PERSONAL DATA PROTECTION COMMISSION

[2021] SGPDPC 4

Cases No DP-1912-B5434 / DP-1912-B5564 / DP-1912-B5558

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

And

HMI Institute of Health Sciences Pte. Ltd.

… *Organisation*

DECISION

HMI Institute of Health Sciences Pte. Ltd.

[2021] SGPDPC 4

Lew Chuen Hong, Commissioner — Cases No. DP-1912-B5434 / DP-1912-B5564 / DP-1912-B5558

20 May 2021

Introduction

1 On 4 December 2019, a file server (the "**Server**") belonging to HMI Institute of Health Sciences Pte. Ltd. (the "**Organisation**") was affected by a ransomware attack. The ransomware encrypted and denied access to various files on the Server, including files containing personal data of the Organisation's staff and trainees (the "**Incident**").

2 On 7 December 2019, the Organisation informed the Personal Data Protection Commission ("**Commission**") of the Incident. The Commission subsequently received two separate complaints about the Incident.

Background

3 The Organisation is a dedicated private provider of healthcare training to individuals ("**Participants**") in Singapore. In the course of carrying out its business activities, the Organisation collects personal data from, among others, (i) its employees, including temporary and contract staff such as associate trainers, ("**Employees**") for the purposes of managing or terminating such employment relationships, and (ii) the Participants, for the purposes of registration and the administration of their enrolment in the Organisation's training courses.

4 The Server affected by ransomware was set up in 2014 and was located in Singapore. It was owned by the Organisation but maintained by the Organisation's appointed IT solution service provider (the "**Vendor**"). The Server stored personal data in Microsoft Word or Excel files, most but not all of which were password-protected.

5 The Server was protected by a firewall that blocked all connections to the Server, except for those through port 3389, a standard port which was used for the Remote Desktop Protocol ("**RDP Port**"). The RDP Port was used by the Vendor for

remote management and/or troubleshooting purposes. According to the Organisation, the RDP Port was kept open from sometime in 2014 up to the date of the Incident on 4 December 2019 (i.e. for more than four (4) years) to allow the Vendor quick and easy access. The significance of the RDP Port being kept open will be elaborated on below.

6 The Server only had one administrator account which was shared by the Organisation's IT administrator and at least three other employees of the Vendor. By use of this administrator account, the Vendor could access the Server remotely through the RDP Port and view, change, or delete all the data in the Server.

7 On 4 December 2019, an employee of the Organisation was unable to access files on the Server containing the personal data of some Participants. An initial diagnostic conducted by the Vendor revealed that the Server had been affected by ransomware. File extensions of the files on the Server had been changed and a ransom note was found on the Server.

8 On 5 December 2019, the Organisation engaged a cybersecurity expert company ("**CSE**") to conduct a thorough assessment of the Incident. The CSE found that:

(a) the attacker had likely discovered the open RDP Port following a random, opportunistic search for vulnerabilities; and;

(b) having discovered the open RDP Port, it was likely that the attacker used brute force attacks to obtain the administrator account password for the Server in order to gain access to the Server and execute the ransomware.

9 In total, the personal data of approximately 110,080 Participants, and 253 Employees were affected by the Incident (the "**Affected Personal Data**").

10 For the affected Participants, the following categories of personal data were affected:

(a) Name;

(b) NRIC number;

(c) Address;

(d) Race;

(e) Gender;

(f) Date of Birth;

(g) Age;

(h) Email address;

(i) Contact number;

(j) Course details;

(k) Nationality; and

(l) Employer details and past employment history.

11 For the affected Employees, the following categories of personal data were affected:

(a) Name;

(b) NRIC number;

(c) Date of Birth;

(d) Nationality;

(e) Citizenship;

(f) Age;

(g) Contact number;

(h) Vehicle licence plate; and

(i) Financial Information (including salary/payment information, Central Provident Fund ("**CPF**") information, and bank account numbers.

12 Not all of the above categories of personal data were affected in every individual's case. For instance, the bulk of the affected Participants (approximately 98,000) only had their names and NRIC numbers stored on the Server.

