PERSONAL DATA PROTECTION COMMISSION

[2019] SGPDPC [34]

Case No DP-1704-B0699

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

And

Marshall Cavendish Education Pte. Ltd.

…Organisation(s)

DECISION

Re Marshall Cavendish Education Pte. Ltd.

[2019] SGPDPC [34]

Tan Kiat How, Commissioner – Case No DP-1704-B0699

30 August 2019

1. With the increasing prevalence of ransomware attacks online, this case gives occasion to restate the importance of making adequate security arrangements to protect personal data and to limit unnecessary exposure of an organisation's computer systems to such potential threats on the internet.

Background

2. Marshall Cavendish Education Pte Ltd ("**MCE**") provided a learning management system ("**LMS**") at www.mconline.com.sg ("**Website**") to the Ministry of Education ("**MOE**") schools. This was pursuant to a contract between MCE and MOE.

3. On 1 February 2017, ransomware affected a substantial portion of MCE's network ("**Incident**"). On 3 February 2017, MCE informed MOE of the Incident. The relevant government agencies were notified of the Incident accordingly, including the Personal Data Protection Commission ("**PDPC**"). The ransomware had encrypted the files found on MCE's servers, including files containing personal data of individuals stored in the LMS, and made them inaccessible until a payment was paid to decrypt them.

4. Investigations revealed that the ransomware was an executable file on 1 server. However, it affected data on 11 servers and network storage devices in MCE's network. These 11 affected servers and network storage devices mostly held teaching material. However, the server in question and a network storage device

each held copies of the database of 206,240 active and 44,688 inactive users. The database held the following personal data of its users, which were mandatory fields that every user who signed up for accounts on the Website had to provide:

a. Login ID comprising an individual's full or partial birth certificate or NRIC no.;

b. Name;

c. School name;

d. Schooling level; and

e. Class.

5. Users could also opt to supply additional personal data using optional fields. According to MCE, however, users rarely provided such additional information, which comprised:

a. Email address;

b. Address;

c. NRIC;

d. Mobile Number;

e. Father/Mother/Guardian's Name;

f. Father/Mother/Guardian's NRIC/Passport Number;

g. Father/Mother/Guardian's Occupation;

h. Father/Mother/Guardian's Mobile Number;

i. Father/Mother/Guardian's Residential Number; and

j. Father/Mother/Guardian's Office Number.

6. MCE found no evidence that the personal data in its servers had been ex-filtrated. MCE's internet service provider's network logs would have captured the downloading of a database of that size.

7. However, as access had been gained to MCE's servers to upload and execute the ransomware, it meant that the personal data in MCE's servers were exposed to unauthorised access. Further, the encryption of the personal data by the ransomware was an unauthorised modification of the personal data in MCE's servers.

Causes of the Incident

8. The primary cause of the Incident was due to a change made to a firewall rule to allow internet access to the server. This allowed the external perpetrator to gain entry into the system to upload and execute the ransomware.

9. MCE had employed a senior system engineer ("**SE**") to, amongst other things, maintain MCE's servers. The SE was part of the Organisation's IT team that also comprised of another system engineer and a manager ("**IT Manager**") who had supervisory duties over the said system engineers. According to the Organisation, the IT Manager together with the SE and a program manager was also responsible for managing the services in the Organisation's datacentre.

10. The SE had found that the backup server's anti-virus definition was not updating automatically. The SE thought that the anti-virus' auto-update function was not working properly due to the limited or restricted access to the Internet, and thus the SE changed a firewall rule to allow direct access from the Internet to the server in question (the "**Firewall Rule Change**"). The Firewall Rule Change had lifted the restrictions that were in place to prevent external access to the MCE backup server and the data it held.

11. Critically, although the Firewall Rule Change was intended to be temporary, the SE had failed to reinstate the firewall rule after completing his investigation, thereby allowing the server to be continuously exposed to internet access. This increased the risk of an external perpetrator being able to gain entry into the server, as had transpired in this case.

12. PDPC's investigations revealed that the perpetrator had gained entry to the server through brute force attacks on the server. As a result of these brute force attacks, the perpetrator had uploaded and executed the ransomware on the server on 1 February 2017.

Remedial actions by the Organisation

13. The Organisation subsequently took the following remedial measures:

a. Put in place security arrangements to protect the personal data held in its servers after assessment of their need for remote internet access;

b. Conducted a review of the existing firewall rules in conjunction with an assessment of the remote internet needs of the IT system;

c. Engaged an external auditor to conduct a thorough review and audit of MCE's IT system;

d. Strengthened controls over deployment of any program to the Website;

e. Strengthened controls over obtaining of source code and database scripts;

f. Improved handling of any reported defects/issues with the LMS portal;

g. Implemented monthly review of user access rights, including a listing of product environment users and their accompanying access rights;

h. Strengthened control user access requests to the RDP server and mechanisms to deal with the deletion of any remote user access requests by non-active accounts;

i. Improved management of the various types of user accounts;

j. Better defined scope of duty for each system engineering team;

k. Hired an IT security officer to focus solely on cybersecurity; and

l. Strengthened its network security by clarifying various steps or approvals that need to be performed or obtained before a system engineer can make any system changes and procedures for follow up actions and management reporting for all IT security incidents.

