PERSONAL DATA PROTECTION COMMISSION

[2023] SGPDPC 3

Case No. DP-2108-B8712

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

And

OrangeTee & Tie Pte Ltd

… Organisation

DECISION

Data Protection *– Protection obligation – Unauthorised access to personal data – Insufficient security arrangements – Failure to conduct reasonable periodic security review*

Data Protection *– Protection obligation – Unauthorised access to personal data – Insufficient security arrangements – Failure to implement sufficiently robust processes for the use of 'live' production data for development and testing purposes*

OrangeTee & Tie Pte Ltd

[2023] SGPDPC 3

Lew Chuen Hong, Commissioner — Case No. DP-2108-B8712

21 February 2023

Introduction

1 On 4 August 2021, the Personal Data Protection Commission ("**Commission**") contacted OrangeTee & Tie Pte Ltd ("**Organisation**") after receiving information indicating that a threat actor had managed to exfiltrate databases in the Organisation's possession, which were believed to contain personal data.

2 Subsequently, on 6 August 2021, the Organisation notified the Commission of an incident involving unauthorised access to its IT network (the "**Incident**"). The Organisation also gave a media statement on the same day informing members of the public about the Incident and inviting any concerned customers to contact the Organisation's call centre for clarification.

3 The Commission then commenced investigations to determine the Organisation's compliance with the Personal Data Protection Act 2012 ("**PDPA**") in relation to the Incident.

Facts of the Case

4 The Organisation is a real estate enterprise based in Singapore and has been in operation since 2000.

5 Four servers maintained by the Organisation were involved in the Incident, namely: the Production Web Server, the Production Database Server, the Development Web Server, and the Development Database Server. The Production Web Server and the Development Web Server (collectively the "**Web Servers**") were internet-facing, in that they were directly accessible from the internet. The Production Web Server was linked to the Production Database Server, while the Development Web Server was linked to the Development Database Server.

6 The personal data of employees and customers of the Organisation was stored on the Production Database Server and the Development Database Server (collectively the "**Database Servers**"). The personal data had not been encrypted.

7 The Databases Servers were running Microsoft SQL Server 2012 Standard version 11.0.6251.0 (Service Pack 3) at the time of the Incident, which Microsoft had ceased support for on 9 October 2018. Additionally, the version of Microsoft SQL Server the Organisation used was also not updated, as the most current Service Pack 4 was not installed.

The Incident

8 On 3 August 2021, the Organisation received a ransom demand email from an organisation which identified themselves as 'ALTDOS'. The email was sent from an email address which is known to be used by the ALTDOS group. The threat actor claimed that they had been hacking the Organisation's network since June 2021 and had stolen "*hundreds of databases*", some of which were claimed to contain sensitive information. The ransom demand also contained video footage of five databases purported to have been stolen, which showed that sensitive data might have been exfiltrated from the Organisation's servers.

9 In the same email, the threat actor demanded a ransom of 10 Bitcoins for the safety and non-disclosure of the exfiltrated databases and threatened disclosure if the ransom was not paid. The Organisation filed a police report and reported the Incident to the Singapore Computer Emergency Response Team, a division of the Cyber Security Agency of Singapore.

10 On 4 August 2021, having not received the demanded ransom, ALTDOS carried out a Distributed Denial-of-Service attack which brought down the Organisation's network, and sent an additional ransom demand via email and WhatsApp to some of the Organisation's employees.

11 The Organisation engaged a private forensic expert ("**PFE**") to ascertain the cause and extent of the Incident. PFE's investigations disclosed that, contrary to their claims, the threat actor exfiltrated personal datasets from eleven databases, containing personal data set out in the table below:

Category of Individuals	**Number of Individuals**	**Types of Personal Data Affected**

Employees	305	Name, full NRIC/FIN/passport number and bank account number
Customers	245,752	Name, full NRIC/FIN/passport number and property transaction amount
Agents	10,526	Name, full NRIC/FIN/passport number and bank account number (*2,301 individuals*) Name, full NRIC/FIN number, bank account number and commission amount (*4,763 individuals*) Name, full NRIC/FIN number, commission amount (*286 individuals*) Name, full NRIC/FIN number (*3,176 individuals*)
TOTAL	256,583	-

12 The PFE's investigations found that the threat actor had carried out certain web-based attacks and exploited vulnerabilities on the Web Servers to successfully exfiltrate databases from the outdated Database Servers. The following observations were made by the PFE:

(a) **Production Web Server** – the PFE concluded that the threat actor used SQL injection attacks on the Production Web Server. SQL injections are a way of exploiting vulnerable website code and forms to return data from a SQL database that should not be available to a user. The PFE also found that the threat actor had likely used a malicious tool known as 'SQL Map' on vulnerable webpages in the Production Web Server, to automate the systematic probing of webpages for SQL injection vulnerabilities. Once the vulnerabilities were discovered, the threat actor then proceeded to exploit the vulnerabilities to access and exfiltrate data from four databases within the Production Database Server at some point(s) between 24 June 2021 and 3 August 2021.

