[This is a redacted version of the Decision which omits certain confidential details]

Learnaholic Pte. Ltd.

[2019] SGPDPC 31

Tan Kiat How, Commissioner — Case No DP-1703-B0567

Data protection – Protection obligation – Disclosure of personal data – Insufficient security arrangements

26 August 2019.

Background

1 The Organisation is an IT vendor that was providing attendance-taking and e-learning systems to schools pursuant to a contract with the Ministry of Education ("**MOE**"). The central issue to this case, in so far as it is related to the Personal Data Protection Act 2012 ("**PDPA**"), is whether the Organisation had made reasonable security arrangements to protect the personal data of approximately 47,802 students, students' parents and staff of various schools that it had in its possession and control at the material time.

Material Facts

2 The Organisation was responsible for the maintenance and installation of the attendance-taking system installed in [redacted] ("**the School**"). The School's attendance-taking system was designed such that the attendance records would be updated each time a student "taps in" with his or her student pass at any one of the card readers located around the School. This attendance-

taking system consisted of an attendance server (the "**Attendance Server**") connected to clusters of attendance controllers linked to card readers. One such cluster was located at the guard post of the School (the "**Guard Post Cluster**").

3 In or around March 2016, the School informed the Organisation of an intermittent problem with the Guard Post Cluster: students' names were not being displayed despite them tapping in at the Guard Post Cluster. In order to investigate into the issues reported by the School, the Organisation decided to troubleshoot the problem remotely as this was more convenient than sending someone down to the School. In order to do so, it installed VNC Server, a remote desktop software, at the Guard Post Cluster. Using VNC Viewer to remotely connect to the VNC Server so that the Organisation would be able to troubleshoot the Guard Post Cluster without having to be physically present at the School (the "**Remote Troubleshooting**" method).

4 In addition to installing the VNC Server, the Organisation also took the following steps to facilitate its Remote Troubleshooting:

(a) Modifying the configuration of the School's Intranet firewall by opening a specific port ("**Port**") to allow external access to the Guard Post Cluster from the internet via the VNC Viewer software.

(b) Disabling the password for the VNC Server software installed at the Guard Post Cluster (*i.e.* no password was required to gain access to the Guard Post Cluster via the VNC Server software). While the Organisation claimed to have disabled the input feature at the client side when using the VNC Viewer program, this would have only affected the Organisation's ability to make changes and would not have affected a hacker's ability to do the same. If the Organisation had disabled the input feature at the server side, it would have been very unlikely that a hacker

could have exploited the vulnerability in the Organisation's system as explained immediately below. The only other potential manner in which the hacker could have exploited the said vulnerability would have been where the Organisation opened all the ports to the system instead of just the VNC specific port.

5 The Organisation's actions would come to have significant consequences. Prior to the opening of the Port, the Guard Post Cluster was only accessible internally from the School network. The opening of the Port was meant to be temporary for the purposes of the Remote Troubleshooting, but the Organisation's Representative (the "**Representative**") conducting the troubleshooting forgot to close the Port and restore the School's original firewall configuration after the troubleshooting was completed. The disabling of the password for the VNC Server software meant that access to the Guard Post Cluster could be easily gained simply with knowledge of the Port number and the IP address of the Attendance Server. This combination of actions led to the creation of a vulnerability in the School's Guard Post Cluster (the "**Vulnerability**") – a vulnerability that would later be exploited by a hacker.

6 The Organisation took the view that the hacker exploited the Vulnerability to retrieve a configuration file stored on the Guard Post Cluster. The Commissioner believes that this is a logical explanation of how the hack occurred. This configuration file was supposed to be stored only on the School's Attendance Server, but had inadvertently been copied to the Guard Post Cluster. This had occurred as the Organisation had stored the configuration file in a folder on the Attendance Server that also held firmware update files for the Guard Post Cluster (the "**Update Folder**"); the Update Folder would be periodically synced with the relevant components of the Guard Post Cluster in the School in order to "push down" firmware updates from the Attendance

Server to these components at the Guard Post Cluster. A copy of the configuration file was therefore copied to the Guard Post Cluster during one of the periodic firmware updates.

