PERSONAL DATA PROTECTION COMMISSION

Case No. DP-2009-B7057

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

And

Trinity Christian Centre Limited

SUMMARY OF THE DECISION

1. On 11 March 2021, Trinity Christian Centre Limited (the "**Organisation**") notified the Personal Data Protection Commission (the "**Commission**") that its database servers containing personal data were infected with ransomware on or around 17 February 2021 (the "**Incident**").

2. The Organisation subsequently requested for this matter to be handled under the Commission's expedited breach decision procedure. In this regard, the Organisation voluntarily provided and unequivocally admitted to the facts set out in this decision. It also admitted that it was in breach of section 24 of the Personal Data Protection Act (the "**PDPA**").

The Incident

3. The Organisation runs Trinity Christian Church in Singapore.

4. At the time of the Incident, the database servers contained 72,285 individuals' data. The types of data affected for each individual varied, and included at times an individual's name, full identification number, residential address, contact number, email address, photograph, date of birth, age, marital status, education level, and/or description of medical condition (if applicable).

5. Investigations by the Organisation revealed that the Organisation maintained an open and publicly exposed remote desktop protocol port. This allowed a threat actor with access to compromised administrator account credentials to enter the Organisation's network and database servers to execute ransomware attack on 17 February 2021, rendering the databases inaccessible.

6. The Organisation managed to restore the affected databases from its back-up copies. Based on the Organisation's investigations, there was no evidence to suggest that the threat actor exfiltrated the Organisation's databases.

The Organisation's Admission

7. The Organisation admitted that it had breached the Protection Obligation under section 24 of the PDPA as:

a. It could have implemented separate access controls (i.e. separate logins) to protect the databases containing personal data; and

b. The initial unauthorised entry to the Organisation's network was through an administrator account that the Organisation had assigned to an IT vendor it had engaged to develop and test applications. The Organisation conceded that it failed to stipulate data protection requirements on its vendor.

Remediation

8. Following the Incident, the Organisation notified its church members on 8 April 2021. The Organisation changed all user and administrator passwords, closed all unused and open ports used for remote access and restricted logon access with domain administrator privileges to servers and workstations. A security review was also conducted and the Organisation implemented real time threat monitoring, detection, and response measures.

The Commission's Decision

9. As noted earlier, the Organisation admitted that it was in breach of section 24 of the PDPA as it could have implemented separate access controls to protect the databases containing personal data. In our view, the number and type of personal data sets in the possession or under the control of the Organisation created a

security need for stronger access control beyond reliance on frontend password protection. Indeed, with increasingly sophisticated phishing and social engineering techniques, adding another layer of protection to protect backend database servers, and manage the risks that frontend login credentials may be compromised was a reasonable security measure, which the Organisation also accepted.

10. The Commission had also previously emphasised in our decisions[1] and in the Commission's Guide to Managing Data Intermediaries that organisations that engage IT vendors should ensure that their IT vendors are aware of the need for personal data protection by making it part of their contractual terms.

11. The Organisation admitted that its contract with its IT vendor only contained a general confidentiality clause not to disclose information obtained without the Organisation's prior written consent. Even though the Organisation was well aware that its IT vendor would process personal data, the Organisation failed to stipulate within the contract any requirements on the vendor to protect the church members' personal data, thereby breaching section 24 of the PDPA.

12. In determining the directions to be imposed on the Organisation for the breach, the Commissioner took into account the following factors:

[1] See examples – Jigyasa [2020] SGPDPC 9, MDIS Corporation Pte Ltd [2020] SGPDPC 11 and Civil Service Club [2020] SGPDPC 15.

Aggravating

(a) The high number of affected individuals of 72,285 which included approximately 8,300 minors;

(b) The nature of the affected data. In particular, the affected databases contained descriptions of medical conditions provided by individuals counselling services and overseas mission applications. Individuals would expect a high level of confidence when they convey such information to the Organisation for handling;

Mitigating

(c) The Organisation's upfront admission of breach of the Protection Obligation, and the prompt remedial actions to mitigate the effects and prevent recurrence of the Incident; and

(d) There was no evidence of exfiltration of the Organisation's databases.

13. On account of the above, the Organisation is directed to pay a financial penalty of $20,000 within 30 days from the date of this direction. In view of the remedial action of the Organisation, the Commission will not be issuing any other directions.

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

Protection of personal data

24. An organisation shall 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, disposal or similar risks; and

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