13 The CSE's investigation found no evidence of any exfiltration of the Affected Personal Data from the Server. The Organisation also managed to retrieve all the Affected Personal Data as most of the affected files were back-up files.

14 Upon being made aware of the Incident, the Organisation took prompt remedial actions. The Organisation:

(a) Decommissioned the Server (without paying the ransom), and isolated the Server from its network and the Internet;

(b) Notified the Commission, SingCERT, and all the affected Employees and Participants that it was able to (approximately 95%) of the Incident; and

(c) Issued a media advisory on the Incident.

15 The Organisation also carried out actions to prevent a recurrence of the Incident. It:

(a) Adopted its own internal password management policy;

(b) Permanently disconnected and blocked remote access for IT support procedures;

(c) Implemented Internet separation measures for all devices containing personal data;

(d) Introduced various endpoint enhancements and gateway security measures including a monitoring system for all Internet-facing traffic, a suite of antivirus and malware protection for all computers and enhancing email hosting security protection and hard disk encryption;

(e) Engaged external IT security consultants to establish an Information Security Management Framework based on the ISO 27001 certification;

(f) Conducted cybersecurity training sessions and cybersecurity awareness workshops for its staff;

(g) Conducted ad-hoc email phishing tests to augment the cybersecurity training sessions and to engender greater awareness and vigilance towards suspicious emails; and

(h) Put in place a monthly IT bulletin post to all employees to keep all staff up to date on IT and cybersecurity issues.

Findings and Basis for Determination

Whether the Organisation had contravened section 24 of the PDPA

16 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 ("**Protection Obligation**").

17 As a preliminary point, even though the Organisation had engaged the Vendor to maintain the Server and the Organisation's other IT infrastructure, the scope of the Vendor's engagement did not involve the processing or handling of any personal data on behalf of the Organisation. The Organisation owned the Server and was in possession and control of the Affected Personal Data at all material times. The Vendor was therefore not a data intermediary and the responsibility to protect the Affected Personal Data fell squarely on the Organisation.

18 For the reasons set out below, the Organisation failed to implement reasonable security arrangements to protect the Affected Personal Data from the risk of authorised access, modification and disposal.

Failure to adequately regulate remote access to the Server

19 First, the Organisation did not have sufficiently robust processes to ensure safe remote access to the Server via the RDP Port. The Remote Desktop Protocol (i.e., RDP) is a proprietary protocol developed by Microsoft Corporation for use in its Remote Desktop Connection application, which allows for remote connections to be established from one computer (i.e., a server) to another computer (i.e., the client) allowing the client to remotely control the server. By default, the server uses port number 3389 (i.e., the RDP Port) for incoming connections and requires authentication in the form of a username and password, before access to the server is granted. While the RDP Port is intended to be used for legitimate RDP client-server connections, its existence is well known and thus susceptible to be exploited by malicious actors to gain unauthorised access to a server if there are weak protective measures in place (e.g. weak user authentication).

20 While there is no strict requirement that the RDP Port must always be closed, organisations should regularly review and assess the potential risks of keeping such public facing ports open. Where it is necessary to keep the RDP Port on a server open, organisations should ensure that there are sufficient measures in place to protect the personal data stored on the server.

21 That said, where an organisation holds a high volume of personal data and/or highly sensitive personal data, the Commission is of the view that the default approach should be to close all ports, including RDP Ports. Where it is necessary to open the RDP Port, organisations must ensure that there are sufficient measures in place to ensure the security and legitimacy of any incoming RDP connection, and to promptly close the RDP Port upon completion of the required use. Additional measures to secure the files, for example, access control to folders and file encryption, may also be deployed. These are different layers of defences that can be used cumulatively or in different combination, depending on the volume and sensitivity of personal data and the requirements of business operations.

22 In this case, the Organisation kept the RDP Port open from the time the Server was set up in 2014 until the occurrence of the Incident on 4 December 2019. According

to the Organisation, the RDP Port was kept open to allow the Vendor quick remote access to the Server for recovery and maintenance works. The Organisation claimed that keeping the RDP Port permanently closed was not practicable, as half a day of down time would be required whenever the RDP Port needed to be opened or closed.

