PERSONAL DATA PROTECTION COMMISSION

Case No. DP-2406-C2514

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

And

Singapore Data Hub Pte Ltd

… *Organisation*

DECISION

Data Protection *– Protection obligation – Unauthorised access to personal data – Unauthorised disclosure of personal data– Failure to implement reasonable access controls – Failure to conduct reasonable periodic security review – Failure to implement regular patching*

SINGAPORE DATA HUB PTE LTD

[2025] SGPDPC 2

Deputy Commissioner — Case No. DP-2406-C2514

7 April 2025

Introduction

1 Singapore Data Hub Pte Ltd (the "**Organisation**") is a provider of point-of-sale and Customer Relationship Management ("**CRM**") software solutions to small and medium enterprises. On 10 and 15 June 2024 respectively, the Organisation notified the Personal Data Protection Commission (the "**Commission**") of two separate incidents on 28 April 2024 and 14 June 2024, which led to exfiltration of files within its servers affecting 698,112 individuals.

2 The investigation proceeded under the Expedited Decision Procedure ("**EDP**"). This means that the Organisation voluntarily provided 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 ("**PDPA**").

Facts of the Case

3 Investigation revealed that there had been unauthorised access within the Organisation's network on two occasions by at least two threat actors on 28 April 2024 (referred to as the first incident) and 14 June 2024 (referred to as the second incident) respectively.

The first incident

4 In the first incident on 28 April 2024, the threat actor ("**TA1**") probed the website of one of the Organisation's enterprise clients and found a vulnerable URL link that led to an application for its point-of-sales system (the "**POS application**"), which had been hosted on one of the Organisation's webservers. TA1 subsequently executed at least 1,370 Structured Query Language ("**SQL**") injection attempts on the POS application and accessed the Organisation's database, which was connected to the webserver. Other identified activities by TA1 included:

a. Exporting at least 371.3MB of data through SQL injection and accessing customer tables from the database which contained personal data;

b. Exploitation of a Local File Inclusion ("**LFI**") vulnerability thus obtaining hardcoded database credentials stored in application source code files and database configuration files; and

c. Path traversal attack to access files stored outside the POS application folder.

5 The personal data at risk of unauthorised access and/or exfiltration included a combination of name, address, personal email address, telephone number, date of birth and NRIC number of approximately 689,000 individuals. The affected personal data was also likely posted on a web hacking forum on 6 May 2024.

6 After the first incident, the Organisation updated the security controls in the webserver and took the following remedial action:

a. Changed the database administrator login URL and password;

b. Restricted access to database administrator account to whitelisted IP address;

c. Implemented additional password prompt on the database administrator login page;

d. Changed all user accounts' passwords and enhanced password policy to require all users to use a mix of at least 12 alpha-numeric characters and/or special characters;

e. Patched the vulnerable application code;

f. Encoded database configuration files for all applications hosted on the affected servers;

g. Implemented a web application firewall for all applications; and

h. Restricted directed IP address access to servers to require all access to go through a protected domain name going forward.

The second incident

7 In the second incident on 14 June 2024, the Organisation received an email from a threat actor ("**TA2**") claiming that it had exfiltrated customer data from the Organisation's systems. Based on the investigation's analysis of the web access logs available, TA2 accessed another webserver on the Organisation's network by accessing four of the Organisation's web applications including a dormant web application used for simulating client POS systems for training purposes. Access logs showed that TA2 had executed at least 820 SQL injection attempts on the various web applications to gain access to data that contained 'doctor' in its fields as well as at least 220,656 http post requests to an endpoint on the system.

8 The personal data in the second incident at risk of unauthorised access and/or exfiltration likely included the affected dataset in the first incident, as well as the gender and health information (i.e. descriptions of patient's skin concerns, skin condition, past and ongoing treatments, prescribed medications) of another 9,122 individuals. TA2 announced in a post on a web hacking forum that it had stolen the Organisation's data but will not be posting the full data for sale to not overshadow TA1's sale of data. Other data that were not part of TA1's alleged posting was uploaded for free in TA2's post.

9 After the second incident, the Organisation took the following additional remedial actions:

a. Shut down unused applications;

b. Reset passwords for all users;

c. Implemented 2-Factor Authentication ("**2FA**") for back-office access;

d. Disabled the export function from the database administration page to prevent remote exporting of data via the database administration page;

e. Implemented additional rules on the web application firewall to prevent SQL injection, including rules to block commonly used keywords;

f. Enhanced Fail2ban configuration to block unauthorised login for five failed logins within seven days from the same IP address; and

g. Performed a penetration test and applied hot fixes to production.

Likely causes of the two incidents

10 Investigations revealed that the following likely contributed to the first and second incidents:

a. The affected webservers were publicly accessible, with multiple open ports and had exposed the Organisation's web directory listing.

b. The Organisation had not conducted security testing for the web application codes, whether as part of pre-launch testing or periodic security reviews, to identify and remediate vulnerabilities in the web application.

c. The affected webservers had an operating system which had not been supported since 30 June 2024 and an outdated PHP:Hypertext Preprocessor ("**PHP**") scripting language which has not been supported since 31 December 2018.

d. It was determined that the Organisation had not deployed a network firewall for its environment to create a barrier from the Internet and enforce access control. A WAF was implemented after the first incident but it was not adequately configured to block further SQL injection attempts.

e. There were no threat detection and monitoring tool(s) in place at the time of the two incidents that would enforce rate limiting and signature detection to prevent brute force attempts and block unauthorised traffic in the Organsiation's network.

f. The Organisation did not implement the following access control measures:

i. Measures to safeguard access to application source code files and database configuration files that contained hardcoded credentials, such as password protection and industry standard encryption.

ii. Measures to safeguard access to administrator accounts, such as multi-factor authentication.

iii. Proper network segmentation to restrict the connections between servers and devices. All servers, end points and other devices were connected on a single Virtual Local Area Network ("**VLAN**") where connections between devices within the network were not restricted.

g. There was no logging capabilities and log monitoring tool(s) to record malicious activity within its network.

h. Applications on the affected webservers and databases were hosted on the same physical server thus increasing the attack surface.

