PERSONAL DATA PROTECTION COMMISSION

[2021] SGPDPC 10

Case No DP-2005-B6353

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

And

The National Kidney Foundation

… *Organisation*

DECISION

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

The National Kidney Foundation

[2021] SGPDPC 10

Yeong Zee Kin, Deputy Commissioner — Case No. DP-2005-B6353

15 September 2021

Introduction

1 On 22 May 2020, the Personal Data Protection Commission (the "**Commission**") received a data breach notification from the National Kidney Foundation (the "**Organisation**"). The Organisation had discovered that on 17 May 2020, a hacker had gained access to the work email account of one of its employees ("**Employee A**") and had likely exfiltrated the personal data contained in the email account (the "**Incident**").

Background

2 The Organisation is a prominent non-profit health organisation in Singapore that provides health services, including subsidised kidney dialysis. Employee A is an executive in the Organisation's Clinical Operations department. which deals with implementation of operations policies, budget planning and working with medical and nursing management team to uphold healthcare standards.

The Incident

3 Investigations revealed that, on 14 May 2020, Employee A received a phishing email containing a hyperlink to a website with a further link to another website seeking his account credentials. The hacker is believed to have obtained Employee A's account credentials in this way. Thereafter, the hacker accessed Employee A's email account (the "**Email Account**") and synchronised the mailbox on 17 May 2020. In doing so, the hacker is believed to have downloaded all the data stored in the Email Account in its entirety. The hacker also used Employee A's email account to send phishing emails to 1,039 external business contacts of the

Organisation, and 9 email accounts belonging to persons within the Organisation. Whilst these phishing emails contained a link to a phishing webpage, they did not disclose any personal data collected from the Email Account.

4 The Email Account comprised of 23,145 emails containing the personal data of approximately 500 individuals (i.e. patients, employees and third parties):

(a) Age

(b) Arrear sum owed (22 patients affected)

(c) Bank account number

(d) Curriculum vitae

(e) Date of birth

(f) Data subject access request form (for 1 Singapore Police Force officer)

(g) Information on the patient's family status and any psycho-social issues faced by the patient

(h) Dialysis readings

(i) Email address

(j) Emergency contact numbers of nurses

(k) Education certificate(s)

(l) Foreign Identification Number

(m) Headshot photo

(n) Health screening virology report of the Organisation’s nurses (25 nurses affected)

(o) Household income band

(p) Marriage certificate; and

(q) Medical condition (8 patients affected)

(collectively, the "**Affected Data**")

Security Measures prior to the Incident

5 At the time of the Incident, the work email accounts of the Organisation's employees were hosted on Microsoft Office 365, and the employees were able to access their email accounts through the internet via a browser, ie web-accessible email or webmail. The following security arrangements were in place to protect the email accounts from unauthorised access:

(a) The password policy requires a minimum of 8 alphanumeric characters, including upper and lower cases, and a special symbol.

(b) A maximum of 3 unsuccessful login attempts before email accounts were locked out.

(c) Deployed Microsoft's Advanced Threat Protection ("**ATP**") email filtering service, with the ATP anti-phishing feature turned on.

(d) Deployed Sender Policy Framework ("**SPF**") and Domain Keys Identified Mail ("**DKIM**") email authentication protocols.

6 In addition, the Organisation also had various storage protection and network protection measures. This included a web isolation tool from Menlo Security, and an appointed Managed Security Service Provider ("**MSSP**") that performs security monitoring round the clock.

7 In relation to its employees, the Organisation implemented a range of measures to increase data protection awareness, including:

(a) Issuing a policy manual which defined the standards for proper usage of all computing and network resources by employees, and how employees should handle suspicious emails;

(b) Conducted training workshops in 2017 and 2018 in relation to the Personal Data Protection Act 2012 ("**PDPA**") for its internal stakeholders, which included a segment on cybersecurity covering the topic of suspicious emails;

(c) Conducting a phishing simulation exercise in 2019, which Employee A participated in;

(d) E-learning modules on cyber-security and the PDPA, which Employee A completed in March 2020;

(e) Sending regular emails and alerts targeted at increasing cybersecurity awareness to its employees; and

(f) Deploying cybersecurity awareness screensavers on all of the Organisation's computers.

Remedial Measures

8 After the Incident, the Organisation carried out the following remedial and rectification measures:

(a) Implemented additional email account security requirements for webmail access in the form of two-factor authentication ("**2FA**") on 22 May 2020;

(b) Appointed a third-party service provider to conduct daily scans for communication relating to the Incident on platforms across all media; and

(c) Notified affected individuals of the Incident on 24 July 2020 and offered the affected individuals subscription to an identity theft service to identify trading or selling of their personal data on the dark web.

Findings and Basis for Determination

Whether the Organisation had contravened section 24 of the PDPA

9 Based on the circumstances of the Incident as set out above, 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 taking reasonable security steps or arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks ("**Protection Obligation**").

10 For the reasons set out below, it is determined that the Organisation failed to implement reasonable security arrangements to protect the Affected Data from the risk of unauthorised access by failing to implement reasonable access controls to its employees' webmail accounts.

