DECISION OF THE PERSONAL DATA PROTECTION COMMISSION

Case Number: DP-1411-A213

THE INSTITUTION OF ENGINEERS SINGAPORE

…Respondent

Decision Citation: [2016] SGPDPC 2

GROUNDS OF DECISION

20 April 2016

Background

1. The Institution of Engineers Singapore (UEN S66SS0041B) ("**IES**") is a society registered with the Registry of Societies. IES was formally established on July 1966 as the national society of engineers in Singapore. Its functions include the accreditation of engineering academic programmes (through its Engineering Accreditation Board); the maintenance of professional registries; and the promotion of social, business, professional, and career development amongst engineers in Singapore.

The IES Website

2. IES operates a website at www.ies.org.sg ("**Site**"), which consists of both publicly-accessible pages, and a members' portal, accessible only by members of IES, upon logging into the portal with their respective user identifications ("**IDs**") and passwords. The Site also allows members of the public, who are non-IES members, to create an account on the Site in order to login to access and post on the Site's forums.

3. According to information provided by IES, the functions of the Site include:

   (a) enabling members to update their membership details such as addresses, emails and contact information;

   (b) applying for courses and events that are created by IES;

   (c) applying for email addresses with ies.org.sg domain, e.g., abc@ies.org.sg;

   (d) payment for membership and courses via PayPal;

   (e) accessing webmail;

   (f) allowing members to search for information about other members;

(g) publishing information on IES events, courses, seminars, job listings, and information on various registries (e.g., ABC Waters Professional Registry and others);

(h) applying for IES membership; and

(i) accessing IES forums.

4. Members of IES who log in to the Site using their membership user IDs are able to access certain dedicated membership Site functions, including receipt of *ad hoc* AGM notices, quick poll functions, profile updates, and change of passwords.

Data Leak Incident

5. On 1 October 2014, the Personal Data Protection Commission ("**Commission**") was informed that the information of users of the Site had been posted on http://pastebin.com ("**Pastebin**"), a website which allows members of the public to post and share information online (the "**Data Leak**").

6. The relevant information was ostensibly uploaded onto the Pastebin website by a Pastebin user with the username "KAMI_HAXOR", in the form of two posts in plain text that could be publicly viewed by any visitor to the Pastebin website. The two posts were dated 30 September 2014 and were respectively captioned:

(a) "*IES.ORG.SG 6,000+ Usersnames + pass Leaked by KaMi HaX*" (the "**User ID List**"); and

(b) "*Ies.org.sg 60,000+ Users Data Leaked by KaMi HaXor*" (the "**Additional List**").

7. The User ID List was titled "*The Institution of Engineers Singapore 6000= [sic.] users , 90,000+ Mobiles leaked By KaMi HaXor… Target= http://www.ies.org.sg/*", and contained a list of characters separated with a colon, in the format "XXXX:XXXX", which was labelled "MemberId:Pass".

8. The Additional List was titled "*The Institution of Engineers Singapore 60,000+ Mobiles leaked By KaMi HaXor… Target= http://www.ies.org.sg/*", and contained a list of eight-digit numbers that were consistent with the format of Singapore telephone numbers.

9. In light of the information received, the Commission commenced an investigation under section 50 of the Personal Data Protection Act 2012 (No. 26 of 2012) (the "**Act**") to ascertain whether there had been a breach by IES of its obligations under the Act.

Nature of the Data Leak Incident

10. IES informed the Commission that the passwords and IDs in the User ID List were those of IES members and that it was made aware of the Data Leak by one Nicholas Lee, who had written to IES on 1 October 2014 at 10.13 am, to inform IES about the Data Leak.

