PERSONAL DATA PROTECTION COMMISSION

[2020] SGPDPC 1

Case No DP-1811-B3058

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

And

Creative Technology Ltd

… *Organisation*

DECISION

Creative Technology Ltd

Tan Kiat How, Commissioner — Case No DP-1811-B3058

2 January 2020

Facts of this Case

1 This case concerns an online support forum (the "**Forum**") operated and hosted by Creative Technology Ltd (the "**Organisation**"). In November 2018, the Personal Data Protection Commission (the "**Commission**") was informed that the Forum had been hacked sometime in mid-2018 resulting in the unauthorised disclosure of personal data of users of the Forum (the "**Incident**").

2 The Organisation first set up the Forum some time in 2004 to help users share ideas and information relating to the Organisation's products. In 2011, the Organisation adopted a third-party forum software known as "vBulletin" to operate and host the forum internally. Unknown to the Organisation, the vBulletin software had a SQL vulnerability which could allow hackers to extract information hosted on the platform using SQL injection techniques. The developers of the vBulletin software released patches to address this SQL vulnerability in 2016. However, the Organisation had not installed these patches at the time of the Incident.

3 On 25 May 2018, an unknown hacker used SQL injection techniques to obtain personal data of Forum users from the Forum's database. In particular, the hacker exploited the vulnerability in the vBulletin software to launch SQL injection attacks by using the "Forumrunner" add-on[1].

4 The Organisation first came to know of the Incident on 4 June 2018, when it was notified by a security researcher that he had received a set of user data extracted from the Forum. The Organisation subsequently found that 484,512 users' account information had been accessed and extracted in the Incident.[2] Of these, only 173,763 appeared to be legitimate email addresses with the remainder, in the Organisation's view, being "disposable" or otherwise not

[1] The Forumrunner add-on allows users to use forums hosted using vBulletin on their mobile devices.

[2] The Commission has not verified the number of user accounts affected for reasons explained at [14].

legitimate[3] email addresses. Further, of the accounts with legitimate email addresses, the Organisation found that there were 8,258 active users[4] ("**Active Users**") who had accessed or posted on the forum between 2014 and 2018 and, amongst these Active Users, approximately 2,600 had email addresses which contained either the names or partial names of individuals.

5 According to the Organisation, the following data of Forum users (the "**Personal Data**") were accessed and extracted by the hacker:

(a) username;

(b) password, salted and hashed by the vBulletin software (each password was hashed using the MD5 algorithm, and the resulting password was hashed for a second time by MD5 and salted with random characters)[5];

(c) email address; and

(d) Internet Protocol address (IP address).

6 In addition, optional personal data which the Forum user may choose to enter (the "**Optional Data**"), including age, date of birth, other contact details (e.g. ICQ number, AIM screen name, Skype name, and MSN and Yahoo! Messenger handles), location, occupation, could be accessed when the password was used to log in to a user's account. These data were viewable by other Forum members, with the exception of date of birth, which the individual could choose to hide from, or disclose to, other Forum users.

Remedial actions

7 Upon discovering the Incident, the Organisation undertook the following remedial measures:

[3] Such as email addresses from the Mailinator Service and addresses which contained gibberish or profanities.

[4] According to the Organisation, users whose (i) accounts were activated (by clicking on a verification link in an email sent to them during the Forum registration process); and (ii) had logged into the Forum with their user account, or had uploaded at least one post in the Forum.

[5] See paragraph 11.

(a) it conducted a review of all its systems, servers, and software used by its IT and Internet Marketing teams and determined that the incident was an isolated occurrence, and the other systems had been subject to regular security reviews and security patches;

(b) it notified the 8,258 Active Users of the Incident; and

(c) it shut down the Forum temporarily on 4 June 2018 to prevent further incursions, and shut it down permanently shortly thereafter (by 20 June 2018).

Findings and Basis for Determination

Whether the Organisation complied with the Protection Obligation

8 Section 24 of the Personal Data Protection Act 2012 (the "**PDPA**") 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**"). It is not in dispute that the Personal Data and the Optional Data were in the Organisation's possession and under its control at the time of the Incident.

9 The Organisation had failed to put in place reasonable security arrangements to protect the Personal Data for the following reasons.

10 First, the Organisation had not patched or updated its version of vBulletin since 2 May 2015, three years prior to the Incident. This was a significant factor leading to the Incident. As stated in the Commission's *Guide to Securing Personal Data in Electronic Medium* (revised 20 January 2017, at [16]), regular security patching is important for organisations to keep their systems and databases current and minimise their vulnerabilities.