7 The purpose of the configuration file was to enable the School's Attendance Server (using the Representative's work email as a relay) to send attendance reports to the School's staff. To facilitate this function, the configuration file contained the login credentials of the Representative's work email. The hacker was thus able to obtain the login credentials from the copy of the configuration file retrieved from the Guard Post Cluster, and thereby gain access to the Representative's work email account. The Representative's work email account contained the unencrypted personal data of approximately 47,802 staff, students, and students' parents of various schools (the "**Personal Data**"). The Personal Data exfiltrated by the hacker included information such as:

(a) Names;

(b) NRIC numbers;

(c) Contact numbers;

(d) Email addresses;

(e) Addresses; and

(f) Medical information, which relate to approximately 372 students.

8 The Personal Data was in the Representative's email as the Organisation had assisted the schools to upload the data onto the respective schools' attendance taking and/or e-learning systems. The Representative had received the Personal Data via email for the purposes of uploading, but had not deleted

these emails after performing the upload as it was thought that it might be useful to retain the Personal Data for future reference.

9 The breach of the School's attendance taking system and the Representative's work email, together with the resulting exfiltration of the Personal Data, were only discovered in February 2017 by the Singapore Police Force ("**SPF**") in the course of investigating a separate hacking incident[1]. The Personal Data Protection Commission ("**PDPC**") was informed of the matter and thereafter commenced its own investigations.

The Commissioner's Findings and Basis for Determination

The Relevant PDPA Provisions

10 In respect of this matter, the relevant provision is Section 24 of the PDPA. Section 24 requires an organisation to protect personal data in its possession or under its control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks (the "**Protection Obligation**").

Preliminary Issues

11 It is not disputed that the Personal Data is "personal data" as defined in section 2(1) of the PDPA. There is no question or dispute that the Organisation falls within PDPA's definition of an "organisation". There is also no dispute that Personal Data was, at all material times, in the Organisation's possession and that the Organisation was responsible for the Personal Data.

---

[1] This hacking incident, and the Singapore Police Force's investigations, are not the subject of these Grounds of Decision.

12 In the course of investigations, it was determined that the Organisation was at all material times an independent third party service provider to, and therefore was not acting on behalf of, MOE or any of the various schools it provided IT services to. The Organisation also did not raise the applicability of section 4(1)(*c*) of the PDPA at any time. In the circumstances, section 4(1)(*c*) of the PDPA does not apply.

13 The key issue is therefore whether the Organisation had protected the Personal Data in its possession by making reasonable security arrangements to prevent unauthorised access and similar risks.

The Organisation failed to make reasonable security arrangements

14 After a review of all the evidence obtained by PDPC during its investigation and for the reasons set out below, the Commissioner is of the view that the Organisation had failed to make reasonable security arrangements to protect the personal data in its possession, and has thereby breached the Protection Obligation under section 24 of the PDPA. This data breach incident occurred due to a series of lapses on the part of the Organisation, all of which could have been reasonably averted.

15 First, the Organisation opened a Port and reconfigured the School's Intranet Firewall to allow remote access to the School's Guard Post Cluster, while simultaneously disabling the password for remote access to the Guard Post Cluster, thereby creating the Vulnerability. In addition, the Representative conducting the Remote Troubleshooting forgot to close the Port, leaving the Vulnerability exposed from March 2016 until end-April 2016, when the Vulnerability was discovered because the Organisation was subsequently requested to troubleshoot the Guard Post Cluster again in or around April 2016.

16 It bears noting that the Organisation did not inform the School that it had made changes to the configuration of the School's Intranet firewall during the Remote Troubleshooting. The changes made to the configuration of the Intranet firewall in this matter was a clear security lapse borne from convenience; in attempting to get around the need to be physically present in the School, the Organisation undermined the security arrangements in place and allowed the hacker to obtain the configuration file. This was exacerbated by the Organisation's failure to inform the School of these configuration changes.

17 Second, the configuration file (containing the login credentials of the Representative's work email account) was supposed to be stored only in the School's Attendance Server. As described at [6] above, this configuration file had been inadvertently copied to the Guard Post Cluster, where the Vulnerability existed as a point of entry for the hacker, which allowed the hacker to consequently gain access to the configuration file.

18 The hacker was thus able to obtain the login credentials of the work email account where the unencrypted Personal Data was stored. The Organisation has represented to PDPC that the email accounts and passwords contained in the configuration file were listed in a jumbled up or random manner, such that it would not have been apparent which email account corresponded with which password. Such an approach falls far below the level of sophistication which one would expect login credentials to be secured with. A relatively low degree brute-force attack (*i.e.* trial and error) would be all that was required to match an email account with its corresponding password. The Organisation failed to appreciate the consequences of placing the configuration file with the login credentials – a file that effectively contained the proverbial keys to the kingdom – in the Update Folder of the Attendance Server. Allowing a file that contained sensitive information such as login credentials to be copied

to each of the clusters represents a clear lapse in the Organisation's security arrangements. The less-than secure manner in which the login credentials were stored and dealt with within their own system was an issue that the Organisation should and could have been reasonably alive to.

