PERSONAL DATA PROTECTION COMMISSION

[2024] SGPDPCS 2

Case No. DP-2303-C0848

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

And

Payroll2U Pte. Ltd.

SUMMARY OF THE DECISION

1. Payroll2U Pte. Ltd. (the "**Organisation**") is a payroll service provider that offers payroll outsourcing services and online payroll Software as a Service (SaaS) solutions.

2. On 27 March 2023, the Personal Data Protection Commission (the **"Commission"**) was notified by the Organisation that the personal data of its client's employees had been posted on a ransomware leak site. The leak arose from a ransomware attack on the servers of the Organisation around 29 December 2022 (the **"Incident"**).

3. On 16 January 2023, the Organisation received extortion emails from a threat actor identified as a LockBit affiliate. The Organisation immediately conducted an

internal investigation and engaged an external forensics investigator to investigate the Incident and undertake remedial actions. Upon further investigations, it was determined that a total of 81.95 GB of data had been exfiltrated in the Incident and posted on the dark web. The personal data of 5,640 employees from the Organisation's client was affected, including their full name, bank account number, salary information, NRIC number, address, date of birth and email address.

4. Investigations revealed that unauthorised activity had occurred from 29 December 2022 to 16 January 2023, with a single compromised account used for Remote Desktop Protocol (RDP) access to five servers on the Organisation's AWS environment. Once connected to the working network, the threat actor gained unauthorised access to the developer's drive and the company's shared drive that were both mapped to the compromised account. These drives gave access to the affected personal data.

5. While the investigations were unable to conclusively determine how the threat actor obtained the credentials to the compromised user account, the investigation revealed the following lapses that could have contributed to the Incident:

a. Employees were given local administrator rights on their laptops, thus enabling a user to install/uninstall applications without restriction. The Organisation confirmed that the compromised user had reformatted his laptop and installed an unlicensed Windows Operating System that might have downloaded ransomware and removed the Symantec

Endpoint Protection. In addition, the compromised user also left the computer powered and web connected, allowing the threat actor to use the account to login to the Remote Desktop Servers.

b. Multi-Factor Authentication ("**MFA**") was not implemented for administrator accounts and non-administrative accounts with access to personal data.

c. There was an absence of tools to detect and remove the download of unauthorised software on company-issued laptops.

d. There was an absence of effective incident response and management control, enabling the threat actor's presence and activity within the Organisation's network to remain undetected between 29 December 2022 to 16 January 2023.

6. Following the Incident, the Organisation took the following remedial action:

a. Deactivated the compromised user account and forced change password for all users accessing the network.

b. Implemented MFA for users accessing internal and remotely accessible resources and environments.

c. Implemented documentation and quarterly review of Windows network drives and folder access. Collected log details and log reviews on a monthly basis.

d. Conducted checks on all workstations to ensure they are equipped with SentinelOne and Symantec Endpoint Protection (SEP).

e. Implemented host-checking for SSL VPN users vis FortiClient to verify that the SentinelOne and SEP processes are running before granting the device access.

f. Reviewed firewall configurations and rules. Fine-tuned web-filtering using Fortinet UTM. Implemented secured file transfer for inbound and outbound traffic. Block sharing over cloud storage and whitelisted URLs based on need to use basis.

g. Performed regular service account reviews to validate that all active accounts are authorised.

7. The Organisation requested for the matter to be handled under the Commission's Expedited Breach Decision Procedure ("**EDP**"). This means that the Organisation voluntarily provided and unequivocally admitted to the facts set out below; and admitted that it was in breach of section 24 of the Personal Data Protection Act 2012 (the "**PDPA**").

8. The Organisation admitted that it failed to implement reasonable access control. While the investigation noted and acknowledged the existence of proactive cybersecurity controls, the Organisation also admitted to storing the affected personal data sets that included the bank account numbers and salary information on unsecured internal shared drives. Given both the volume and types of personal data handled, the Organisation ought to have adopted additional access control beyond the baseline of password protection.

9. The Organisation had the option of either frontend access control or other options that focused on the backend. Frontend access control included MFA, at least for users with remote access to the more sensitive data mentioned. Backend access control included, for example, restrictive allocation according to the user's need for administrator-level rights that would impact personal data security as well as network segmentation. Sensitive personal data could have been stored in segments of the network that allowed access only on the basis of need.

10. As stated in the Commission's Guide to Data Protection Practices for ICT Systems (the "Guide")[1], access control privileges should be restricted and defined based on the user roles/rights to data. Users should not be able to see information that they do not need to know, and this should be reflected in an organisation's access control policy. In the present case, the Organisation should have assessed whether

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

the developer in question needed account access rights to personal data of the type affected in the Incident.

11. Another backend access control option recommended in our Guide was disallowing non-administrator employees from installing software and/or changing security settings and restricting the right to do so to specific administrator accounts. The Organisation failed to do so and non-administrative accounts were able to download unauthorised software on issued devices without being detected.

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

The Deputy Commissioner's Decision

13. In determining whether the Organisation should be required to pay a financial penalty under Section 48J of the PDPA or if directions would suffice, the Commission considered that a financial penalty was appropriate given the role of the Organisation as a payroll service provider and the types of personal data handled. In deciding the appropriate financial penalty amount, the Commission first considered all the 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.

14. In deciding what would be the appropriate financial penalty amount, the Commission also considered the Organisation's turnover to arrive at a figure that

would be a proportionate and effective amount, to ensure compliance and deter non-compliance with the PDPA. The Commission also considered the following mitigating factors, which led to a further reduction in the financial penalty:

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

b. The Organisation voluntarily admitted to a 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.

15. For the reasons above, the Commission hereby requires the Organisation to pay a financial penalty of $4,000 within 30 days of 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.

WONG HUIWEN DENISE
DEPUTY COMMISSIONER
FOR PERSONAL DATA PROTECTION