11 Secondly, the use of the MD5 algorithm is no longer sufficiently secure for password hashing, as compared with other available algorithms. Passwords hashed with MD5 are susceptible to some forms of attacks and, if they are compromised, this could lead to the disclosure of other personal data. Individuals may face additional risks if they had used the same email address and passwords for other online accounts. In this regard, the developers of vBulletin no longer used MD5 hashed password by default, opting for the more secure bcrypt,

since the March 2014 version of vBulletin. This reinforces the point that if the Organisation had implemented the updates, the users' hashed passwords would be more secure.

12 In the circumstances, the Commissioner found the Organisation in breach of section 24 of the PDPA.

The Commissioner's Directions

13 In determining the directions to be imposed on the Organisation under section 29 of the PDPA, the Commissioner took into account the following mitigating factors:

(a) the Organisation was cooperative in the investigations and had provided prompt and detailed responses to the Commission's requests for information;

(b) the Organisation implemented reasonable remedial and corrective actions to address the Incident, which includes notifying the affected Active Users;

(c) even though the Organisation had deleted the database, it made the effort to go through its email logs to determine the number of affected user emails which contained either names or partial names.

14 In the course of settling this decision, the Organisation made representations highlighting the low sensitivity of the personal data that was disclosed and the fact that the disclosure was unlikely to have caused serious or substantial harm or injury. The type of personal data involved in the Incident (as set out at [5] above) has already been taken into consideration when deciding on the quantum of the financial penalty to be imposed and, as such, no further reduction in the quantum is warranted.

15 The Organisation's deletion of the user database is an aggravating factor that affected the Commission's investigations. The number of affected individuals estimated by the Organisation could not be verified given their deletion of the user database. The Organisation was notified about the Incident by a security researcher on 4 June, verified that user account information had been exfiltrated, and by 20 June it had shut down the forum and deleted the user database: see [8]. These decisions were made within a short period of 2 weeks but cast a shadow stretching far into the future. By the time the Organisation was formally notified that

the Commission was commencing investigations in November 2018, the user database had been expunged for 5 months.

16 In *Re NTUC Income Insurance Co-operative Ltd* [2018] SGPDPC 10, the Commission stated that all organisations have the duty to preserve evidence and that it does not look favourably on the destruction or deletion of potentially relevant documents and records. The decision sets out some of the factors that the Commission would take into account in determining whether or not an organisation would be sanctioned for such deletion or destruction. These factors include whether or not the deletion prejudiced a fair investigation and whether or not legal proceedings were anticipated or contemplated. In this case, investigations were prejudiced given that the number of affected individuals could not be verified.

17 The Organisation made representations stating that it had deleted the user database to comply with section 25 of the PDPA, which imposed an obligation on organisations to cease retention of personal data once the purpose for its collection is met, and retention is no longer necessary for legal or business purposes. The Organisation submitted that section 25 applied to a situation where there was an ongoing legal course of action or a risk of potential litigation, neither of which existed at the time. The Organisation's interpretation of section 25 is unnecessarily narrow. As the Commission held in *NTUC Income Insurance Co-operative Ltd*, section 25 allows for the retention of personal data where it is required for legal purposes such as investigations by the Commission.

18 The question is whether, in June 2018 when the user database was deleted, the Organisation could have anticipated an investigation by the Commission. There are a number of facts that the Organisation should have considered before deciding to delete the user database. First, the source of information about the exfiltration was an *external* security researcher; second, the nature of notification was that the security researcher had received personal data extracted from the Forum from a *third party source*; third, the Organisation verified that personal data from *484,512 user accounts* had been exfiltrated: see paragraph 4. Collectively, these facts point to a not insignificant data breach that affected a significant number of users, anyone of whom might initiate a complaint.

19 The Organisation ought to have retained the user database offline for a period, but could have limited access to it. It is not necessary at this point to venture an opinion about how long the Organisation ought to have preserved the user database. The necessity of preservation and the period of preservation is determined on the facts of each case. What can be said is that the decision to delete the user database within 2 weeks of discovering the Incident was taken too hastily.

20 The Organisation made representations stating that it had not deleted the user database in bad faith. Whilst it has been said that the decision was taken too hastily, there is no evidence to suggest that the decision was taken in bad faith or in order to put evidence beyond the reach of investigations. These are not considerations that factored in the determination of the directions.

21 The Commissioner hereby directs the Organisation to pay a financial penalty of $15,000 within 30 days, 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.

22 The Commissioner decided not to impose any other direction as the Organisation has ceased to operate the Forum and no longer retains the database of Forum users.

YEONG ZEE KIN
DEPUTY COMMISSIONER
FOR COMMISSIONER FOR PERSONAL DATA PROTECTION