Findings and Basis for Determination

Issue for determination

14. The issue to be determined is whether MCE had complied with its Protection Obligation under section 24 of the PDPA in this case.

15. There is the preliminary issue of whether MCE was a data intermediary for MOE and whether it could avail itself of the exception under section 4(1)(c) of the PDPA, which states that Parts III to VI of the PDPA, including section 24 of the PDPA, shall not impose any obligation on any public agency or organisation in the course of acting on behalf of a public agency (in this case, MOE). Investigations disclosed that MCE was a vendor providing IT tools and hosting services for MOE's teaching and administrative programmes. MCE was not acting on behalf of a public agency for the purposes of section 4(1)(c) of the PDPA and is subject to the full gamut of obligations under the PDPA qua its capacity as a data intermediary.

16. Section 24 of the PDPA provides that an organisation shall 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 similar risks (the "**Protection Obligation**").

Whether MCE breached section 24 of the PDPA

17. The personal data in question was stored on MCE's backup server. It was in MCE's possession or under its control. MCE therefore had a duty to protect that data by making reasonable security arrangements against unauthorised access or modification.

18. MCE did not fulfil its obligation under section 24 of the PDPA when the circumstances are viewed in totality. The SE had intended the Firewall Rule Change to be temporary. However, the SE had failed to reverse the Firewall Rule Change as he was interrupted by other work matters in the middle of attempting to establish the reason for the failure of the antivirus software to update automatically. This was a critical mis-step.

19. This was exacerbated by the fact that the SE had, at some time prior to this, already installed remote access software on the backup server. Only the Remote Desktop Protocol (RDP) server was meant to be configured to be accessible remotely. However, it appears that the SE had configured the backup server as a secondary RDP server.

20. While the Firewall Rule Change in and of itself was a security risk as it opened the MCE's backup server to a wide range of possible attacks, the installation of remote access software on the server and its configuration as a secondary RDP server would have allowed an attacker a greater chance of success in infiltrating it, especially where no safeguards were implemented to mitigate this risk. These threats are real – as has been exemplified in this case where the perpetrator had managed to use brute-force attacks to gain access to the backup server in order to upload and execute the ransomware.

21. As an organisation, MCE bore responsibility for putting in place the requisite measures to prevent data breaches from taking place. As mentioned in *Re Aviva Ltd* [2018] SGPDPC 4, relying solely on employees to perform their tasks diligently is not a sufficiently reasonable security arrangement, and the organisation would need to take proactive steps to protect personal data. In this case, the SE was part of the Organisation's IT team supervised by an IT Manager. However, it appears that the IT Manager did not exercise competent supervision over the IT team. In this regard, the Organisation admitted, through a written statement made

by the Organisation's General Manager of Product Development ("**GM of Prd. Devpt.")**, that:

a. User accounts in the data centre for former staff, including that of a staff who had left in 2014, had not at the material time been removed;

b. The SE was not familiar with the new firewall and that this may have contributed to the Incident. If the Organisation was aware of the SE's unfamiliarity with the new firewall, the IT manager ought to have supervised the SE more closely; and

c. That there were no standard operating procedures in place to document changes to the firewall configurations and there were no measures in place to monitor for the installation of unauthorised software. We have addressed this issue in paragraphs 35 to 37 below in addressing the representations made by the Organisation.

22. In these circumstances, the IT Manager may not have been able to effectively supervise the daily operational actions of the SE.

23. What is required on the part of the Organisation are practicable steps, and these can take the form of identifying areas of risks that require higher level approval and adequate supervision of such risky areas. One such area that ought to have been identified was the installation of remote access software as every installation of remote access software is a channel for web-based threats that have to be guarded against. In this regard, the Organisation did not implement a process which provided adequate supervisory oversight over the installation of the remote access software, apart from identifying the installation of remote access software as an act that required higher level approval. Records of any installation of the remote access software could also be, but were not, maintained. This would have been a practicable step that MCE could have put in place. Of course, this cannot prevent

the situation where the SE wilfully disregarded such a policy and proceeded to install remote access software on the backup server without authority, but the analysis of the facts and conclusion on MCE's liability might well be different had such supervisory measures been implemented.

