PERSONAL DATA PROTECTION COMMISSION

[2020] SGPDPC 19

Case Nos. DP-1912-B5514 and DP-1912-B5559

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

And

ST Logistics Pte Ltd

… *Organisation*

DECISION

Data Protection *– Protection obligation – Unauthorised access to personal data – Insufficient security arrangements*

ST Logistics Pte Ltd

[2020] SGPDPC 19

Lew Chuen Hong, Commissioner — Case Nos. DP-1912-B5514 and DP-1912-B5559

26 October 2020

Introduction

1 Phishing attacks are increasingly prevalent and are one of the top cybersecurity threats faced by organisations[1]. In its latest report, the Cyber Security Agency of Singapore reported 47,500 cases of phishing in Singapore last year, almost triple the number of cases in 2018[2]. This case is yet another example of an organisation falling victim to phishing.

---

[1]Phishing is a method employed by cyber criminals, often disguising themselves as legitimate individuals or reputable organisations, to fraudulently obtain personal data and other sensitive or confidential information. Once cyber criminals obtain an individual's personal data, they may gain access to the individual's online accounts and may impersonate the individual to scam persons known to the individual. See Cyber Security Agency of Singapore, *Cyber Tip – Spot Signs of Phishing* (25 February 2020) https://www.csa.gov.sg/gosafeonline/go-safe-for-me/homeinternetusers/spot-signs-of-phishing.

[2] See "Phishing attacks last year tripled from 2018", The Straits Times, 27 June 2020.

2 On 16 December 2019, ST Logistics Pte Ltd (the "**Organisation**") notified the Personal Data Protection Commission (the "**Commission**") that the Organisation had detected an Emoted malware ("**Emotet**") in their network which had infected 6 of its users' laptops (including 4 laptops containing personal data), potentially affecting up to 4,000 individuals in the Ministry of Defence ("**MINDEF**") and Singapore Armed Forces ("**SAF**") (the "**Incident**"). Subsequently, on 23 December 2019, the Commission received a complaint from an individual affected by the Incident.

Facts of the Case

3 The Organisation provides logistical services to Singapore's government and defence sectors, as well as commercial sectors. It has more than 800 employees worldwide and an annual revenue of approximately S$350 million[3].

4 On 2 October 2019, the Organisation's users received phishing emails from email addresses with the text "Stlogs" in the sender name field (e.g. "Account Executive (Stlogs)" and "Assistant General Manager (Stlogs)"). Each email contained an attachment with the file extension "doc". A total of 13 users from the Organisation opened the malicious attachment (the "**Affected Users**"). 7 Affected Users had the Palo Alto Traps software ("**Traps Software**"), an advanced endpoint protection solution, installed in their laptops and were therefore protected from Emotet. The remaining 6 Affected Users ("**Infected Users**") did not have Traps Software installed in their laptops. This resulted in the Incident with Emotet being installed and executed on the laptops of the Infected Users. Emotet subsequently harvested the emails in the Infected Users' accounts, created approximately 100 new phishing emails, and sent these new

[3] <https://www.stlogs.com/our company/about-st-logistics>.

phishing emails on 3 October 2019. Those new phishing emails quoted the bodies of real emails in the email accounts of the Infected Users.

5 Unencrypted files containing personal data were stored in 4 of the Infected Users' laptops. The files were offline working copy files used in relation to the logistics services provided by the Organisation to the MINDEF and SAF. The working files contained personal data relating to a total of 2,400 MINDEF and SAF personnel ("**Affected Individuals**"). The types of personal data of the Affected Individuals at risk of unauthorised access (collectively, the "**Disclosed Data**") were:

(a) Names;

(b) Mailing addresses;

(c) Email addresses;

(d) Telephone numbers; and

(e) NRIC numbers (1,320 full NRIC numbers and 1,080 masked (last 3 digits and checksum) NRIC numbers).

6 Based on the Organisation's investigations (including anti-virus scans performed following the Incident), the infection by Emotet was limited to the laptops of the Infected Users. At the time of the Incident, the Organisation's proxy logs captured information which showed that some exfiltration had taken place. However, there was insufficient information in the proxy logs to confirm that the exfiltration included files containing the Disclosed Data.

7 Upon discovery of the Incident, the following remedial actions were taken to mitigate the effects of the Incident:

(a) The Organisation immediately disconnected the Infected Users laptops from the Organisation's corporate network;

(b) Security advisories (including guidelines on how to identify phishing emails) were sent to all the Organisation's users to inform them of the Incident and to be vigilant; and

(c) All Affected Individuals were notified by MINDEF through text messages by 27 December 2019.

