PERSONAL DATA PROTECTION COMMISSION

[2025] SGPDPCS 4

Case No. DP-2405-C2330

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

And

People Central Pte. Ltd.

SUMMARY OF THE DECISION

1 People Central Pte. Ltd. (the "**Organisation**") is a cloud-based Human Resource ("**HR**") solutions provider that offers online HR management Software as a Service ("**SaaS**") solutions.

2 On 3 May 2024, the Organisation notified the Personal Data Protection Commission (the "**Commission**") of unauthorised access to and deletion of its clients' employees personal data from the Organisation's Amazon Web Services ("**AWS**") cloud servers (the "**Incident**").

3 The Organisation requested, and the Commission agreed, for the matter to be handled under the Commission's Expedited Decision Procedure ("**EDP**"). This meant the Organisation voluntarily provided and unequivocally admitted to the facts set out in this decision. It also admitted breach of the Protection Obligation under section 24 of the Personal Data Protection Act 2012 (the "**PDPA**").

Facts of the Case

4 On 29 April 2024, the Organisation received an extortion email from a threat actor. The Organisation immediately conducted an internal investigation and determined that the threat actor had deleted databases and likely exfiltrated data. Personal data allegedly taken from the databases had also been found for sale on the dark web.

5 The personal data of 95,000 employees of the Organisation's clients had been put at risk of unauthorised access, including name, gender, employee pass type, NRIC number, date of employment, place and date of birth, nationality, salary, marital status, religion, bank account number, mobile number, email address and address. Further, the personal data of 24,765 individuals who were the emergency contacts and/or children of the employees had also been put at risk of unauthorised access. The affected data included names and contact numbers in respect of 18,125 emergency contacts and the name / alias and date of birth in respect of 6,640 children of the affected employees.

6 Investigations revealed the following lapses that could have contributed to the Incident:

(a) SQL injection vulnerabilities had been present in the Organisation's web application. Multiple SQL injection attempts had been observed. In this regard, the Organisation did not have a Web Application Firewall ("**WAF**") to limit exposure of applications to exploitation traffic, which left it vulnerable to SQL injections;

(b) There had been weak access controls. Remote Desktop Protocol ("**RDP**") access had been open to the internet and did not require two-factor authentication ("**2FA**"). In addition, settings allowed network inbound traffic from all IP addresses in the cloud environment; and

(c) There had been insufficient security testing. Vulnerability scanning had been conducted only every 2 years.

Remedial Action

7 After the Incident, the Organisation took the following remedial action:

(a) Established a policy requiring the use of dedicated devices, implemented the use of virtual private network ("**VPN**") connection and disabled RDP for accessing its cloud environment;

(b) Closed and secured network ports;

(c) Implemented application-level security enhancement and conducted web application vulnerability assessment and penetration testing. All vulnerabilities identified have been rectified;

(d) Reviewed and implemented additional privileged account management measures;

(e) Enabled logging and monitoring for its cloud environment; and

(f) Updated and implemented new password requirements.

8 The Organisation also informed the Commission that it is in the process of implementing the following remedial actions:

(a) 2FA for RDP access, when access to RDP is required;

(b) Encryption for all personal data fields in its web application. Previously, only passwords and salary information had been encrypted; and

(c) Quarterly vulnerability scans and regular penetration testing.

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 Taking into account the Organisation's admissions, and for the reasons set out below, the Deputy Commissioner determines that the Organisation failed to implement reasonable security arrangements to protect the personal data in its possession and/or control, thus acting in breach of section 24 of the PDPA. Particulars of the breach are stated below:

(a) Failure to conduct reasonable periodic security review. The volume and types of personal data in the possession and under the control of the Organisation required it to increase its security against web-based threats beyond legacy password logins. In order to increase its web

security, the Organisation's periodic security reviews should have included web security assessments. The Organisation admitted to having an open RDP access to the internet, which increases the risk of cyber attacks. As stated in the Commission's Checklists to Guard Against Common Types of Data Breaches (the "**Checklists**")[1], organisations should, as a basic practice, periodically assess the need for remote access to servers, including configuration of open RDP access to the internet. Organisations should consider applying additional controls where possible, such as restricting access to specified external IP addresses and ensuring remote desktop is used behind a secure VPN.

(b) Additionally, the Checklists had recommended the use of WAF to defend against typical web application attacks such as SQL injections as an enhanced practice to provide multiple layers of security.

(c) The Organisation's security reviews had also been lacking in that, at the time of the incident, no network vulnerability assessments had been conducted. Vulnerability scanning had been conducted only every 2 years. As stated in the Checklists, organisations should, as a basic practice, periodically conduct web application vulnerability scanning and assessments in post deployment. The absence of network vulnerability assessments and the 2-year interval between vulnerability scans

[1] https://www.pdpc.gov.sg/help-and-resources/2021/08/data-protection-practices-for-ict-systems

supported the assessment that the Organisation had failed to conduct reasonable periodic security reviews.

(d) Further, CIS Critical Security Controls[2] also indicated that internal and external penetration tests should be conducted as least annually, and vulnerability assessments should be conducted quarterly. The role of the Organisation as a HR management SaaS provider meant that it would have processed the type of personal data that should have made penetration testing a good practice to have adopted.