(b) **Development Web Server** – the PFE could not locate forensic artefacts to confirm the mode of attack by the threat actor. However, the PFE identified evidence of cross-site scripting attacks. Cross-site scripting attacks involve the injection of malicious scripts into trusted websites which are then executed on end-users' browsers. In this case, malicious code had been injected into the Development Web Server. This led the PFE to believe that the Development Web Server was compromised. The threat actor is believed to have exploited the compromised Development Web Server to access and exfiltrate data from seven databases on the Development Database Server, although it was unclear how and when this had occurred.

Remedial actions

13 Following the Incident, the Organisation implemented the following remedial measures:

Immediate remedial steps to contain the Incident

(a) Shut down and isolated the affected servers from the rest of the IT network;

(b) Updated its servers with the latest security patches;

To prevent recurrence or similar incidents

(c) Tested the affected servers for vulnerabilities and deployed enterprise-grade anti-malware software across the IT network;

(d) Carried out security hardening activities, including the removal of redundant services, restricting access and services, and ensuring the server is secure to 'Center for Internet of Security' (CIS) benchmarking standards;

(e) Carried out detailed analysis of intrusion prevention logs;

(f) Reviewed and secured the firewall configuration;

(g) Separated the public-facing website from the internal agent portal and ensured that the former was securely hosted;

(h) Implemented a web application firewall to protect the network; and

(i) Liaised with the PFE on the recovery process as well as improving IT security.

Findings and Basis for Determination

14 Based on the circumstances of the Incident, 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**"). The Organisation was determined to have breached the Protection Obligation in the following two respects.

Use of production data in Development Servers for testing purposes

15 First, the Organisation used 'live' production data for development and testing purposes without sufficiently robust processes to protect the personal data through proper safeguards.

16 The 'live' production data used included personal data and had been stored in the development environment (i.e. the Development Servers) from which the datasets had been exfiltrated by the threat actor. The Organisation explained the use of 'live' production data as being necessary in order for the testing computations to be accurately derived, and for the actual business process flow to be effectively tested.

17 The Commission has advised in its *Handbook on How to Guard Against Common Types of Data Breaches* (the "**Handbook**") at page 11 that use of 'live' production personal data for testing creates a security risk.[1] The safer practice would be to use anonymised data for testing purposes. Synthetic data, which is fake data that contains similar characteristics as the real data, is a form of anonymised data. Another way is to use pseudonymised data where direct identifiers have been replaced with pseudonyms. The Commission has explained the rationale for anonymisation of personal data for development and business study in the Advisory Guidelines on the PDPA for Selected Topics:

> "3.14 **Anonymisation of personal data enables businesses to tap on data for insights and innovation while at the same time provides protection to individuals.** It also reduces the impact of harm to individuals in the event of a data breach. Where possible,

[1] Handbook on How to Guard Against Common Types of Data Breaches ("**Handbook**"), page 11: "*Out of convenience, many organisations use production data for system testing in their test environments. But as test environments tend to be much less secured, there is a high risk of data breach in a test environment*." (https://www.pdpc.gov.sg/news-and-events/announcements/2021/05/handbook-on-how-to-guard-against-common-types-of-data-breaches-now-available)

> Organisations should adopt such practices for external sharing of data. **It can even be adopted when sharing data internally, particularly where individuals need not be identified for the purposes of processing**.
>
> 3.15 In the event of a data breach, the level of data anonymisation, corresponding safeguards implemented and proper assessment by organisations in considering the harms of the anonymised data would be taken into consideration to assess if data has been properly anonymised."[2]
>
> (emphasis in bold added)

18 The Commission's position on this issue had been reiterated in *Re PINC Interactive Pte Ltd* [2022] SGPDPC 1, in which it was held that the organisation had breached the Protection Obligation by using a synthetic dataset that contained personal data belonging to real users. It should have used 100% synthetic data.[3]

19 However, where the use of 'live' personal data is operationally necessary, sufficiently robust processes should be implemented to safeguard the personal data. Testing or development environments are usually not as secured as production environments. The Organisation in this case had failed to implement sufficiently robust processes in the form of a security assessment of the risk from using, and storing, 'live' personal data in a testing environment. Such a security assessment could consider, for example, whether to restrict access to a smaller group of testers and limit the duration when live data is loaded in the testing environment. If the testing

[2] Advisory Guidelines on the PDPA for Selected Topics, page 14, paragraphs 3.14 – 3.15 (https://www.pdpc.gov.sg/guidelines-and-consultation/2020/02/advisory-guidelines-on-the-personal-data-protection-act-for-selected-topics)
[3] *Re PINC Interactive Pte Ltd* [2022] SGPDPC 1, [10] – [12]

environment is accessible from the Internet, security assessment ought to also be carried out of the risk of unauthorised web entry.

20 Without such an assessment, the Organisation was not positioned to make an informed decision on whether the security arrangements to protect the personal data had been reasonable or had needed to be enhanced. The lack of sufficiently robust processes to protect personal data through proper safeguards, such as the conduct of a reasonable security assessment, amounted to a breach of the Protection Obligation by the Organisation.