19 Third, the Personal Data was sent to and stored in the Representative's work email account in an unencrypted form. The PDPC encourages the encryption of personal data that is sensitive or when sent in bulk. As this case demonstrated, personal data sent in bulk were stored in the clear in the Representative's email account effectively giving the hacker free rein to access the information once access to the email account was obtained. The originator of the Personal Data shared some of the blame in failing to encrypt the file. But the risks would not have materialised had the Representative deleted the email containing the Personal Data once his task was completed (e.g. uploading of data). This he failed to do. He kept the email containing the Personal Data, just in case he needed it in the future. If there was a valid legal or business purpose for retaining a copy of the Personal Data for an extended period of time, it should not have been retained in the Representative's work email account in an unencrypted format. The Organisation could have downloaded a copy of such data into a computer and encrypted the same if it needed to retain it (and thereafter deleting the originating email and attachment). This is a basic security arrangement that could have been reasonably expected of the Organisation.

20 The Organisation's inadequate security measures were therefore directly responsible for the breach and exfiltration of the Personal Data. Any of the individual lapses on their own would have been a cause for concern; combined together, the lapses created the perfect opportunity for any opportunistic hacker armed with basic hacking tools to strike.

21 Based on the foregoing, the Commissioner finds that the Organisation has breached the Protection Obligation under section 24 of the PDPA.

The Commissioner's Directions

22 Having found the Organisation to be in breach of section 24 of the PDPA, the Commissioner is empowered under Section 29 of the PDPA to give the Organisation such directions as he deems fit to ensure compliance with the PDPA.

23 In determining the appropriate directions to be imposed on the Organisation, the Commissioner has taken into account the following aggravating factors:

(a) In the course of its work with the schools and MOE, the Organisation was handling large volumes of personal data relating to minors, including sensitive personal data such as their medical information, family structure and NRIC numbers. The unauthorised disclosure of such data could potentially have caused significant harm.

(b) The Vulnerability was left unattended for a period of more than a month during which other hackers could have easily obtained access to the Personal Data[2].

(c) Actual data exfiltration had taken place.

24 To its credit, the Organisation acted fairly swiftly to address the causes of the breach once they were made aware of the same, a response which carries

---

[2] During the investigations, there had been some uncertainty as to the duration for which the Vulnerability was left uncorrected. This is further discussed at [27] below.

some mitigating value. The following remedial actions taken by the Organisation have therefore been taken into account:

(a) Changed the passwords for all the Organisation's work email accounts;

(b) Activated Two Factor Authentication for all of the Organisation's work email accounts after being informed of the data breach by SPF;

(c) Deleted all emails with the Personal Data from the Organisation Representative's work email account;

(d) Deleted the configuration file from the Guard Post Cluster;

(e) Implemented a new practice of having the Organisation's representatives delete emails from their work email account once action has been taken in respect of the same; and

(f) Put in place a script to ensure that the Update Folder of the Attendance Server only contains essential php files such as system codes, and that any non-essential files are automatically deleted prior to the syncing of the Update Folder with the other attendance clusters in the School.

The Organisation's Representations

25 The Organisation made representations to the PDPC, in particular to reduce the quantum of the financial penalty imposed, after the preliminary decision was issued to the Organisation. The Organisation's representations are addressed as follows.

26 First, the Organisation represented that the total number of individuals affected was 35,000 (and not 60,000 according to initial calculations), and that the total number of students whose medical data was accessed and exfiltrated was 372. PDPC has reviewed the evidence and determined that the number of unique individuals affected by the incident was 47,802. The Commissioner accepts that 372 individuals' medical data was accessed. The financial penalty has, therefore, been adjusted to take into account the number of individuals whose medical data was accessed and exfiltrated and the reduction in the number of affected individuals.

27 Second, the Organisation represented that the Vulnerability had been discovered and fixed sometime at the end of April 2016 when the Organisation was requested to troubleshoot the Guard Post Cluster again (as described in [15]). The Organisation had previously indicated that they were unaware of the duration during which the Vulnerability was left uncorrected. In the circumstances, the financial penalty quantum was initially based on the Vulnerability having only been corrected on or about February 2017 when the Organisation was notified of the incident by SPF in the course of investigating a separate hacking incident. The Commissioner has given the Organisation the benefit of the doubt as to the period of time the Vulnerability existed and has adjusted the quantum of the financial penalty accordingly.