23 Given the fact that a minority of records (i.e. 253 Employees) contained more sensitive financial information and bank account numbers, as well as the volume of personal data stored on the Server, it is questionable whether the RDP Port should have been kept open *permanently* for recovery or maintenance work. Even if this meant incurring some down time in activating and deactivating the firewall for the RDP Port, the inconvenience associated with this down time should have been measured against the risk to the type and volume of personal data that was stored on the Server. Nonetheless, the benefit of doubt is given to the Organisation as the majority of records were personal particulars and contact information.

24 Even if it was necessary for the RDP Port to be kept open, the Organisation should at least have put in place other types of technical measures to secure the RDP access, such as:

(a) Using a different port (other than the default port 3389) for RDP connections;

(b) Restricting access to specific IP addresses or IP addresses within specified ranges, i.e. "whitelisting";

(c) using a RDP gateway; and/or

(d) Conducting log reviews for unusual activity, whether upon automated alerts or scheduled monitoring.

25 The risks arising from poor management of RDP Ports have also been highlighted in the Cyber Security Agency of Singapore's ("**CSA**") recent advisory dated 28 December 2020, titled "*Protect Your Systems and Data From Ransomware Attacks*" [1] . The CSA similarly cautioned that some ransomware variants take

[1] https://www.csa.gov.sg/singcert/advisories/ad-2020-006

advantage of exposed services and open ports such as the RDP Port to spread across a network. As such, in order to minimise the chance of a ransomware attack, the CSA emphasised that organisations should review their port settings, particularly, to assess whether there was a need to leave the RDP Port exposed, and if so, to restrict RDP connections to only trusted hosts.

26 The Organisation represented to the Commission that it would have been impractical to whitelist specific IP addresses as connections to the Server were generally made through dynamic, instead of static, IP addresses. Even so, the onus remained on the Organisation to put in place alternative security measures that were commensurate with the standard of protection required to protect sensitive data stored on the Server. However, the Organisation failed to implement any such alternative security measures.

27 The Organisation's inaction on this front placed the Server at risk for more than **four years** - from the time the Server was set up in 2014 until it was disconnected from the Internet after the Incident.

Failure to implement proper password management

28 Second, the Organisation failed to implement proper password management policies. The Organisation had adopted and generally directed its staff to follow the password policy of one of its affiliates (the "**Password Policy**"). The guidelines and standards in the Password Policy are consistent with the Commission's recommendations in its *Guide to Securing Personal Data in Electronic Medium*[2], which recommends that passwords used for authentication have a length of at least 8 characters, containing at least one alphabetical character and one numeric character.

29 However, the Organisation failed to take steps to ensure that the Password Policy was compiled with in practice. None of the passwords used by the Organisation for the administrator account of the Server or the files containing the Affected Personal Data (including those containing financial information) met the Password Policy's recommended complexity rules. The passwords used by the Organisation also

[2] https://www.pdpc.gov.sg/help-and-resources/2017/10/guide-to-securing-personal-data-in-electronic-medium

incorporated an acronym of the organisation's name, which made them easy to guess and vulnerable to brute force attacks.

30 As noted in *Re Chizzle Pte Ltd* [2020] SGPDPCR 1 at [5(d)]:

> "*In this regard, various articles/guides have stated that the* ***use of an organisation's name as a component of the password is not recommended*** *because it is not difficult to guess and cracked by hackers. The digits "2018" as a component of the password was also guessable, for example, through brute force or dictionary attacks. As such, the password used by the Organisation failed to prevent unauthorised copying and deletion of the Chizzle Database.*"
>
> [Emphasis added]

31 The login credentials for the administrator account on the Server were also shared between one administrator in the Organisation and at least three other individuals in the Vendor. Other than the login credentials, there were no other access controls to the administrator account (e.g. 2FA or anti-hammering features). As previously stated in *Re Orchard Turn Developments Pte Ltd* [2017] SGPDPC 12 (at [31]) user accounts should generally not be shared between different individuals, and all the more so for administrator accounts:

> "*Additionally,* ***there should not be a sharing of credentials amongst users****. When credentials are shared among multiple users, it is* ***difficult to ensure accountability*** *as it is* ***difficult to track the activity of each individual*** *using the common set of credentials.*"
>
> [Emphasis added]

32 Although the sharing of the administrator account credentials was not a direct contributing factor to the Incident, the sharing of account credentials – in particular, administrator accounts with high privileges – created an additional risk factor which could have diminished the robustness of other security measures put in place by the Organisation.

