PERSONAL DATA PROTECTION COMMISSION

[2023] SGPDPC 4

Case No. DP-2102-B7850

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

And

The Law Society of Singapore

… *Organisation*

DECISION

Data Protection *– Protection obligation – Unauthorised access to personal data – Third-party software not patched - No breach –Reasonable oversight exercised over IT vendor*

Data Protection *– Protection obligation – Insufficient security arrangements - Weak password - Failure to conduct reasonable periodic security review*

The Law Society of Singapore

[2023] SGPDPC 4

Yeong Zee Kin, Deputy Commissioner — Case No. DP-2102-B7850

14 March 2023

Introduction

1 On 4 February 2021, the Law Society of Singapore (the "**Organisation**") notified the Personal Data Protection Commission (the "**Commission**") of a ransomware attack on its servers which had encrypted and denied the Organisation access to the personal data of its members and former members (the "**Incident**"). The Commission commenced investigations to determine whether the circumstances behind the Incident disclosed any breaches by the Organisation of the Personal Data Protection Act 2012 ("**PDPA**").

Facts of the Case

2 The Organisation is a body corporate established under the Legal Profession Act 1966 and represents members of the legal profession in Singapore. Every advocate and solicitor called to the Singapore bar is a statutory member of the Organisation as long as they have a practising certificate in force. At the material time, the Organisation stored the personal data of its current and former members ("**Members**") in one of its servers for the purposes of carrying out its statutory functions.

3 The Organisation had implemented an off-the-shelf secure VPN solution, FortiOS, to manage remote access to its servers (the "**VPN System**"). The Organisation also engaged a vendor (the "**Vendor**") to provide IT support services, including maintenance of the VPN

System. For completeness, the Vendor was not the Organisation's data intermediary as it did not access or process the personal data of the Members in the course of carrying out its IT support services.

4 The Organisation also implemented antivirus / malware detection software at the servers, and password complexity requirements for its users' accounts. In particular, account passwords had a maximum lifespan of 3 months before a compulsory change was required.

5 Additionally, the Organisation had in place a written data protection policy and conducted data protection training for its staff highlighting cybersecurity threats such as phishing and ransomware. Periodic emails on data protection awareness and reminders were also sent to staff.

The Incident

6 On 27 January 2021, a threat actor gained access to the account of the Organisation's IT administrator ("**compromised admin account**") and used this to create a new account with full administrative privileges. Using this new account, the threat actor moved through the Organisation's network without detection and located the Organisation's servers. The threat actor then executed a ransomware attack on the servers, encrypting their contents.

7 A total of 16,009 Members' personal data was affected in the Incident, including each Member's full name, residential address, date of birth, and NRIC number. Other data items were also affected but they are either in the nature of business contact information or publicly available information.

8 The attack was detected on the same day by antivirus / malware detection software deployed by the Organisation. The Organisation took immediate steps to remove the new administrator account created by the threat actor and restored the servers to their original state from secured back-ups.

Remedial actions

9 Following the Incident, the Organisation also took the following remedial actions:

(a) Removed unused administrator accounts and initiated password resets for all administrator accounts;

(b) Reduced privileged access for the compromised admin account (to create new administrator accounts);

(c) Hired an in-house cybersecurity professional to take charge of the Organisation's IT security matters;

(d) Implemented multi-factor authentication ("**MFA**") for all VPN access; and

(e) Implemented VPN IP location whitelisting to allow only Singapore-based IP addresses.

Findings and Basis for Determination

10 The Commission's investigation centred on whether the Organisation had breached its obligation 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**"). As the Vendor was not the Organisation's data intermediary, the Protection Obligation in this case was borne solely by the Organisation.

Findings from the investigations

11 Investigations disclosed that there could have been multiple threat actors targeting the Organisation or the same group of threat actors targeting the Organisation through multiple channels – through brute force attacks, phishing email, and exploiting the unpatched VPN vulnerability of the VPN System.

12 **Brute-force attacks.** Around ten days before the Incident, multiple unsuccessful login attempts using a "guest" account were found since 18 January 2021. There were also further unsuccessful attempts made using random accounts. However, investigations did not surface evidence that the initial entry by the threat actor had been via a successful brute force attack on the compromised admin account.