Failure to conduct reasonable periodic security reviews prior to the Incident

21 Second, the Organisation failed to conduct reasonable periodic security reviews for its servers.

22 The Commission's previous decisions[4] and the Guide[5] have established that periodic security reviews should be conducted to a reasonable standard to identify and remedy any vulnerabilities. Such scheduled reviews should be in place as a basic practice as it would likely have resulted in the detection of the vulnerabilities arising from the outdated software and the risk of SQL injection techniques. The Organisation admitted in its submissions to the Commission that it had not considered the need for such security reviews in its IT security policy.

23 Both Web Servers were internet-facing and were connected to production data stored in both Database Servers, thereby exposing the 'live' production data contained therein

[4] *WTS Automotive Services Pte. Ltd.* [2018] SGPDPC 26 and *Commeasure Pte Ltd* [2021] SGPDPC 11
[5] Guide, page 21, paragraph (g)

(containing personal data) to security risks. However, owing to its failure to conduct periodic security reviews for the Web and Database Servers, the Organisation did not recognise the risks engendered by the outdated software and did not take steps to assure itself that all internet-facing servers were adequately protected. Had the Organisation conducted reasonable periodic security reviews prior to the Incident, the vulnerabilities to SQL injection techniques in the Web Servers would have been known and remedied. The Incident could then very likely have been avoided.

24 For the above reasons, the Organisation was determined to have breached the Protection Obligation by (i) using personal data belonging to real users in a development environment (i.e. the Development Servers) without a sufficiently robust process for a reasonable security assessment of the risk, and (ii) failing to conduct reasonable security reviews prior to the Incident.

Organisation's position on the failure to update Microsoft SQL Server 2012

25 The Organisation explained its failure to update the Database Servers' Microsoft SQL Server 2012 version and install Service Pack 4 as follows:

(a) The Organisation's IT team relied on Microsoft's own auto-scan function to be alerted to available updating patches as a prompt for installation. This Microsoft tool ran once a month before the Incident. The tool, however, failed to detect that the installed version of Microsoft SQL Server 2012 in the servers required patching, and that the required patch in the form of Service Pack 4 had been available.

(b) The tool had not previously failed to detect and alert about required updates.

(c) The alternative option of requiring the IT team to conduct a manual review of all updates released by Microsoft every month had not been practical or reasonable as compared to relying on the auto-scan function.

(d) The Organisation's IT team did not use third-party scanning software to monitor and detect available patches because even these might not have identified the need to patch Microsoft SQL Server 2012 with Service Pack 4.

26 The Commission's investigation revealed no known issues relating to the availability or installation of Microsoft SQL Server 2012 Service Pack 4 updates. The Protection Obligation required the Organisation to have sufficiently robust processes to protect personal data through regular patching / updates / upgrades of important software. The question is whether the Organisation's reliance on system prompts in the form of alerts from the Microsoft auto-scan function had amounted to a sufficiently robust process for patching in the circumstances of this case.

27 Service Packs are significant collations of updates and patches that have been released. When released, Service Packs effectively provide a new baseline of updates and patches. On the question above, the Commission noted that the Microsoft Knowledge Base site indicated that the Service Pack 4 update had been available through the usual Windows Update auto-scan function since October 2017. This means that it would have been available for almost 4 years at the time of the Incident. Considering that an important software patch in the form of the Service Pack 4 had in this case been available for almost 4 years, the Organisation's reliance on system prompts such as alerts through the auto-scan function had not been a sufficiently

robust process to patch important software for the security of personal data. The Organisation should be aware of significant Service Packs and consciously decide whether to upgrade.

The Commissioner's Decision

28 In determining whether to impose a financial penalty on the Organisation pursuant to section 48J(1) of the PDPA, and the amount of any such financial penalty, the matters set out at section 48J(1), and the factors listed at section 48J(6) of the PDPA were taken into account, including the following mitigating factors:

Mitigating Factors

(a) The Organisation took prompt remedial actions, including notifying the affected individuals;

(b) The Organisation was cooperative during investigations; and

(c) The Organisation voluntarily admitted that it had breached the Protection Obligation in Section 24(a) of the PDPA in failing to protect personal data in its possession by making reasonable security arrangements to prevent unauthorised access.

29 The Commission further notes that names and property transaction amounts were among the categories of personal data which was exfiltrated. Whilst the Commission took the exfiltration of such personal data into account in its decision, it does not consider these

categories to be highly sensitive in nature as this information is, to a certain extent, already in the public domain. For example, a member of the public is able to look up such information through a land titles search on the Singapore Land Authority website (for names), or a search on the Urban Redevelopment Authority website for caveats lodged (for property transaction amounts). Thus, this information is publicly available as defined in s 2(1) of the PDPA.

30 Having considered all the relevant circumstances of this case, the Commissioner hereby requires the Organisation to pay a financial penalty of $37,000 within 30 days from the date of the relevant notice 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.

31 No further directions are necessary on account of the remedial measures already taken by the Organisation.

YEONG ZEE KIN
DEPUTY COMMISSIONER
FOR COMMISSIONER FOR PERSONAL DATA PROTECTION