7 January 2020

Data Protection: Protection Obligation

Recent PDPC decisions

Between August and September 2019, the Personal Data Protection Commission ("**PDPC**") imposed financial penalties of S$25,000, S$40,000 and S$60,000 on Singapore Telecommunications Limited ("**SingTel**"), Marshall Cavendish Education Pte. Ltd. ("**MCE**") and Learnaholic Pte. Ltd. ("**Learnaholic**") respectively, for failing to make reasonable security arrangements to comply with their protection obligations under the Personal Data Protection Act ("**PDPA**").

In SingTel's case, an anonymous informant reported to the PDPC that a design issue in the Application Programming Interface ("**API**") linking the "My Singtel" mobile app with the SingTel servers could be exploited to access the account details of SingTel customers. The vulnerability was a relatively basic design issue and well-known security risk that a reasonable person would have considered necessary to detect and prevent. A third party security vendor had been engaged by SingTel to conduct regular security penetration tests, and had advised SingTel to take precautions against this specific vulnerability. However, SingTel omitted to conduct a full review of its systems, hence failing to discover the vulnerability that was exploited.

In MCE's case, a ransomware attack on 1 February 2017 on MCE's network compromised the personal data of more than 250,000 individuals. The primary cause of the ransomware attack was a change made to a firewall rule to allow internet access to the server, which was not reinstated. This allowed the external perpetrator to gain entry into the system to upload and execute the ransomware. MCE had also installed remote access software on the backup server, which would have allowed an attacker a greater chance of success in infiltrating it. While MCE did put in place certain policies to prevent such data breaches from taking place, the PDPC found that MCE failed to take practicable steps to *implement* these policies.

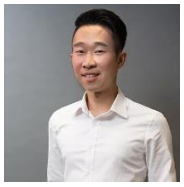
In IT vendor Learnaholic's case, Learnaholic opened a port in a school's firewall and disabled the password for server software, to enable remote troubleshooting. The vendor failed to restore the original firewall configuration. This led to the creation of a vulnerability which was exploited by a hacker and the personal data of approximately 48,000 individuals was compromised. The PDPC found that the data breach incident occurred due to a series of lapses on the part of Learnaholic, all of which could have been reasonably averted, such as reinstating firewall configurations after remote troubleshooting and encryption of personal data that is sensitive or when sent in bulk.

Under Section 24 of the PDPA, an organisation is required 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 above cases illustrate the standards to which the PDPC holds organisations for compliance with this Protection Obligation.

If you would like to find out more details on the above cases or your organisation's obligations under the PDPA, you may contact us:

Wilson Wong
Director
wilson.wong@amicalaw.com
(65) 6303 6213

Nicholas Tong
Senior Legal Associate
nicholas.tong@amicalaw.com
(65) 6303 8397



Dawn Chua
Legal Associate
dawn.chua@amicalaw.com
(65) 6303 8191