24. Similarly, MCE could also have implemented some form of approval process for changes to firewall configuration. In this case, a manual record of firewall changes in a log book or other form of supervisory monitoring, for example, could have been practicable steps put in place by MCE. This would have heightened the awareness of the SE that changes to firewall rules cannot be made in a cavalier manner, and that his actions were subject to scrutiny. Again, this will not prevent wilful disregard of such control measures but the lack of such practicable steps deprived MCE room to raise a credible claim that it had put in place reasonable security measures to protect the personal data.

25. In addition to the failure of supervision, 15 accounts with remote access to MCE's system through the primary RDP server were found during MCE's post-Incident review. MCE reduced this number of accounts to 5. The unnecessary number of permitted users with remote access to the system pointed to a less than adequate appreciation of the risk that comes with remote access. This buttresses the Commissioner's findings that MCE has not adequately met its section 24 obligation to protect personal data. The personal data stored on the server was not only subject to unauthorised access, it was modified without authorisation through the encryption process of the ransomware.

26. In the premises, the Commissioner is satisfied that MCE failed to make reasonable security arrangements to protect the personal data in its servers from risk of unauthorised access, modification and disposal. The Commissioner therefore finds MCE in breach of its obligation under section 24 of the PDPA.

Directions

27. The Commissioner is empowered under section 29 of the PDPA to give the Organisations such directions as it deems fit to ensure the Organisations' compliance with the PDPA. This may include directing the organisations to pay a financial penalty of such amount not exceeding S$1 million as the Commissioner thinks fit.

28. Pursuant to section 29(2) of the PDPA, and the investigation and assessment of this matter having been completed, the Commissioner is satisfied that MCE did not make reasonable security arrangements and is in breach of section 24 of the PDPA.

29. Having carefully considered all the relevant factors of this case, the Commissioner hereby directs that MCE pays a financial penalty of S$40,000 within 30 days from the date of the directions, failing which interest shall be payable on the outstanding amount of such financial penalty.

30. In assessing the breach as determining the directions to be imposed on MCE in this case, the Commissioner took into account the following mitigating factors:

a. MCE was cooperative in the investigations;

b. There was no misuse of the affected personal data that was reported or indicated; and

c. MCE had put in place several remedial measures as indicated at paragraph 13 above.

However, the Commissioner had to balance these mitigating factors against the fact that MCE's failure to protect in this case led to loss of personal data in the possession of the organisation to the control of the ransomware attacker.

31. Representations were made by MCE after being informed of the proposed decision in this case, submitting that they had complied with the Protection Obligation under section 24 of the PDPA. In the alternative, MCE requested for a warning in lieu of a financial penalty or to otherwise reduce the quantity of the financial penalty imposed.

Compliance with the Protection Obligation under section 24 of the PDPA

32. In support of the assertion that MCE had complied with section 24 of the PDPA, MCE made the following representations:

a. By installing remote access software on the backup server and changing the firewall configuration without higher level approval from MCE's IT manager, the SE *wilfully disregarded* MCE's IT security policy;

b. As acknowledged by the Commission at paragraph 23, no practicable steps can be taken to prevent a situation of wilful disregard; and

c. MCE had adequate supervisory measures, as seen by the fact that the Incident was discovered after MCE carried out its routine monitoring of the system, and MCE subsequently took prompt action to investigate the Incident.

33. The Commissioner has considered the representations and maintains his finding that MCE is liable under section 24 of the PDPA for the actions of the SE.

34. At the outset, it is crucial to note that the breach was not one-off, as the SE's installation and usage of the unauthorised remote access software on the backup sever took place on more than one occasion, but went undetected. In fact, the SE had fully configured the backup server to function as an RDP server, should the primary server fail, without the knowledge of his supervisor. This shows the inadequacy of MCE's supervisory mechanisms.

35. It should be noted that the Organisation, through a written statement made by its GM of Prd. Devpt. on 2 June 2017, had admitted that:

a. "At the time of the incident, there were no measures in place to prevent system engineers to install unauthorised software, such as Teamviewer [a remote access software]"; and

b. "They [the IT team] were not required to notify anyone else if changes were made to the firewall configurations. There are no standard operating procedures to document such changes." The Organisation also admitted that this was a lapse on their part and have tightened their process following a security audit by their vendor.

36. The Organisation in its representations has stated that it had a policy in place which required the SE to seek higher level approval from the IT Manager for the installation of remote access software and the Firewall Rule Change. Assuming that the statement made by the GM of Prd. Devpt. on 2 June 2017 and the statements made in the representations are true and are consistent with each other, the reasonable conclusion is that, while there was a policy requiring such higher level approvals, this policy was not adequately implemented and there was a lack of

supervision and monitoring over both the installation of remote access software and the Firewall Rule Change. In practice, the SE was allowed to take whatever action he deemed fit without any supervisory oversight from the IT Manager or any other supervisor even if this resulted in compromising the Organisation's IT security.