28 Third, the Organisation also represented that the medical information subject to unauthorised access relates to types of medical conditions[3] which it

---

[3] For instance, colour vision; whether the student was on regular medication; respiratory disorders; allergies; asthma; epilepsy; heart condition; ear disorder; hearing loss; periodic loss of consciousness; and modified exercise.

(*cont'd on next page*)

asserts are non-sensitive in nature. However, the medical data that was accessed was those of minors, *ie* less than 21 years of age. Medical data and personal data of minors is treated as being sensitive in nature[4]. For such sensitive personal data, organisations are required to take extra precautions and ensure higher standards of protection under the PDPA.

29 Fourth, the Organisation represented that it had requested the schools to upload personal data on their own, to limit any personal data sent to the Organisation to what is absolutely necessary, and if the schools were to send data via email, to password protect the data file attachments. However, the preferred practice of many of the schools was to send unencrypted personal data to the Organisation for it to be uploaded. To give the Organisation the benefit of doubt, even if it is accepted that the Organisation had informed the schools to password protect data file attachments sent by email, the evidence shows that this policy was not observed in practice. Merely having a policy is not a sufficient security arrangement particularly when this policy is observed only in its breach.

30 As a corollary to the above point, the Organisation also represented that "*as a vendor and a small enterprise serving the educational institutions, [the Organisation was] understandably subservient to the decisions of their customers*". If the Organisation chooses to accede and upload the personal data that was sent to its email account, then it ought to have reviewed its policies and implemented different security arrangements to protect such personal data, *e.g.* by deleting file attachments containing personal data promptly.

---

[4] See Advisory Guidelines on the Personal Data Protection Act for Selected Topics at [8.12] and *Singapore Taekwondo Federation* [2018] SGPDPC 17 at [22] to [27].

31 Fifth, the Organisation represented that its practices were to delete emails containing personal data when no longer required (*e.g.* after uploading onto the appropriate databases), and that the reason that the attacker was able to gain access to so many email attachments containing Personal Data is because he had access to the email account for 3 months. While this may be true, the Organisation previously admitted that emails containing Personal Data would still be required to address enquiries from schools, and thus, were retained in the Representative's email account for months (and not immediately deleted after uploading). As stated in [19], the fact that the Personal Data was retained in such a manner facilitated the hacker's access to the Personal Data; if the Organisation needed to keep the Personal Data for operational purposes, it should have properly secured it.

32 Sixth, the Organisation represented that the following should be taken into account as mitigating factors:

(a) it was a victim of a cyberattack that had maliciously exploited the lapses on the part of the Organisation;

(b) the Organisation tried their even best to secure personal data, but its lone efforts were insufficient without reciprocation from the schools; and

(c) based on SPF's investigations there was no evidence of further exploitation, use or disclosure of the Personal Data by the attacker.

33 With respect to [32(a)], it should be reiterated that being a cyberattack victim is not in itself a mitigating factor, especially in this case where the lapses of the Organisation, including the existence of the Vulnerability, were such that

the attacker would not require sophisticated means to obtain unauthorised access to the Personal Data.

34 Paragraph [32(b)] has been addressed above[5]. With respect to [32(c)], while there was actual exfiltration of the Personal Data in this case[6], there was no evidence of further exploitation, use or disclosure of the Personal Data by the attacker. This has been taken into account in the revised financial penalty.

35 Finally, the Organisation also sought to compare the penalty imposed against it with that of previous cases[7]. However, the cases cited dealt with identification data while this case involved medical data of minors. The Commissioner is satisfied that the financial penalty imposed in this case is justified, in particular given the aggravating factors set out above at [23].

36 Having considered all the relevant factors of the case, the Commissioner hereby directs the Organisation to pay a financial penalty of S$60,000.00 within 30 days from the date of the Commissioner's direction, 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 the financial penalty until the financial penalty is paid in full.

---

5 See [29] and [30].

6 This has been taken into account as an aggravating factor, see [23(c)].

7 Specifically, *Re K Box Entertainment Group Pte Ltd* [2016] SGPDPC 1, *Re JP Pepperdine Group Pte Ltd* [2017] SGPDPC 2, and *Re Orchard Turn Developments Pte Ltd* [2017] SGPDPC 12.