PERSONAL DATA PROTECTION COMMISSION

[2024] SGPDPCS 4

Case No. DP-2308-C1326

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

And

Academy of Medicine Singapore

DECISION

Data Protection *– Protection obligation – Unauthorised access to and disclosure of personal data – Insufficient administrative and technical security arrangements*

SUMMARY OF THE DECISION

1 Academy of Medicine Singapore (the "**Organisation**") is a professional institution providing postgraduate medical education and specialist training in Singapore. On 4 August 2023, the Personal Data Protection Commission (the "**Commission**") was informed about a data breach incident involving the Organisation's servers being infected by ransomware on or about 13 July 2023. Consequently, personal data of 6,574 individuals had been exfiltrated and posted on the dark web (the "**Incident**").

2 The Organisation requested, and the Commission agreed, for the investigation to proceed under the Expedited Decision Breach Procedure. To this end, the Organisation voluntarily and unequivocally admitted to the facts set out in this decision. It also admitted to a breach of the Protection Obligation under Section 24 of the Personal Data Protection Act 2012 (the "**PDPA**").

Facts of the Case

3 The Organisation first discovered malware artifacts in its servers after reports by staff members of network connectivity issues on 13 July 2023. The Organisation immediately disconnected the affected servers and sought an external IT forensic investigator to investigate the extent of the Incident and undertake remedial action.

4 Investigations revealed that data from the Organisation had been uploaded on the dark web (the "**Leaked Data**"), including full credit card information of over 1,000

individuals. Separately, a total of 4.4TB of files in the Organisation's servers had been encrypted due to ransomware deployment.

5 From system event logs, upon gaining initial entry the threat actor accessed 6 servers (the "**Affected Servers**") and 1 staff computer using Remote Desktop Protocol ("**RDP**") connections, then deployed malicious tools that could harvest credentials within folders and disarm antivirus and threat detection software. The investigation revealed the following lapses which could have contributed to the Incident:

(a) The Organisation's firewall FortiOS had not been patched since July 2021 and had been susceptible to a critical severity attack[1] which could be exploited at pre-authentication to allow a remote attacker to gain entry to systems without using credentials.

(b) Endpoint Detection and Response ("**EDR**") applications installed on the Affected Servers and devices did not detect and prevent the execution of malicious tools. The EDR Manager was compromised early and disabled by the threat actor before executing ransomware and file encryption.

(c) The Organisation's environment was highly vulnerable to exploitations due to operating systems in 2 of the Affected Servers having reached End-of-Life stages in July 2015 and January 2020 respectively.

[1] *CVE-2023-27997* is a critical heap buffer overflow vulnerability in Fortinet FortiOS' SSL-VPN pre-authentication component that is exploitable by attackers to execute arbitrary code.

(d) Critical hosts and staff computers had not been regularly scanned for vulnerabilities.

(e) There had been a lack of essential threat detection solutions and proper logs retention as EDR applications installed in the Organisation's environment either could not be supported by its operating systems or had outdated network signatures[2].

(f) There had been a lack of documented robust processes implemented at the time of the Incident to ensure regular patching and updates of important software.

6 The Organisation informed the Commission that the exfiltrated data contained personal data of 6,574 current and former members, participants of events, activities and/or in-training examinations organised/administered by the Organisation. The types of affected personal data are set out below. Not every affected individual had all of the personal data below in their personal data sets.

i. Name;

ii. Address;

iii. Personal email address;

iv. Telephone number;

[2] Network signatures match patterns of an attack that can crash applications or exploit the operating systems on client computers. It can be changed to block or allow traffic.

v. NRIC number;

vi. Passport number;

vii. Photograph number;

viii. Photograph (ID photo);

ix. Date of birth; and

x. Financial information, including bank account details, partially redacted credit card numbers, and credit card numbers with CVV and expiry date of 1,083 individuals.

7 The Commission's analysis of the Leaked Data by the threat actor found that it had contained approximately 12.7GB of data from the Organisation. It was observed that bank account details and credit card numbers with CVV and expiry dates had been stored in clear text without password protection or current standard file encryption. A list of login credentials to various online platforms used by the Organisation could also be found within the Leaked Data, including credentials to its website management system and passwords to various administrative emails.

Remedial Action

8 Following the Incident, the Organisation promptly notified the affected individuals about the Incident. The Organisation also took the following remedial actions:

(a) Activated a Crisis Response Team to facilitate forensic investigations and address queries related to the Incident;

(b) Notified the relevant authorities i.e. Singapore Police Force, Cyber Security Agency of Singapore and Ministry of Health of the Incident;

(c) Replaced its outdated firewall firmware to a newer version;

(d) Tightened access controls by enabling geo-blocking on the firewall and VPN configured to only allow access to its networks via local IP addresses;

(e) Installed and activated two-factor authentication for all staff members;

(f) Implemented Action 1 Patch Management that automated vulnerability remediation for operating systems and third-party applications, and continuous patch compliance for all servers;

(g) Implemented monthly checks on system and software patches;

(h) Conducted vulnerability scans on all staff-issued computers and devices;

(i) Restored files from their tape backup and performed malware scans of the restored files and all staff-issued laptops and devices; and

(j) Engaged a third-party vendor to provide credit monitoring services to affected individuals at no charges, whose financial information had been affected in the Incident, to help detect any suspicious transactions that might affect the affected individuals' credit reputation.

