SPH Magazines Pte Ltd

[2020] SGPDPC 3

Tan Kiat How, Commissioner — Case No DP-1802-B1731

Data Protection – Protection obligation – Unauthorised access to personal data – Insufficient security arrangements

31 January 2020

Facts of the Case

1 On 20 February 2018, SPH Magazines Pte Ltd (the "**Organisation**") voluntarily notified the Personal Data Protection Commission (the "**Commission**") that the account of a senior moderator of its HardwareZone forum site (the "**Forum**") had been accessed by an unknown hacker who used the senior moderator's credentials to retrieve personal data of members of the Forum. The Organisation subsequently discovered through its consultants who were engaged to assist in its investigations into the incident that the senior moderator's email address and password had been published on a credential leak database on 5 December 2017. The Organisation believed that the hacker had obtained the senior moderator's credentials from this source or other similar databases as its investigations showed that its systems and applications had not been compromised during the incident.

2 The Organisation operates, hosts and maintains the Forum, an online Internet portal for members to engage in discussions on technology and other matters. Members are required to provide their usernames, email addresses, full names and passwords during registration and this personal data would form part of a member's user profile. Members also have the option of including the following personal data in their user profile:

(a) Year of Birth

(b) Gender

(c) Country

(d) Education

(e) Job Scope

(f) Role in IT Procurement

(g) Occupation

(h) Industry

(i) Company Size

(j) Monthly Income (range)

(k) Area of interest

(l) Home Page URL

(m) Use of MSN, Yahoo, ICQ, AIM, Skype

3 Senior moderators of the Forum are volunteers selected by the Organisation from amongst the members of the Forum and appointed to review and moderate the discussion threads in the Forum and to ensure that any postings comply with applicable laws and the Forum's Terms of Service. Senior moderators are also responsible for issuing warnings and other sanctions (such as suspensions or bans) to members who do not comply with the Forum's Terms of Service. Access to members' user profiles was given to senior moderators (through their respective senior moderator accounts) to allow them to carry out their duties. The senior moderators would be able to view the Forum members' usernames, email addresses and any optional information included by the members in their user profiles. While the full names and passwords of the members were salted and hashed using the MD5 algorithm, and ordinarily senior moderators would not be able to view these fields, it is well-known that the MD5 algorithm is outdated and could be circumvented: see *Fei Fah Medical Manufacturing Pte Ltd* [2016] SGPDPC 3 at [19] and [20].

4 The Organisation first realised that something was amiss when it was notified of an unauthorised post published using the account of a website administrator. The website

administrator is employed by the Organisation. Using the administrator's credentials, the hacker published the unauthorised post and changed the avatar of the administrator account. However, as the Forum administrators could only access the user profiles of members by way of a two-factor authorisation ("**2FA**") process, the hacker was unable to access the user profiles using the administrator account.

5 The Organisation also subsequently discovered the website administrator's credentials in the same credential leak database which published the senior moderator's credentials.

6 It thus appears that the hacker used the compromised senior moderator account to access the user profiles of members. At the material time, there were a total of 685,393 user profiles in the Organisation's system. The Organisation's investigations further showed that the senior moderator's account was used to perform 704,764 attempted views of Members' user profiles using networks that did not reveal the actual source IP address, between 22 September 2017 to 30 September 2017. The frequent number of attempted views and the use of networks which are difficult to trace suggest that the senior moderator's account was used to access personal data of Members without authorisation. The investigations also showed that the senior moderator's account experienced unusual activity from at least December 2015.

7 Upon being notified of the Incident, the Organisation took the following remedial actions:

(a) The access rights of senior moderator accounts to user profiles was temporarily suspended on 19 February 2018;

(b) The Organisation sent emails to members informing them of the breach and advising members to change their passwords. The Organisation also posted a notification of the breach on the Forum website.

(c) The Organisation revised its Password policy on 23 February 2018 requiring passwords to have a minimum of 8 characters and include both alphanumeric and upper/lower case characters. Passwords will also expire within 3 months;

(d) 2FA was implemented for senior moderator accounts in April 2018;

(e) Captcha for the Site's login page was implemented;

(f) Entries in the filed for full names was removed from the application level and purged from the database; and

(g) Additional information in optional fields were also removed from the application level and purged from the database.

Findings and Basis for Determination

8 Section 24 of 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.

9 The key finding in this case was that the Organisation had omitted to implement reasonable password security requirements for its senior moderators. While the Organisation did have in place a Password Policy which, amongst other things, required passwords to be of a certain length and complexity and provided for the expiration of passwords, the Policy and the security measures therein were applicable to the Organisation's employees and did not apply to senior moderators. In fact, there was no requirement for senior moderators to change their passwords regularly or to have passwords of an acceptable length and complexity.

10 During the investigations it was discovered that the password used by the relevant senior moderator was not changed in 10 years and did not meet the length and complexity standard the Organisation implemented for its employees. In this regard, the permissions and privileges granted to senior moderators allowed senior moderators to set password expiry rules and to set prohibitions for the re-use of passwords within a selected period (i.e. password history setting) but did not compel them to do so.

11 Finally, the Organisation did not perform any security testing of the Forum website. It therefore did not have an overall picture of its security needs in relation to the website.

12 The failure to implement and enforce reasonable password security requirements on the senior moderator accounts and to conduct security testing to acquire knowledge of the Forum website's security amounted to a breach of section 24 of the PDPA by the Organisation.

The Commissioner's Directions

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

Mitigating factors

(a) the Organisation voluntarily notified the Commission of the Incident and members of the Forum promptly;

(b) the Organisation took prompt action to implement measures to prevent a recurrence of such an incident;

(c) the Organisation cooperated with the Commission's investigations;

Aggravating factors

(d) The password which was compromised had not been changed for a very long period of 10 years; and

(e) The Organisation was unable to detect the unauthorised access of personal data for about 2 years.

14 Having carefully considered all the relevant factors of this case, the Commissioner directs the Organisation to pay a financial penalty of $26,000 within 30 days of the date of this 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 such financial penalty until the financial penalty is paid in full. No additional directions are required in light of the remedial measures taken by the Organisation.