33 Similarly, while strong passwords may only slow but not entirely deter threat actors, the absence of strong passwords could greatly facilitate unauthorised access to IT systems, including IT systems holding personal data.

Failure to take reasonable steps to ensure that the Vendor would protect personal data

34 Thirdly, while the Organisation claims to have relied on the Vendor's technical expertise with regard to the security of the Server, the Organisation did not take reasonable or sufficient steps to stipulate clear requirements of its Vendor to ensure that the Vendor understood its role in the protection of the personal data in the Server.

35 As mentioned in the Commission's *Guide to Managing Data Intermediaries*[3]:

> "*The primary means by which a DC* (i.e. a Data Controller) *may ensure appropriate protection and retention of the personal data processed by its DI* (i.e. a Data Intermediary) *is through a contract. As the range of data processing activities that can potentially be outsourced is very broad, it is necessary for the scope of outsourced data processing activities to be clearly defined and agreed upon. There should be clear communication between the DC and the DI on the scope of outsourced data processing activities and the personal data requirements. For the DC, this is crucial in ensuring that its business requirements and management decisions in relation to the outsourcing are made clear to the DI.*"

36 The Vendor in this case was not a Data Intermediary. However, the Vendor was nevertheless expected to handle personal data in the course of its work or make decisions which affected the security of personal data stored in the Server[4]. As such, in order for the Organisation to say that it had discharged its Protection Obligation by relying on the Vendor's technical expertise, clear business requirements on the protection of the data in the Server should have been specified. Alternatively, the Vendor could have made recommendations on the data protection requirements based on its understanding of the engagement (including for protection of the data in the Server), which the Organisation could have approved and adopted. In either case,

[3] https://www.pdpc.gov.sg/Help-and-Resources/2020/09/Guide-to-Managing-Data-Intermediaries
[4] See *Civil Service Club* [2020] SGPDPC 15 at [13] and [14]

reasonable efforts should have been taken by the Organisation to verify that the Vendor was meeting its data protection requirements.

37 The exact requirements for a given case would depend on the services that a vendor is engaged to provide. If a vendor is engaged to put in place protection features for a Data Controller's IT systems, the business requirements should describe the risks that the vendor is to address. In this case, the Organisation's contract with the Vendor did not specify any business requirements for the protection of personal data in the Server. Neither could the Organisation provide any evidence to suggest that the Vendor made any recommendations about how to protect the data in the Server. As such, the Organisation could not say that it had discharged its Protection Obligation by relying on the expertise of the Vendor.

38 In the circumstances, the Commissioner finds that the Organisation failed to make reasonable security arrangements to protect the personal data in the Server from the risk of unauthorised access, modification and disposal. Accordingly, the Commissioner finds the Organisation in breach of its obligation under section 24 of the PDPA.

The Commissioner's Directions

39 In determining whether any directions should be imposed on the Organisation under section 48I of the PDPA, and/or whether the Organisation should be required to pay a financial penalty under section 48J of the PDPA, the factors listed at section 48J(6) of the PDPA and the following aggravating and mitigating factors were taken into account:

Aggravating Factor

(a) the Organisation's failure to put in place reasonable security measures put the personal data in the Organisation's possession and/or control at risk of exposure for more than four years. The failure to protect led to the unauthorised access and modification of the personal data in the Incident;

Mitigating Factors

(b) the Organisation took prompt remedial actions following the Incident; and

(c) the Organisation was cooperative during the investigations.

40 Having considered all the relevant factors of this case, including representations made by the Organisation on 1 April 2021 after being notified of the Commissioner's Preliminary Decision, the Commissioner hereby directs the Organisation to pay a financial penalty of $35,000 within 30 days from the date of the relevant notice, 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.

41 In view of the remedial actions that have already been taken by the Organisation, no other directions are necessary.

YEONG ZEE KIN
DEPUTY COMMISSIONER
FOR COMMISSIONER FOR PERSONAL DATA PROTECTION