13 **Phishing emails.** Investigations also revealed that the Organisation was attacked by the Netwalker ransomware, most commonly introduced via phishing emails. From the Vendor's explanations, the administrator of the compromised admin account could have received a phishing email with a link and entered his credentials. However, investigations did not surface evidence of any phishing email relevant to this ransomware; neither was there evidence that the compromised admin account's credentials was obtained by a threat actor through phishing.

14 **Vulnerability of the VPN System.** At the material time before the Incident, MFA was not implemented for the Organisation's administrator access to its servers. This meant that once authenticated, an admin user had rights to create new accounts, assign privileged security groups, and access all of the Organisation's servers without the need for a second factor.

15 Investigations revealed that there was a vulnerability in the VPN System which could be exploited to gain access credentials if left unpatched (the "**Vulnerability**"). This was assessed to be a possible way in which the threat actor obtained the credentials of the compromised admin account:

(a) Around November 2020, a file containing more than 45,000 session links and IP addresses for the VPN System of affected organisations (including the Organisation) was found posted in online forums by someone who had obtained the information by exploiting the Vulnerability.

(b) Without patching the VPN System's firmware, each session link would disclose the credentials of users in plain text, including passwords.

(c) The date/time of the online publication (i.e. November 2020) was sufficiently proximate to the threat actor's successful intrusion in January 2021 using the compromised admin account.

16 From the foregoing, it would appear that of the three possible attack vectors, the vulnerability in the VPN System could have given the threat actor entry into the Organisation's environment.

No breach of the Protection Obligation for omission to patch the Vulnerability

17 The developer of the VPN System, Fortinet, had disclosed the Vulnerability as early as 24 May 2019. It released an Operating System ("**OS**") upgrade to remedy the issue, which contained the updates to remedy the issue. The VPN System had a user interface ("**UI**") through which the OS upgrade availability could be notified. According to the Vendor, the Vendor had regularly checked the UI if OS upgrades were available but there were no prompts of updates available for download prior to the Incident. According to the Organisation, it was only after it

communicated the issue to the developer, after the incident, that the UI subsequently prompted availability of some patches that included the OS upgrade remedying the Vulnerability.

18 The Commission recognises that organisations may rely on vendors engaged to provide IT security maintenance to obtain and apply needed software upgrades and patches. If so, the Protection Obligation requires organisations to stipulate such requirements clearly in writing as part of the job specifications of such vendors. In this case, patching of the VPN System had been a specific obligation explicitly outsourced by the Organisation to the Vendor via contract.

19 In addition to clearly stipulating the vendor's scope of IT maintenance and/or development work, organisations are expected to exercise reasonable oversight over the vendor's performance of the subcontracted services, including patching – *Re Smiling Orchard (S) Pte Ltd and Ors* [2016] SGPDPC 19[1]. There should be a clear meeting of minds as to the services the service provider has agreed to undertake and organisations must *follow through with procedures* to check that the outsourced provider is delivering the services.

20 The Commission appreciates that the technical nature of information on software patching and upgrades limits the degree of oversight that many organisations can exercise on vendor performance in this regard. The Commission notes that the Organisation had put in place a process to ensure that there were maintenance logs in respect of the Vendor's activities. Thus, the Organisation, to its credit, had put in place a system to monitor its Vendor's activities. In technical areas where the Organisation depends on its Vendor's technical expertise, this is reasonably adequate. The situation may be different if there was a very well-publicised issue

[1] See also *Singapore Health Services Pte. Ltd and Integrated Health Information Systems Pte Ltd* [2019] SGPDPC 3.

with a well-known commercial solution (e.g. vulnerabilities affecting a network router) that the Organisation ought to know that it uses. In such situations, the Organisation might be at least expected to query its Vendor about whether it is exposed and ask for a remediation plan. But this is probably limited to well-known and well-publicised issues in mass media.

21 Carefully weighing the above circumstances, the Commission has decided that: (a) it had been reasonable for the Organisation to rely on the Vendor to perform software security patching, including of the Vulnerability, and (b) that the Organisation had in this case discharged its duty of oversight of the Vendor's patching function. Therefore the Organisation has not breached the Protection Obligation.