8 In addition, the following remedial actions have been taken, or are committed to be taken, by the Organisation to prevent recurrence of the Incident or similar incidents.

(a) The Organisation conducted a "PDPA awareness" programme in February 2020 for its staff. "PDPA awareness" training materials were made available to all staff on the Organisation's intranet. Selected users also attended the PDPA training offered by NTUC Learning Hub in February 2020;

(b) Malicious email domains were identified. Enhanced firewall protection was implemented to inspect traffic to the Organisation's email gateway. Email rules were created to block similar phishing emails from reaching the Organisation's users;

(c) The Organisation performed a company-wide validation exercise to ensure that Traps Software was installed on the laptops of all its users;

(d) The Organisation conducted a Sender Policy Framework verification to reduce the number of spam and phishing emails reaching its users;

(e) The Organisation implemented the display of warning banners for emails that do not originate from the Organisation's email server;

(f) The Organisation will increase the frequency of sending "Cybersecurity Advisory & Personal Data Protection Awareness" notices to all users;

(g) The Organisation implemented internet separation via URL filtering and has been exploring a sandbox feature and URL checking for all emails;

(h) Periodic phishing exercises will be conducted as part of the Organisation's Cybersecurity Awareness Program; and

(i) Independent security experts will be engaged to perform compromise assessment to validate the security status of the Organisation's systems environment in the third quarter of 2020.

The Commissioner's Findings and Basis for Determination

9 Most phishing attacks are sent by email,[4] and the most common form is the general, mass-mailed type, where the cyber attacker sends an email pretending to be someone else and tries to trick the email recipient to log into a website or download malware.[5] Based on the Commission's past investigations, there are generally 2 scenarios when a data breach involves phishing attacks on e-mail accounts:

(a) First, where malware harvests email addresses from the victim's email address book to send further phishing emails to contacts of the

---

[4] https://www.cisco.com/c/en_sg/products/security/email-security/what-is-phishing.html; See also National Cyber Security Centre (United Kingdom), *Phishing attacks: defending your organisation* (version 1.1, 8 August 2019) https://www.ncsc.gov.uk/guidance/phishing: Phishing can be conducted via a text message, social media, or by phone, but the term 'phishing' is mainly used to describe attacks that arrive by email.

[5] https://www.csoonline.com/article/3234716/types-of-phishing-attacks-and-how-to-identify-them.html

victim. In this scenario, the only personal data that are accessed and used by the malicious actor are email addresses; and

(b) Second, where the content of the victim's email account is compromised, and emails are downloaded and/or forwarded by malicious actors. In this scenario, there may be personal data within the body of the email message (e.g. customer information, employee human resource data, payroll information etc.) as part of its communication content. Some of these may be confidential or commercially sensitive information.

10 The first type of email phishing attack at [9(a)] is more common, and the risk of harm is relatively low as the unauthorised access and use is limited to email addresses. Conversely, while the second type of email phishing attack at [9(b)] is less common, the risk of harm is significantly greater. This is because in addition to email addresses, communication content exposed to unauthorised access and use may contain other type(s) of personal data (including those of a sensitive nature, e.g. medical and financial data). Consequentially, a breach of data protection obligations resulting in the organisation falling victim to the second type of email phishing attack generally results in more serious consequences.

11 The present case falls into the first type of email phishing attack, and the issue for determination is whether the Organisation had complied with its obligations under Section 24 of the Personal Data Protection Act 2012 (the "**PDPA**"). Section 24 of the PDPA requires an organisation 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 or similar risks (the "**Protection Obligation**").

12 As a preliminary point, it is not disputed that the Organisation was in possession and control of the Disclosed Data at all material times, and was obliged to put in place reasonable security arrangements to protect the Disclosed Data.

13 The Commission's investigations revealed that the Organisation failed to conduct periodic security reviews to detect vulnerabilities in its IT systems.

(a) As stated in the Commission's previous decisions, organisations are expected to conduct periodic security reviews of its IT systems.[6] Conducting regular information and communication technology ("**ICT**") security audits, scans and tests to detect vulnerabilities help organisations to ensure that ICT security controls developed and configured for the protection of personal data are properly implemented[7]. The comprehensiveness of such security reviews should be scoped based on the organisation's assessment of its data protection needs, and be conducted to a reasonable standard;

(b) In the present case, a reasonably conducted security review should have included (i) verifying complete installation and proper configuration of the security software on all of the Organisation's users' laptops; and (ii) checking that the security software is updated;

(c) The Organisation's failure to conduct a security review to a reasonable standard resulted in the following undetected security gaps that led to the Incident[8]:

---

[6] See *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].