(e) The Commission is cognisant of the skillset required and costs involved in penetration testing. However, the Commission would encourage organisations to assess the need and frequency of penetration testing as part of periodic security review.

11 For the above reasons, the Organisation is found to have breached the Protection Obligation under section 24 of the PDPA.

The Deputy Commissioner's Preliminary Decision

Financial Penalty

12 In determining whether to impose a financial penalty on the Organisation under Section 48J of the PDPA, the Commission considered that a financial penalty is appropriate given the role of the Organisation as an SaaS provider that processes personal data entrusted to it by its clients. As an SaaS provider, the Organisation

[2] https://learn.cisecurity.org/cis-controls-v8-1-guide-pdf

should possess the necessary technical expertise to implement reasonable cybersecurity measures to address the evolving threats.

13 In deciding the appropriate amount of financial penalty, 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. 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.

14 The Commission also considered the following factors:

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

(b) The Organisation voluntarily admitted to breach of the Protection Obligation under the EDP; and

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

15 For the reasons above, the Deputy Commissioner made a preliminary decision to impose a financial penalty of $17,500 on the Organisation for its breach of the Protection Obligation.

Directions

16 In addition, to ensure the Organisation's compliance with the PDPA, the Deputy Commissioner also directed the Organisation to:

(a) Review its web application to ensure secure implementation in accordance with industry best practices such as those indicated in Open Worldwide Application Security Project ("**OWASP**")[3];

(b) Implement an adequately configured WAF;

(c) Complete its implementation of regular annual external and internal penetration tests;

(d) Complete its ongoing implementation of 2FA for RDP access;

(e) Complete its ongoing implementation of encryption for all personal data fields; and

(f) Report to the Commission upon the completion of all the above actions.

Representations Made by the Organisation

17 The Organisation was notified of the preliminary decision by way of the Commission's letter dated 2 December 2024 and was invited to make representations. On 13 and 17 December 2024, the Organisation made the following representations:

(a) The Organisation did not implement a WAF as it encountered service disruption disruptions when attempting to implement it previously;

(b) The Organisation had conducted vulnerability assessments and adhered to International Organization for Standardisation ("**ISO**") procedures.

[3] https://cheatsheetseries.owasp.org/

There are no definitive or standardised rules specifying how frequently vulnerability assessments should be conducted; and

(c) The Organisation sought a waiver of the financial penalty, citing financial difficulties including decline in sales, increase in outstanding loans and reduced director salaries as part of its efforts to cut down on costs.

18 After careful consideration, the Organisation's representations were not accepted for the reasons outlined below:

(a) Organisations that have a high volume of personal data within their possession should implement sufficiently robust security arrangements. Organisations should also implement security arrangements to fit the nature of the personal data held and the possible harm that might result from a data breach. The Organisation as a provider of cloud-based HR solutions was in possession of a sizeable volume of client HR related personal data. The volume and types of personal data in the Organisation's possession necessitates the implementation of a WAF. The fact that the Organisation had encountered difficulties in implementing a WAF is not a valid mitigating circumstance for failing to do so;

(b) While there are no definitive or standardised rules on the frequency of vulnerability scans, the volume and types of personal data in the Organisation's possession meant that it ought to put in place increased security. Based on the CIS Critical Security Controls as referenced in [10(d)] above, this should also include conducting internal and external

penetration tests at least annually, and the conducting of quarterly vulnerability assessments; and

(c) The financial situation described by the Organisation did not justify a waiver of the financial penalty. Based on the financial statements provided by the Organisation, it had remained profitable. However, the Deputy Commissioner noted the likely impact of the financial penalty on the Organisation's immediate cashflow. Having taken into consideration the possible impact on the Organisation's ability to continue its usual activities, the Deputy Commissioner has decided to allow the Organisation to pay the financial penalty in 12 monthly instalments.

The Deputy Commissioner's Decision

19 Having considered all the relevant circumstances of this case, the Deputy Commissioner hereby requires the Organisation to pay a financial penalty of $17,500 in 12 instalments by the due dates as set out in the notice accompanying this decision, failing which, the full outstanding amount shall become due and payable immediately and interest at the rate specified in the Rules of Courts in respect of judgement debts shall accrue and be payable on the outstanding amount of such financial penalty until the financial penalty is paid in full.

20 For completeness, the Organisation is also directed to, within 90 days from the date of this decision:

(a) Review its web application to ensure secure implementation in accordance with industry best practices such as those indicated in OWASP;

(b) Implement an adequately configured WAF;

(c) Complete its implementation of regular annual external and internal penetration tests;

(d) Complete its ongoing implementation of 2FA for RDP access;

(e) Complete its ongoing implementation of encryption for all personal data fields; and

(f) Report to the Commission upon the completion of all the above actions.

WONG HUIWEN DENISE
DEPUTY COMMISSIONER
FOR PERSONAL DATA PROTECTION

The following are the provision of the Personal Data Protection Act 2012 cited in the above summary:

Protection of personal data

24. An organisation must 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 or disposal or similar risks and;

(b) the loss of any storage medium or device on which personal data is stored.