Breach of the Protection Obligation by the Organisation in other aspects

22 Investigations revealed that the password for the compromised admin account was "Welcome2020lawsoc". Despite this password complying with the Organisation's own password complexity rules, the Organisation acknowledged that this was a weak password and vulnerable to dictionary attacks due to the use of a full word and the Organisation's name. As highlighted in *Chizzle Pte Ltd* [2020] SGPDPCR 1, a password that meets complexity rules in form could still be regarded as a weak password if it was easily determined and vulnerable to brute force attacks. In that case, the password "Chi!zzle@2018" incorporated the organisation's name and was determined to be a weak password. Further, the Organisation informed that the compromised admin account's password had been used for more than 90 days and had not been changed every 3 months, as required by the Organisation's password

policy. In the circumstances, the Organisation failed to enforce its password policy in relation to the compromised admin account.

23 In the Commission's recent Guide to Data Protection Practices for ICT systems[2], it has been observed that unauthorised access is one of the most common types of data breaches. This can happen, for example, through the use of a weak password which is easily guessed by hackers. To remediate this, it may be practical to look into implementing processes in ICT systems to minimise risk of brute force attacks (e.g. a pre-defined number of failed login attempts) and ensure information is accessed only by the authorised/authenticated persons performing the intended activities. Additionally, as 2FA or MFA becomes more broadly available, the adoption of these tools should become the norm for accounts with administrative privileges, for systems managing sensitive data or large volumes of personal data[3].

24 Next, the Organisation also did not conduct a review of its security arrangements within the last 3 years prior to the Incident. Regular assurance checks help organisations ensure that ICT security controls developed and configured for the protection of personal data are properly implemented and practised[4]. In *Re WTS Automotive Services Pte Ltd* [2018] SGPDPC 26[5], the Commission emphasised (at [18]) for the need for regular review of security arrangements and tests to detect vulnerabilities.

[2] Published on 14 September 2021, replacing the *Guide to Data Protection by Design for ICT systems* published on 31 May 2019, after the Incident.
[3] See the Commission's recent release of the handbook on common causes of data breaches in *How to Guard against Common Types of Data Breaches* published on 24 May 2021 (at page 13), after the Incident; See *Love Bonito Singapore Pte Ltd* [2022] SGPDPC 3.
[4] See the *Guide to Data Protection Practices for ICT systems*.
[5] See also *Jigyasa* [2020] SGPDPC 9.

25 For the above reasons, the Organisation is found to have negligently breached the Protection Obligation by (i) using an easily guessable password for the compromised admin account, (ii) failing to change the password for the compromised admin account at reasonable intervals, and (iii) failing to conduct any periodic security reviews in the three years leading up to the Incident.

The Deputy Commissioner's Decision

26 Notwithstanding that the Organisation's breaches of the Protection Obligation were not directly related to the Incident, the Commission's role is not limited to investigating only the immediate or proximate causes of a data breach incident[6]. In determining whether directions (if any) should be given to the Organisation pursuant to Section 48I of the PDPA, and/or whether a financial penalty ought to be imposed pursuant to Section 48J of the PDPA, the Deputy Commissioner took into consideration the relevant facts and circumstances of the case, and in particular the following factors:

(a) The Organisation's breaches of the Protection Obligation were not the most proximate cause of the Incident (which was the VPN Vulnerability);

(b) The datasets affected in the Incident were not of a higher sensitivity (e.g. personal data of a financial or medical nature);

(c) The risk of unauthorised access to the Members' personal data was limited due to early detection of the unauthorised access, which also allowed prompt containment and restoration of the servers to its original state;

(d) There was no evidence of any exfiltration or misuse of the personal data of the Members; and

(e) The Organisation took prompt remedial actions in response to the Incident.

[6] See *Love Bonito Singapore Pte Ltd* [2022] SGPDPC 3.

27 For the above reasons, it is adequate for directions to be issued in this case. The Deputy Commissioner hereby directs the Organisation to:

(a) Engage qualified security service providers to conduct a thorough security audit of its technical and administrative arrangements for the security, maintenance, creation and removal of accounts with administrative privileges that can access directly and/or create access to personal data in the possession or control of the Organisation;

(b) Furnish to the Commission within 14 days a schedule stating the scope of the security audit;

(c) Provide the full security audit report to the Commission, by no later than 60 days from the date of the issue of this direction;

(d) Rectify any security gaps identified in the security audit report, review and update its personal data protection policies as applicable, and

(e) Inform the Commission within 1 week of completion of rectification and implementation in response to the security audit report.

YEONG ZEE KIN
DEPUTY COMMISSIONER
FOR PERSONAL DATA PROTECTION