11. IES also provided the Commission with a copy of a Site audit report which was conducted by its website vendor, Forecepts Pte. Ltd. ("**Forecepts**"), using Acunetix software, in the aftermath of the Data Leak. The report, titled "Acutenix Website Audit Developer Report", dated 3 November 2014 ("**1st Scan Report**") indicated a number of vulnerabilities with the Site, including 48 high-severity vulnerabilities in the Site set out below:

High-Severity Type Vulnerability Identified	**Variation**
Blind SQL Injection	1
Cross site scripting	8
Cross site scripting (verified)	30
Cross site scripting [stored] (verified)	1
FCKeditor spellchecker.php cross site scripting vulnerability	2
HTML Form found in redirect page [high severity]	4
jQuery Cross Site Scripting	1
PHP allow_url_fopen enabled	1

12. Forecepts suspected that the attack on the Site was likely to have been caused by cross-site scripting but was unable to confirm this. In any case, the Commission notes that cross-site scripting was identified in the 1st Scan Report as a high-severity vulnerability that existed in the Site.

13. In relation to the number of individuals affected by the Data Leak, the Commission notes that the titles of the User ID List and the Additional List respectively indicate that the data of more than 6,000 users had been disclosed in the User ID List, and that the data of more than 60,000 users had been disclosed in the Additional List. However, IES submitted that it was unable to identify the total number of IES members which were affected by the Data Leak, as the "*data published online are in random*".

14. At the time of this decision, both the User ID List and the Additional List appear to have been removed from the Pastebin website.

15. Having reviewed the relevant facts and circumstances, including the written responses to the NTPs submitted by IES, the Commission sets out below its findings and assessment in relation to the Data Leak.

THE COMMISSION'S FINDINGS AND ASSESSMENT

Personal Data Leaked

16. "Personal data" is defined under section 2 of the Act, as follows:

> "'*personal data' means data, whether true or not, about an individual who can be identified –*
>
> *(a) from that data; or*
>
> *(b) from that data and other information to which the organisation has or is likely to have access.*"

17. As noted above, IES admitted that the passwords and IDs in the User ID List belonged to its members. According to publicly-available information on the Site, IES's membership comprises both individuals and organisations. Organisation members may be represented in IES by up to two individuals from the organisation. Individuals who are not part of any organisation can also join as members of IES with the relevant engineering qualifications.

18. IES also acknowledged that the personal data of its members was stored in its web server and could be retrieved using the members' respective user IDs and passwords. In particular, IES stated that "*personal data such as Member ID, Name, Contact, Email and Address were stored in the database in www.ies.org.sg.*"

19. In light of the foregoing, it is clear that the person or persons who had obtained and posted the User ID List on the Pastebin website in the first place, as well as any member of the public who came across the User ID List on the Pastebin website, could have used the IDs and passwords disclosed to log in to the accounts of individual and organisation members (represented by their nominated employees) on the Site, and thereby access personal data relating to these members that was stored on the Site.

20. Furthermore, given that anyone who had obtained a valid user ID and password combination would have been able to log in to the Site to retrieve personal details relating to the respective IES member, the Commission is of the view that anyone with a valid user ID and password combination would effectively be able to access the entire profile of an IES member and identify him or her. Accordingly, the Commission is of the view that the user IDs and passwords that were leaked would fall within the definition of "personal data" under the Act.

21. The Commission notes that IES had taken the view that the possibility of any individual using the information in the User ID List to access the personal data in IES's webserver was remote as the listing of user IDs and passwords were "random, unrelated and unlinked". IES was also of the view that it was unlikely that the person or persons who had obtained and posted the User ID List on the Pastebin website had used the IDs and passwords displayed to log in to

the accounts of its members on the Site to access personal data stored on the Site "or he would have placed the relevant information in a different (database) format" (sic).

22. The Commission disagrees with the views expressed by IES. The risk of access by any individual using the user IDs and passwords combination in the User ID List is not remote. The User ID list is effectively a dictionary of valid user IDs and passwords that can be used in a dictionary attack. With automatic scripting, an individual can log in to any IES member's account notwithstanding that the manner in which the user IDs and passwords had been presented in the list appeared "random, unrelated and unlinked". Indeed, the Commission cannot exclude the possibility that the person or persons who had obtained and posted the User ID List on the Pastebin website may have already done so notwithstanding the lack of complaints of abuse of personal data from IES members thus far.