11 In determining what constitutes reasonable security steps or arrangements, an organisation should have regard to the nature of the personal data in its possession and control, as well as the impact that the disclosure of the data might have on the affected persons. As stated in the Commission's Advisory on Key Concepts in the PDPA[1]:

> "There is no 'one size fits all' solution for organisations to comply with the Protection Obligation. Each organisation should consider adopting security arrangements that are reasonable and appropriate in the circumstances, for example, taking into consideration *the nature of the personal data, the form in which the personal data has been collected (e.g. physical or electronic) and the possible impact to the individual concerned if an unauthorised person obtained, modified or disposed of the personal data.* For example,

[1] See sections 17.2 – 17.3 of Advisory Guidelines on Key Concepts in the PDPA (Rev 1 February 2021)

in the employment context, it would be reasonable to expect a greater level of security for highly confidential employee appraisals as compared to more general information about the projects an employee has worked on.

In practice, an organisation should:

a) design and organise its security arrangements to fit the nature of the personal data held by the organisation and the possible harm that might result from a security breach;

b) identify reliable and well-trained personnel responsible for ensuring information security;

c) implement robust policies and procedures for ensuring appropriate levels of security for personal data of varying levels of sensitivity; and

d) be prepared and able to respond to information security breaches promptly and effectively.

In addition, it might be useful for organisations to undertake a risk assessment exercise to ascertain whether their information security arrangements are adequate. In so doing, the following factors may be considered:

a) the size of the organisation and the amount and type of personal data it holds;

b) *who within the organisation has access to the personal data;* and

c) whether the personal data is or will be held or used by a third party on behalf of the organisation."

(emphasis added)

12 Where the personal data held by the organisation or particular employees are sensitive and may cause damage to affected individuals if compromised, strong access control measures, including robust authentication measures, are important safeguards. On top of basic authentication measures such as implementing a proper password policy and password expiration mechanism, strengthened measures such as two-factor authentication ("**2FA**") should be considered for webmail accounts with sensitive personal data, such as personal data relating to health and finances. As stated at paragraphs [7.3] and [7.4] of the Commission's Guide to Securing Personal Data in Electronic Medium[2]:

> "7. 3. The strength of authentication, such as password requirements or other mechanisms for access to personal data, *should depend on the potential damage to the individual, such as potential damage to reputation or finances,* if such personal data is compromised…
>
> 7.4 More secure authentication methods include two-factor or multi-factor authentication. These involve the use of a combination of information that the user knows, such as a password or PIN, and an object that only the user possesses, such as a digital key, token or smart card, or a unique physical trait, such as the use of fingerprints in biometric technology. *The use of multi-factor authentication increases confidence in the identity of the user accessing the system.*"
>
> [emphasis added]

13 Having regard to the nature of personal data handled by the Organisation in its daily operations, it had higher-level security needs that had to be met when discharging its Protection Obligation. The Organisation is one of Singapore's most prominent non-profit health organisations and a key provider of subsidised dialysis treatment, with a significant number of patients under its care. Given the nature of its operations, the Organisation's employees routinely handle the medical data of its patients and financial data relating to the processing of

[2] Guide to Securing Personal Data in Electronic Medium (revised Jan 2017)

patient subsidies. The vulnerability of its employees' email accounts (including the Email Account) is made more acute by the fact that they are web-accessible. In this regard, the Organisation should have conducted a risk assessment to identify the employee email accounts that warranted a more robust authentication process by virtue of the sensitivity of the personal data expected to be received in or sent from their email accounts.

14 As stated at 4 above, the Email Account contained the personal data of approximately 500 individuals. A subset of the Affected Data included sensitive personal data such as the medical conditions of patients, arrears owed and health screening virology reports of some of the Organisation's nurses. In this regard, even though the Organisation did put in place a host of technical measures and processes to address phishing risks prior to the Incident, we are of the view that these security steps and arrangements did not satisfy the standard required under section 24 of the PDPA, for the reasons set out below, especially when the nature of the personal data routinely handled by the Organisation is considered.

15 First, the Organisation did not adopt a risk-based approach to identify employees whose roles and functions required them to handle sensitive personal data and strengthen the access control measures to their email accounts.

16 Second, in relation to the email accounts of the employees who handle sensitive personal data (in particular, Employee A) in their daily work, the Organisation also did not implement more secure authentication processes access control measures to their email accounts prior to the Incident. As stated in paragraph 5, the Organisation's access control requirements were confined to a password policy and the locking out of email accounts after 3 unsuccessful login attempts. These measures are too basic and inadequate to safeguard webmail accounts from the threat of hackers seeking to access them from the internet, and left the personal data contained therein vulnerable to unauthorised access and exfiltration. Examples of more secure authentication methods include 2FA, which the Organisation eventually implemented only after the Incident had occurred. If 2FA had been implemented earlier, this

would have ensured that the use of stolen credentials such as passwords would not, *per se*, be sufficient to access the account.

17 In the premises, the Organisation has breached the Protection Obligation.

The Deputy Commissioner's Decision

18 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 Commission considered the factors listed at section 48J(6) of the PDPA, and gave particular weight to the following mitigating factors:

Mitigating Factors

(a) The Organisation had cooperated fully with the Commission during its investigations;

(b) The Organisation had put in place extensive measures to prevent phishing and educate its employees about data protection;

(c) The Organisation took prompt remedial actions following the Incident, including notification of the affected individuals; and

(d) The Organisation had conducted various data protection and cybersecurity training for its employees.

19 Having considered all the mitigating factors listed above, the Organisation is administered a warning in respect of its breach of the Protection Obligation. No other directions are necessary in view of the remedial actions already taken by the Organisation.

YEONG ZEE KIN
DEPUTY COMMISSIONER
FOR PERSONAL DATA PROTECTION