Findings and Basis for Determination

Whether the Organisation had contravened the Protection Obligation

9 Under section 24(a) of the PDPA, organisations must 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 disposal, or similar risks.

10 The Organisation's admissions amounted to the following breaches of section 24 of the PDPA:

(a) *Lack of sufficiently robust processes for updates or upgrades of important software or firmware*, which resulted in vulnerabilities that were not removed in the Organisation's firewall and servers. The Organisation said that its IT vendor at the time of the Incident had only been onboarded in April 2023 and had been focused on troubleshooting issues that arose in 2 events of system downtime in May and June 2023. Prior to the system downtimes, the Organisation also conducted an IT infrastructure review completed on 26 June 2023 that included identifying obsolete devices to remove and improving network security. Hence, written procedures or policies on patch management for software and firmware had yet to be developed and implemented at the time. However, the Commission determined that these circumstances did not mitigate the lack of sufficiently robust processes for updating or upgrading important software and firmware that saw firewall

patches not being carried out since July 2021 and servers with End-of-Life ("**EOL**") operating systems not being upgraded.

(b) *Failure to have reasonable access control*, in response to the need to enhance access control to the type of financial information in its possession or under its control. This financial information had included credit card numbers with their security codes (CVVs). These had been stored in servers in plain text without password protection. Given the risk of harm due to the nature of this personal data, the Organisation could have considered additional security options to enhance access controls to protect this data. The Commission highlighted in *Re Tokyo Century Leasing (Singapore Pte Ltd [2023] SGPDPC 9* in paragraph 11 that such data has a heightened risk of identity theft and/or financial loss, which called for a higher standard of security arrangements. Examples may include separate password protection for the server holding this data, encryption of the data, restrictions to the export of this data, or, given the Organisation's choice of endpoint security solutions, real-time security monitoring of the data server.

(c) *Failure to stipulate data protection requirements or clear job specifications in the contract of its IT vendor*, specifically in the areas of the management and maintenance of IT system security and the conduct of security reviews. Where organisations rely on vendors to perform IT security maintenance and/ or review, the scope of these services must be stipulated in the vendor

contract as part of the duty of a data controller under the Protection Obligation.

11 For the above reasons, the Organisation was determined to have breached the Protection Obligation.

The Deputy Commissioner's Decision

12 In determining whether the Organisation should be required to pay a financial penalty under Section 48J of the PDPA, the Commission considered all relevant factors listed at Section 48J(6) of the PDPA, in particular, the impact of the personal data breach on the individuals affected and the nature of Organisation's non-compliance with the PDPA.

13 The Commission considered that the personal data of 6,574 individuals had been affected as a result of the above breach. Further, the affected data included financial information comprising of bank account numbers and full credit card information of 1,083 individuals were leaked on the dark web.

14 The Commission also considered the fact that for more than 3 years, the Organisation had continued to deploy vulnerable servers with EOL operating systems for which support and security updates had ceased since July 2015.

15 The Commission considered the following mitigating factors:

(a) The Organisation was cooperative during the course of our investigations;

(b) The Organisation voluntarily admitted to breach of the Protection Obligation under the Commission's Expedited Decision Procedure; and

(c) This is the Organisation's first instance of non-compliance with the PDPA.

16 For the reasons above, the Commission hereby requires the Organisation to pay a financial penalty of $9,000 within 30 days of the date of the relevant notices accompanying this decision, 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.

Directions

17 In addition, to ensure the Organisation's compliance with the Protection Obligation, the Organisation is directed to report to the Commission on the completion of the following remedial actions:

(a) Assess the need for perimeter firewalls to restrict nonstandard outbound port access as per its network requirements and configure said firewalls if needed;

(b) Conduct a thorough security architecture review and assess the need to segregate sections of its network that support primary processing of personal data for its purposes from sections of the network that store personal data to reduce the risk of unauthorised access from within the network;

(c) Assess the need to implement hardening for endpoints, servers and network devices including password policies;

(d) Identify the sensitive personal data stored in its environment and remove or encrypt the information according to data security best practices e.g. the Payment Card Industry Data Security Standards for handling payment card data;

(e) Delete any stored CVV numbers and implement policy against storing CVV numbers after the initial transaction authorisation;

(f) Implement annual periodic security reviews of IT policies, processes and procedures to ensure compliance and alignment with security best practices; and

(g) Prepare and submit to the Commissioner a written report of the completion of the remediation actions directed above within 60 days.

WONG HUIWEN DENISE
DEPUTY COMMISSIONER
FOR PERSONAL DATA PROTECTION

The following section of the Personal Data Protection Act 2012 had been cited in the above summary of the Decision:

Protection of personal data

24. An organisation shall protect personal data in its possession or under its control by making reasonable security arrangements to prevent –
(a) unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks; and
(b) the loss of any storage medium or device on which personal data is stored.