37. In this regard, the fact that the SE was able to wilfully disregard MCE's procedures on more than one occasion over a period of time, without this activity being detected, highlighted MCE's failure to translate the policy into a process which sufficiently complies with section 24 of the PDPA. Merely putting in place policies is insufficient to fulfil MCE's obligation under section 24 of the PDPA – MCE must also have taken practicable steps to *implement* these policies, for example, as set out above at paragraph 21 through adequate supervision and/or monitoring.

Imposition of financial penalty

38. In support of their request that the Commission should issue a warning instead of a financial penalty or otherwise reduce the quantity of the financial penalty imposed, MCE made the following representations:

a. The Commission failed to consider all relevant mitigating factors in arriving at the preliminary decision;

b. The proposed financial penalty is manifestly excessive in light of previous decisions issued by the Commission for similar or even more serious breaches; and

c. It would be extremely prejudicial for MCE if the Commission were to issue a decision and impose penalties on MCE almost two years after the Incident, as the public may have the misconception that the Incident took place recently and MCE currently does not have

reasonable security arrangements to protect personal data that is in its possession.

39. MCE raised the following mitigating factors in its representations:

a. There was clearly no loss of personal data;

b. No personal data was accessed by the perpetrator or any third party and no individual can or will be affected by the Incident;

c. MCE took immediate steps to reduce the damage caused by the Incident;

d. There were no prior breaches of the PDPA on the part of MCE; and

e. MCE had not acted deliberately or wilfully.

40. As the personal data had been rendered inaccessible by encryption, MCE had in fact lost access and control of the personal data. Also, because of the unauthorised encryption of files containing the personal data, MCE was forced to delete these encrypted files in accordance with its data protection policy. The main database was modified because it was encrypted, and there would have been a loss of new incremental data created during the interval between the last backed up copy and ransomware attack. Furthermore, personal data was put at risk as the perpetrator of the ransomware attack could access the personal data if they chose to do so.

41. Nevertheless, as noted at paragraph 30 above, the Commission took into account the fact that there was no misuse of the affected personal data that was reported or indicated, and the fact that MCE had put in place remedial measures following the Incident. The fact that there were no prior breaches of the PDPA is not a mitigating factor in itself. On the contrary, if MCE had breached the PDPA

repeatedly, this would have been an aggravating factor, and it is trite that the absence of an aggravating factor is not a mitigating factor. In addition, the deliberateness or wilfulness of MCE in breaching the PDPA is not a relevant consideration in this case.

42. Furthermore, the three cases cited by MCE – *Challenger Technologies Ltd and Xirlynx Innovations* [2016] SGPDPC 6 ("*Challenger*"), *Institute of Singapore Chartered Accounts* [2018] SGPDPC 28 ("*ISCA*") and *Bud Cosmetics* [2019] SGPDPC 1 ("*Bud Cosmetics*") are not analogous to the present facts.

43. Firstly, MCE submitted that only a warning was imposed in *Challenger* although the personal data of more than 165,000 individuals was compromised. However, the personal data leaked in *Challenger* was limited – it comprised only individuals' names, membership expiry dates and accumulated points. However, the personal data in the present case includes personal data of minors and NRIC numbers, and is thus of a more sensitive nature.

44. Secondly, MCE submitted that the personal data compromised in *ISCA* was even more sensitive as it included employment records and exam results, however a financial penalty of only $6,000 was imposed. Employment and exam results are not treated as sensitive data. Furthermore, the number of affected individuals in *ISCA* was substantially lesser – 1,906 individuals as opposed to more than 250,000 individuals in the present case, and the unauthorised disclosure was limited to a *single* unintended recipient for a short period of 10 minutes. This consequentially affects the quantity of the financial penalty imposed.

45. Thirdly, MCE submitted that in *Bud Cosmetics*, the Commission imposed a financial penalty of only $11,000 despite the fact that the Commission found breaches under sections 12, 24 and 26 of the PDPA. As with *Challenger*, the personal data compromised in *Bud Cosmetics* was not sensitive. Furthermore, the

number of affected individuals in *Bud Cosmetics* was substantially lesser – 2,457 individuals as opposed to more than 250,000 individuals in the present case.

46. Lastly, the time taken to complete investigations into PDPA breaches and issue decisions may vary from case to case due to a myriad of factors. The present case involved substantial technical complexities requiring a longer a period of time to complete investigations, consider representations and issue the decision. The present Grounds of Decision clearly state the date of the Incident and the remedial measures taken by MCE. This would address MCE's concerns that the public would be of the view that the incident took place recently or that it has not remediated the breach.

47. In view of the remedial measures taken by MCE, no further directions are necessary.

48. The Commissioner urges organisations to take the necessary action to ensure that they comply with their obligations under the PDPA. Appropriate enforcement action against non-compliant organisations will be taken.

YEONG ZEE KIN
DEPUTY COMMISSIONER
FOR COMMISSIONER FOR PERSONAL DATA PROTECTION