Findings and Basis for Determination

Whether the Organisation had contravened the Protection Obligation

11 Under section 24(a) of the PDPA, organisations must protect personal data in their possession or under their control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification or disposal, or similar risks. The Commission notes that the Organisation is a Software-as-a-Service (SaaS) vendor that possesses and / or controls a high volume of personal data on behalf of its clients. Given the volume of personal data the organisation handles, the Organisation is required to implement security arrangements that are commensurate with its higher-level security needs.

12 The Organisation is found to have breached section 24 of the PDPA for the following reasons:

a. Failure to have reasonable access control. The Organisation did not implement basic access control measures to protect its systems and the personal data contained therein. In particular:

i. As explained in [10(a)], the affected webservers were web accessible and exposed the personal data contained therein to risk.

ii. Network firewall was not deployed by the organisation. When the first incident occurred, the Organisation did not have a WAF in place. In the Commission's Guide to Data Protection Practices for ICT Systems, the Commission recommended as a basic practice that organisations use a network firewall to separate their environment from the Internet and enforce access control. The Commission recommends as an enhanced practice that organisations deploy a properly configured WAF to defend against typical web application attacks such as SQL injection and XSS attacks.

iii. Further, the Organisation failed to protect the application source code files and database configuration files that contained important access credentials through measures such as password protection or encryption. The Commission had highlighted in *Re Redmart Limited [2022] SGPDPC* that important API keys should not be included in a configuration file.

For avoidance of doubt, the Commission's view is that complying with the Protection Obligation does not mean that organisations have to implement enhanced access controls with every solution or arrangement that is available. It is for organisations to make reasonable determinations of the types of access controls that

should be implemented based on the data that they are holding and to act accordingly.

In this regard, the Organisation had different options for enhancing access controls to protect the personal data in its possession or under its control. It could have deployed firewalls to protect the affected webservers or reviewed how important access credentials stored in its database configuration file should have been protected, such as by passwords or encryption.

b. Failure to conduct reasonable periodic security review including vulnerability scanning. As part of its operations, the Organisation rolled out changes to its applications almost every month, which it admitted was likely to give rise to security vulnerabilities. Given the risk engendered by such frequent changes, it was necessary for the Organisation to conduct security checks for vulnerabilities before the changes went live. Additionally, the Organisation should also have conducted periodic security reviews including basic vulnerability scanning on its networks to guard against cybersecurity risks. The Organisation did not do either, and only carried out internal acceptance testing which was meant to check if the application was functioning properly and did not include identifying cybersecurity vulnerabilities.

In this connection, the susceptibility of the Organisation's applications to SQL injection could have been detected and mitigated as part of a periodic security review or as part of pre-launch testing of its web applications. Organisations that lack the ability to conduct their own periodic security review are encouraged to engage the necessary assistance.

c. Lack of sufficiently robust processes to protect personal data through regular patching/ updates/ upgrades of important software. The Organisation continued to use outdated operating systems / scripting language for which support had ceased and lacked sufficiently robust processes for necessary upgrades of key software and firmware.

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

The Deputy Commissioner's Decision

Financial Penalty

14 The Commission is of the view that the imposition of a financial penalty is appropriate. As a provider of POS and CRM software solutions, the Organisation was expected to implement IT security arrangements beyond basic access control to secure its network from external threats especially when it possessed and/or controlled a high volume of personal data belonging to its clients.

15 In deciding the appropriate financial penalty amount, the Commission first considered the impact of the personal data breach on the individuals affected and the nature of Organisation's non-compliance with the PDPA. The Commission also considered the following factors:

a. The Organisation was cooperative during the course of the Commission's investigations;

b. The Organisation voluntarily admitted to the facts set out in this decision and to its contraventions 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 In addition, in order to ensure that the financial penalty imposed is proportionate and effective, having regard to achieving compliance and deterring non-compliance with the PDPA, the Commission also considered the Organisation's turnover.

17 For the reasons above, the Deputy Commissioner hereby requires the Organisation to pay a financial penalty of $17,500 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

18 In addition, to ensure the Organisation's compliance with the Protection Obligation, the Organisation is also directed to implement, within 90 days from the date of this decision;

a. Adequate perimeter security controls such as network firewalls and VPN configured with location-specific access;

b. Rate limiting on login attempts to prevent brute force attacks;

c. Network segmentation and tighten access controls in its network;

d. Segregation of production and training environments and conduct review to locate unused applications with a view to update or decommission;

e. Endpoint Detection and Response on all servers and clients;

f. Improvement to logging capabilities with a central repository;

g. A documented process to conduct periodic vulnerability assessment and penetration testing, at least annually and after major systems upgrade/assessment;

h. Strict input parameter validation to prevent SQL injection and LFI attacks;

i. Review and enhance its asset and patch management process;

j. Sufficiently robust processes to ensure all servers and clients are updated with the latest patches, and to update/replace outdated applications and operating systems;

k. Ensure username and password information are not included in a configuration file or properties file in cleartext and enable encryption where it may not be adequate to obfuscate the information; and

l. Report to the Commission upon the completion of all the above actions.

WONG HUIWEN DENISE
DEPUTY COMMISSIONER
FOR PERSONAL DATA PROTECTION