23. Accordingly, it is clear that, as a result of the Data Leak, the security of personal data relating to IES members was compromised as such personal data could have been accessed by one or more unauthorised persons with knowledge of the leaked user IDs and passwords.

Personal Data under the Possession and Control of IES

24. The Commission notes that, at all material times, the Site was fully owned and administered by IES. For completeness, the Commission also notes that although IES had engaged two vendors for the Site, these vendors undertook their respective functions on behalf of IES and did not own or administer the Site:

    (a) Forecepts, as IES's website vendor, was engaged to supply and design the website design and Content Management System. Forecepts was also engaged to provide maintenance to the Site, but only upon request by IES; and

    (b) the Site was hosted at the premises of ReadySpace (SG) Pte Ltd ("**ReadySpace**"), IES's hosting service provider, on a dedicated server.

25. Further, the Commission's investigations found that there were four individuals within IES who could access the list of member IDs and passwords and personal data relating to IES members. These were IES's IT manager, IT executive, membership manager, and membership executive.

26. Accordingly, the Commission is satisfied that, at all material times, the relevant personal data of IES members, which was stored on the Site and whose security was compromised as a result of the Data Leak, was in the possession and/or under the control of IES.

Adequacy of Security Arrangements

27. Section 24 of the Act states:

> "***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 unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks.*"

28. Pursuant to section 24 of the Act, IES, being an organisation which had its members' personal data under its possession and/or control, is required to make reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks (the "**Protection Obligation**").

29. IES informed the Commission that it had put in place the following security measures at the material time:

    (a) the Site's server was hosted in a secure site and in a dedicated server, and protected by a firewall and anti-virus software (namely, Parallels Plesk Panel 11.0.9);

    (b) software updates had been performed on the Parallels Plesk Panel 11.0.9 firewall and anti-virus software; and

    (c) a list of user IDs and passwords relating to the IES members could be extracted from the members' portal and saved; however such a function could only be performed by the four individuals within IES who could access the list of member IDs and passwords (namely, IES's IT manager, IT executive, membership manager, and member executive). Forecepts was also authorised to access such a function for the purposes of maintaining, troubleshooting, and updating the Site.

30. However, from the Commission's investigations, it was also apparent that:

    (a) the Site had not provided for the encrypted storage of member passwords;

    (b) prior to the Data Leak, no audit had been conducted on ReadySpace's enterprise hosting services and/or the security of the Site;

    (c) IES had not conducted any penetration testing on the Site, and was not aware of penetration testing software; and

    (d) while IES represented that it had made phone calls to its vendors ReadySpace and Forecepts to inform them about the Act, there was no indication that IES had otherwise given instructions to its vendors to make security arrangements so as to ensure that personal data stored

in the Site would be protected in compliance with IES's obligations under the Act. Furthermore, the contractual terms between IES and its vendors, as submitted by IES, did not appear to contain any specific security arrangements or requirements for its vendors to put in place security measures to safeguard IES members' personal data stored in the Site.

31. In addition, as already mentioned earlier, the 1st Scan Report by Forecepts following the Data Leak indicated that there existed a number of vulnerabilities with the Site, including 48 high-severity vulnerabilities such as cross-site scripting and SQL injections.

32. Cross-site scripting is a common web vulnerability, which could have been easily detected by performing a vulnerability scan, such as the one performed by Forecepts after the Data Leak. Once identified, the vulnerabilities can be patched according to the many guides that are readily available on the Internet. The conduct of vulnerability scans using automated tools like Acunetix is considered industry best practice.

33. In this case, IES acknowledged that it had not undertaken any sort of audit to detect security vulnerabilities on the Site. IES had also not demonstrated that it had made any effort to require its vendors to evaluate and/or ensure the security of personal data stored on the Site.

