an IT security vendor to assist with updating the Server's operating system, managing patches for the Server, and conducting regular IT vulnerability assessments.

Findings and Basis for Determination

9 The main issue for determination is whether the Organisation breached section 24 of the PDPA. 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.

10 As a preliminary point, it is noted that, during the material time, the Organisation was responsible for the maintenance of the Server, while Times was in charge of providing technical support for the TimeSoft application, such as maintaining its web portal and database, as well as troubleshooting the application. Times provided its technical support on an ad hoc basis via remote access granted by the Organisation. During this process, the Organisation's IT personnel would supervise the activities of Times to ensure that there was no unauthorised access to, or collection of, the personal data hosted on the Server. Accordingly, Times did not have any control or possession of the personal data hosted on the Server. In any event, the Incident did not relate to the scope of Times' services rendered to the Organisation. As such, the Commissioner found that only the Organisation was in possession and control of the personal data, including the Employee Data Files, hosted on the Server during the material

time.

11 To determine whether the Organisation was in breach of section 24, the relevant question is whether it had put in place reasonable security arrangements to safeguard the personal data hosted on the Server. The Commission's Advisory Guidelines on Key Concepts in the PDPA (revised 27 July 2017) (at [17.2]) provide the following examples of factors that are taken into consideration in assessing the reasonableness of an organisation's security arrangements:

(a) the nature of the personal data;

(b) the form in which the personal data has been collected (*e.g.* physical or electronic); and

(c) the possible impact to the individual concerned if an unauthorised person obtained, modified or disposed of the personal data.

12 In assessing the security arrangements adopted by the Organisation, the Commissioner considered that the Employee Data Files included sensitive personal data in the form of NRIC numbers, FINs, passport numbers, bank account details and salary details. In this regard, it bears repeating what was stated in *Re Aviva Ltd* [2018] SGPDPC 4 at [17]:

> "All forms or categories of personal data are not equal; organisations need to take into account the sensitivity of the personal data that they handle. In this regard, the Commissioner repeats the explanation in *Re Aviva Ltd* [2017] (at [18]) on the

higher standards of protection that should be implemented for sensitive personal data:

> The Advisory Guidelines on Key Concepts in the PDPA states that an organisation should "implement robust policies and procedures for ensuring appropriate levels of security for personal data of varying levels of sensitivity". **This means that a higher standard of protection is required for more sensitive personal data. More sensitive personal data, such as insurance, medical and financial data, should be accorded a commensurate level of protection.** In addition, the Guide to Preventing Accidental Disclosure When Processing and Sending Personal Data expressly states that documents that contain sensitive personal data should be "processed and sent with particular care"."

[Emphasis added.]

13 It should also be borne in mind that NRIC numbers are of special concern as they are "*a permanent and irreplaceable identifier which can be used to unlock large amounts of information relating to the individual*" (*Re Habitat for Humanity Singapore Ltd* [2018] SGPDPC 9 at [19])

14 The standard of security arrangements expected in relation to IT systems was elaborated upon in *Re The Cellar Door Pte Ltd and Global Interactive Works Pte Ltd* [2016] SGPDPC 22 ("***Re The Cellar Door***") at [29]; "reasonable security arrangements" for IT systems must be sufficiently robust and comprehensive to guard against a possible intrusion or attack:

> "Another important aspect of a "reasonable security arrangement" for IT systems is that **it must be sufficiently robust and comprehensive to guard against a possible**

> **intrusion or attack**. For example, it is not enough for an IT system to have strong firewalls if there is a weak administrative password which an intruder can "guess" to enter the system. The nature of such systems require there to be sufficient coverage and an adequate level of protection of the security measures that are put in place, since a single point of entry is all an intruder needs to gain access to the personal data held on a system. In other words, **an organisation needs to have an "all-round" security of its system. This is not to say that the security measures or the coverage need to be "perfect", but only requires that such arrangements be "reasonable" in the circumstances.**"
>
> [Emphasis added.]

15 In this case, the Organisation had failed to put in such "all-round" security of its system which is accessible via the Internet by all of its branches, and which contained sensitive personal data of its employees, e.g. NRIC/FIN and passport numbers, bank account details. The Commission's investigations revealed the following significant gaps in the security measures implemented in relation to the Server during the Incident:

(a) first, the Organisation initially did not have a firewall for the Server and, even after a firewall had been installed following its recent IT migration pursuant to its business re-organisation, it failed to configure the Server's firewall to filter out unauthorised traffic and close unused ports;

(b) second, the Organisation did not conduct periodic penetration tests to assess the overall security of its IT infrastructure and bolster the effectiveness of its defensive mechanisms and

determine what measures (including patches) may be required to fix vulnerabilities; and

(c) Third, the Organisation failed to ensure that the Server and the TimeSoft application were regularly patched.

16 As regards the failure in paragraph 15(a), although the Server was kept in a secure physical location with physical access only granted to authorised personnel, the same level of precaution had not been implemented for virtual or remote access. There was no firewall for a while, and even when installed, the Server's firewall was not configured to block any unused ports or unauthorised traffic at all material times. In other words, the Server's firewall was ineffective at filtering out any external threats.

