PERSONAL DATA PROTECTION COMMISSION

[2022] SGPDPCS 14

Case No. DP-2106-B8484

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

And

Cognita Asia Holdings Pte Ltd

SUMMARY OF THE DECISION

1. On 16 June 2021, Cognita Asia Holdings Pte Ltd (the "**Organisation**") notified the Personal Data Protection Commission (the "**Commission**") of a ransomware attack on 13 June 2021. The ransomware incident (the "**Incident**") affected the servers of three schools run by the Organisation.

2. The ransomware encrypted the personal data of 1,260 individuals, of which 1,195 are students. The personal data included copies of identification/passport page, salaries of the affected employees and the bank account details necessary for the crediting of salaries.

3. The Organisation’s internal investigations found that the threat actor gained initial entry to one of the school's network in April 2021 through a VPN session. The VPN logs showed no brute-force entry attempts, suggesting the use of compromised administrator account credentials. Investigations disclosed that between 8 and 12 June 2021, the threat actor gained broad network access and deployed the encrypting ransomware.

4. The Organisation requested that this matter proceed via the Expedited Decision Breach Procedure, which the Commission acceded to. To this end, the Organisation voluntarily and unequivocally admitted to the facts set out in this decision. It also admitted to a breach of section 24 of the Personal Data Protection Act (the "**PDPA**"), also referred to as the Protection Obligation.

5. At the time of the Incident, even though the Organisation employed VPN, the Organisation’s existing configuration of VPN required merely a username and password for authentication. However, the personal data collected and processed by the Organisation included copies of the photographic identification documents of students as well as salary and bank account information of employees. In view of the nature of personal data that it holds, the Organisation needed a higher level of security and stronger access control for its administrator accounts, such as multi-factor authentication for VPN connection to its administrator accounts to protect such personal data.

6. The Organisation also failed to have reasonable password policies or ensure compliance with their existing password policies. The Organisation did not enforce their password policies in the following areas:

    (i) Although the Organisation's password policy specified a minimum requirement of 10 characters, in practice the requirement that was enforced by their IT systems was only 8 characters; and

    (ii) Its password policy of requiring the default password to be changed after the first usage was not enforced.

7. The Commission's Handbook on "*How to Guard Against Common Types of Data Breaches*", which is complemented by the "*Checklists to Guard Against Common Type of Data Breaches*", has identified poor management of accounts and passwords as one of the five common causes and types of data breaches. Organisations must adopt, implement, and enforce a strong password policy as a necessary measure of data protection.

8. Finally, the Organisation also failed to ensure that personal data protection training was conducted for its staff. In this regard, the Commission wishes to reiterate that staff training in personal data protection is an important and necessary component of the Protection Obligation of an organisation.

9. In light of the above, the Organisation is found to have breached section 24 of the PDPA.

10. The Commission acknowledged that, the Organisation informed the relevant stakeholders of the Incident and implemented real time threat monitoring and Deep and Dark Web monitoring for potentially exposed personal data.

11. The Organisation also undertook remedial actions to mitigate the effects of the Incident and improve the robustness of its security measures. This included the engagement of a cybersecurity expert to investigate the cause of the Incident and working together with the said expert to enact a Remediation Plan.

12. The Remediation Plan included measures such as, enforcing multi-factor authentication of all staff accounts, enhancing the password requirements for administrator accounts, and increasing the frequency of security reviews and cyber security trainings for its staff.

13. The Organisation also conducted security awareness webinars and offered a 12 months' personal identity monitoring services to all the staff and parents (who can sign up on behalf of the affected students) of these three schools.

14. The Commission's decision to require payment of a financial penalty, and on the quantum of the penalty, took into account sections 48J(1) and 48J(6) of the PDPA, and all the relevant circumstances of the case. This included the Organisation's admission of breach of the Protection Obligation, which the Commission considers

is a significant mitigating factor. Having considered all the facts of this case, the Commissioner hereby requires the Organisation to pay a financial penalty of S$26,000.

15. The Organisation must make payment of the financial penalty within 30 days from the date of the 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.

16. In view of the remedial actions taken by the Organisation, the Commission will not issue any directions under section 48I of the PDPA.

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.