34. While the Site may have had a firewall and anti-virus software in place, these measures alone were clearly inadequate to reasonably ensure the security of personal data stored in the Site, as the firewall and anti-virus software would not protect against common vulnerabilities such as cross-site scripting. This would have been apparent, and indeed was made apparent, by a vulnerability scan such as the one conducted by Forecepts after the Data Leak.

35. From the above, it would appear that prior to the Data Leak, IES had made insufficient effort to inquire into and/or ensure the security of personal data stored on the Site. As a result, numerous security vulnerabilities existed in the Site at the time of the Data Leak, which could have been reasonably detected and patched by available means.

36. In light of the foregoing, the Commission is of the view that IES has failed to make reasonable security arrangements in respect of personal data relating to its members, as required under the Protection Obligation.

THE COMMISSION'S DIRECTIONS

37. In its representations to the Commission, IES took the position that it was a small organisation that had relied on external specialists for security related advice and hence should not be heavily penalised for any breaches of the data protection provisions. IES was of the view that its external specialists had not advised any actions on possible areas of protection and/or detection until the breach to the Site occurred.

38. However, the Commission notes that IES' claims regarding its reliance on external specialists were not borne out by the investigations. Further, IES, as an organisation with several thousand members, cannot be described as "a small organisation".

39. In determining the directions to be given to IES, the Commission has given due consideration to all the relevant factors, including the following:

    (a) IES was cooperative and forthcoming throughout the Commission's investigation;

    (b) following its discovery of the Data Leak on 1 October 2014, IES promptly took the following measures to manage the effects of the Data Leak:

        (i) disabling of the members' portal on the Site;

        (ii) changing of the passwords for all IES members' accounts, and resetting of the passwords for its administrator accounts in the members' portal;

        (iii) on 2 October 2014, IES sent an email notification to all IES members, informing them of the "hacking activity" on the Site, as well as the measures (listed in (i) and (ii) of this paragraph 43(b)) IES had taken to minimise damage; and

        (iv) removal of the telephone numbers and addresses of IES members previously stored on the database of the Site;

    (c) following the Data Leak, IES implemented the following additional security measures:

        (i) instructed Forecepts to conduct a security audit of the Site and to patch up any vulnerabilities detected pursuant to such audit, and to conduct a monthly audit on the Site upon completion of the security hardening process;

        (ii) installation of a new intrusion detection system, along with endpoint protection in the Site's server; and

        (iii) installation of Secure Sockets Layer ("**SSL**") certification in the Site's server; and

    (d) the high-severity vulnerabilities identified in the 1st Scan Report pursuant to Forecepts' audit of the Site appear, from the Acunetix Website Audit Developer Report dated 12 January 2015, which was provided by IES to the Commission, ("**2nd Scan Report**"), to have been patched by Forecepts.

40. Pursuant to section 29(2), and having completed its investigations and assessment of this matter, the Commission is satisfied that IES was in breach of the Protection Obligation under section 24 of the PDPA. Having carefully considered all the relevant factors of this case, the Commission hereby directs IES to do the following:

(a) IES shall within 60 days from the date of the Commission's direction:

(i) conduct a further vulnerability scan of the Site; and

(ii) patch all vulnerabilities identified by such scan;

(b) IES shall, in addition, submit to the Commission by no later than 14 days after the conduct of the abovementioned vulnerability scan, a written update providing details on:

(i) the results of the vulnerability scan; and

(ii) the measures that were taken by IES to patch all vulnerabilities identified by the vulnerability scan; and

(c) IES shall pay a financial penalty of S$10,000.00 within 30 days from the date of the Commission's direction, failing which interest shall be payable on the outstanding amount of such financial penalty.

41. The Commission emphasises that it takes a very serious view of any instance of non-compliance under the PDPA and with the Commission's directions.

LEONG KENG THAI
CHAIRMAN
PERSONAL DATA PROTECTION COMMISSION