17 In its response to the Commission's queries, the Organisation had explained that the lack of configuration for the firewall was because the Organisation had recently undergone a full IT migration and its IT team was waiting for the IT infrastructure to be refreshed before configuring the appropriate firewall settings. Pending this refresh, it had not configured any firewall setting as the Organisation did not have any server firewall before the IT migration and therefore no pre-existing configuration it could use for the firewall in the interim period. Thus, there was effectively no firewall in place during the relevant period.

18 The Commissioner reiterates what was said in *Re The Cellar Door* (at [30(a)] and [30(b)]) that "*a firewall is* ***fundamental*** *to the security of the server to protect against an array of external cyber threats*" and "*leaving unused ports on a server open increases the risk of an external hacker exploiting the services*

running on these ports". In this case, the firewall was not configured to close *any* ports.

19 As regards the failures in paragraphs 15(b) and 15(c), the Organisation admitted that it did not conduct any penetration tests on the Server within the last 12 months prior to the Incident. The Organisation was also unable to provide evidence that it had done any patching on the Server during the same period. This suggests that the Organisation did not have any processes in place to ensure regular security testing and patching of its IT systems.

20 The Commissioner emphasises that regular security testing and patching are important security measures. 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. Moreover, as stated in the Commission's Guide to Securing Personal Data in Electronic Medium (revised 20 January 2017) at [16.3] and [16.4]:

> "Vulnerabilities discovered [in software] are often published, hence cyber attackers are well aware of vulnerabilities available for exploiting.
>
> It is therefore important for organisations to keep their software updated or patched regularly to minimise their vulnerabilities."

21 Generally, organisations should, to the extent possible, test and apply updates and security patches as soon as they are available to the relevant components (*e.g.* network devices, servers, database products, operating systems, applications, software libraries, programming frameworks and firmware) of the Organisation's IT system. There should also be processes and people responsible to monitor new patches and updates that become available

with respect to such components. In this regard, the arrangement with Times for maintenance and technical support of the TimeSoft application was inadequate.

22 The failures highlighted above contributed to a system that had a number of vulnerabilities and gaps that a hacker could easily exploit. In this case, the ransomware may have successfully exploited these gaps to reach the Employee Data Files and the other files on the Server. For a server that held sensitive personal data, the security measures implemented by the Organisation were inadequate. In fact, the standard of protection provided was not even sufficient for non-sensitive personal data.

23 For the reasons above, the Commissioner finds the Organisation in breach of section 24 of the PDPA.

Representations by the Organisation

24 In the course of settling this decision, the Organisation made representations on the amount of financial penalty which the Commissioner intended to impose. The Organisation raised the following factors for the Commissioner's consideration:

(a) There was no evidence that the personal data had been subjected to exfiltration, unauthorised disclosure or modification;

(b) The Organisation did not pay the ransom amount to positively discourage and disincentivise unauthorised and criminal behaviour by the ransomware attacker; and

(c) The Incident occurred during the period where the Organisation's new management was in the midst of the IT migration and the strengthening of the IT infrastructure.

25 The Commissioner has decided to maintain the financial penalty set out at [29] for the following reasons:

(a) As explained at [4], there had been unauthorised modification to personal data belonging to approximately 360 current and former employees of the Organisation. In determining the quantum of financial penalty, the Commissioner had already taken into consideration that there was no evidence of the encrypted Employee Data Files being subjected to exfiltration or unauthorised disclosure.

(b) Notwithstanding that there was criminal activity on the part of the ransomware attacker, the finding of section 24 breach relates to the Organisation's own failings to put in place reasonable security measures. As such, whether the ransom amount is paid is not a mitigating factor.

(c) A transition to a new management team does not lower the standard expected of an organisation to protect personal data in its possession and/or control. Notwithstanding that the Organisation was in the midst of IT migration and strengthening of IT infrastructure, it was obliged to put in place reasonable security measures to protect the Employee Data Files at all times. These are therefore not mitigating factors. In any event, as stated at [15], the Commission's investigations revealed that the

Organisation did not have adequate security measures in place for the Server even before the IT migration.

The Commissioner's Directions

26 Given the Commissioner's findings that the Organisation is in breach of section 24 of the PDPA, the Commissioner is empowered under section 29 of the PDPA to issue the Organisation such directions as he deems fit to ensure its compliance with the PDPA. This may include directing the Organisation to pay a financial penalty of such amount not exceeding $1 million.

27 In determining the directions, if any, to be imposed on the Organisation in this case, the Commissioner took into account the following mitigating factors:

(a) the Organisation voluntarily notified the Commission of the breach;

(b) the Organisation fully cooperated with the Commission's investigations; and

(c) the Organisation took prompt action to mitigate the effects of the breach.

28 The Commissioner also took into account, as an aggravating factor, that the failure to make reasonable security arrangements to protect the personal data led to a loss of control over the Employee Data Files, which contained sensitive

personal data.

29 Taking into account the above mitigating and aggravating factors, 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.

30 The Commissioner has not set out any further directions for the Organisation given the remediation measures already put in place.

YEONG ZEE KIN
DEPUTY COMMISSIONER
FOR PERSONAL DATA PROTECTION