[7]Commission's *Guide to Securing Personal Data in Electronic Medium* (revised 20 January 2017) at [6.1].

[8]As an updated anti-virus software and Traps Software both offered protection against Emotet, the Organisation could have chosen to take a phased approach to its security review.

(i) The anti-virus software installed on users' laptops was not updated because they had not been properly configured to receive updates. This security gap affected all of the Infected Users, whose laptops were not so configured. The investigations into the Incident revealed that if anti-virus software had been updated, it would have been able to block and remove Emotet at the material time; and

(ii) Due to a rollout gap, the Traps Software was not installed on the laptops of some Organisation's users. In contrast with signature-based anti-virus software (which is used to identify "known" malware), Traps Software detects malware based on their behaviour. This enables Traps Software to detect newly released forms of malware (which signature-based anti-virus software may potentially fail to detect) based on behavioural analysis. As mentioned at [4], this security gap affected all of the Infected Users, on whose laptops the Traps Software had not been installed. Conversely, the laptops of the remaining 7 Affected Users (who had also opened the malicious attachment) had Traps Software installed, and were accordingly protected from Emotet.

14 Based on the Commission's preliminary findings, it appeared that the Organisation also did not conduct proper data protection training for its staff. In particular, the Organisation had conceded during investigations that not all the Affected Users had completed the relevant data protection training at the time the Incident occurred. The failure to conduct proper data protection training would have been an additional ground (other than the omission to conduct periodic security reviews to detect vulnerabilities in the IT system) in support of finding the Organisation in breach of the Protection Obligation.

15 However, the Organisation subsequently clarified in its representations to the Commission's preliminary findings that its data protection training for its staff prior to the Incident included PDPA awareness programmes conducted in March and April 2019 and bi-monthly staff induction programmes covering cybersecurity and PDPA compliance. In addition, the training material for the PDPA awareness programme, as well as relevant reference materials and the URL link to the Commission's website were provided in the Organisation's intranet to allow staff ready access to data protection related resources.

16 The Commission recognises that staff movement will always have to be factored into staff training programmes, and at any one point in time, there will always be members of staff at different stages of training. Having a training programme in place and a system to track staff training is therefore important. Thus, while not all the Affected Users had completed the relevant data protection training at the time of the Incident, the arrangements the Organisation had implemented towards trainings its staff on data protection was reasonable in the circumstances.

17 For the reasons set out at [13] above, the Commissioner finds the Organisation in breach of section 24 of the PDPA.

18 In addition to the representations made on data protection training, the Organisation also raised the following factors for consideration in support of a reduction in the quantum of financial penalty which the Commissioner intended to impose:

> (a) The Organisation had put in place reasonable security arrangements to protect the Disclosed Data prior to the Incident. These included advanced end point solution (Palo Alto Traps) on corporate servers and workstations; privileged access management; monitoring of security events through security information and events management

systems; and web penetration test performed for corporate applications by CREST accredited vendor. Notwithstanding these arrangements, the Organisation was a victim of a phishing attack; and

(b) There was a low risk of harm arising from the Incident as the unauthorised access and use of the Disclosed Data by the cyber attacker were limited to email addresses. There was also no evidence that any Disclosed Data had been exfiltrated.

19 The Organisation's representations that it had put in place reasonable security arrangements to protect the Disclosed Data prior to the Incident is not accepted. As explained at [13], the Organisation failed to conduct periodic security reviews to detect vulnerabilities in its IT systems. The requirement for organisations to conduct periodic security reviews to comply has been emphasised in the Commission's previous decisions.[9] Separately, the Organisation's representation that there was a low risk of harm arising from the Incident is accepted and has been taken into account in determining the financial penalty.

20 Having carefully considered the representations, the Commissioner has decided to reduce the financial penalty to the amount set out at [22]. The quantum of financial penalty has been determined after due consideration of the low risk of harm arising from the Incident and the mitigating factors set out at [21].

The Commissioner's Directions

21 In determining the directions, if any, to be imposed on the Organisation under Section 29 of the PDPA, the Commissioner took into account the

[9] See cases listed at Footnote 6.

Organisation's cooperation with the investigations and its prompt and forthcoming responses to the Commission's queries.

22 Having considered all the relevant factors of this case, the Commissioner directs the Organisation to pay a financial penalty of S$8,000 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 the 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