LHAG

SPECIAL ALERT!

Technology, Media & Telecommunications

G. Vijay Kumar
Partner
TMT
E: vkg@lh-ag.com

Wee Yun Zhen
Associate
TMT
E: wyz@lh-ag.com

Nicole Shieh E-Lyn
Associate
TMT
E: sel@lh-ag.com

Harvey Ng Yih Xiang
Associate
TMT
E: nyx@lh-ag.com

James Lau Jian hui
Pupil-In-Chambers

Navigating Data Breach: Recent Insights and Analysis

23 JUNE 2023

Our previous alert[1] discussed the potential legal exposure of companies in the event of a data breach. In this alert, we will examine the latest Singaporean cases of data breach investigated by the Singapore Personal Data Protection Commission ('**PDPC**') and provide a summary of its key takeaways.

Fortytwo Pte. Ltd. [2023] SGPDPCS 3

Fortytwo ran an online store selling furniture. Unfortunately, as a consequence of a data breach, the personal and credit card information of thousands of customers were compromised. The cyberattack was successful primarily due to the company website's outdated security protocols.

Investigations by the PDPC found that Fortytwo breached its obligations under the Singapore Personal Data Protection Act 2012 ('**PDPA**') as it had failed to install security patches despite its availability four years prior.

[1] Access our previous alert here: <https://lh-ag.com/employment-legal-exposure-of-a-company-in-the-event-of-a-data-breach>

Moreover, Fortytwo had also neglected to upgrade its utilised software to a version that is supported with updates despite reminders by the developers to do so. Consequently, Fortytwo was directed by the PDPC to upgrade its software and conduct a cybersecurity vulnerability assessment within six months. It was also slapped with a financial penalty of SGD8,000.

Kingsforce Management Services Pte Ltd [2023] SGPDPCS 1

This case involved a recruitment firm which had an extensive database of approximately 54,900 jobseekers' information. After a cyberattack, the data stolen from the database (which includes personal data, educational qualifications, and salary information) was put up for sale on online forums by the threat actors.

The PDPC's investigations concluded that Kingsforce had breached its obligations under the PDPA by failing to monitor and ensure that the website developed by IT vendors satisfied the requisite digital security requirements, such as; regular patching, updates and upgrades for all software and firmware. Moreover, Kingsforce also failed to conduct a periodic security assessment on its website. Accordingly, Kingsforce was instructed to implement the necessary security upgrades as directed by the PDPC within a specific time frame. No fine was deemed appropriate in this case due to, amongst others, the company's efforts made towards the security of the website, cooperation rendered to the PDPC and the voluntary admission of the breach.

Sembcorp Marine Ltd [2023] SGPDPCS 2

Sembcorp Marine is an engineering group specialising in the construction and repair of offshore structures and naval vessels. The cyberattack caused the personal information of approximately 25,925 employees of Sembcorp Marine to be compromised. The threat actors exploited a then newly discovered weakness within Sembcorp Marine's software application known as the

Log4J zero-day vulnerability which had also consequently plagued many other corporations worldwide.[2]

Despite the cyberattack's success, the PDPC concluded that Sembcorp Marine had sufficiently carried out its obligations under the PDPA 2012 for two reasons. First, Sembcorp Marine had, prior to the attack, carried out regular assessments of its cybersecurity protocols. Second, subsequent to the attack, Sembcorp Marine immediately took action to reduce their reliance on the vulnerable software. In addition, the PDPC noted that Sembcorp Marine was one of the earliest targets where this vulnerability was exploited and thus, would have little chance of anticipating and defending against the cyberattack.

Key takeaways

Given the similarities between the Protection Obligation under Section 24 of the Singaporean PDPA and the Security Principle under Section 9 of the Malaysian Personal Data Protection Act 2010, Malaysian companies are advised to implement the following best practices to comply with personal data protection regulations:

(a) Promptly install all available security patches for software;

(b) ensure that all utilised software are currently supported by the developer;

(c) observe industry guidelines on data protection;

(d) undertake periodic security reviews of all software;

[2] NehaPradhan Pruhani, 'Log4j Zero-Day Vulnerability: Everything You Need To Know About the Apache Flaw' (Spiceworks, 1 August 2022) <https://www.spiceworks.com/it-security/vulnerability-management/articles/log4j-apache-vulnerability-everything-you-need-to-know/> accessed 20 June 2023

(e) monitor the performance of third parties responsible for the Company's cybersecurity;

(f) enforce password complexity and renewal protocols;

(g) promptly take action to remedy any discovered vulnerabilities in the software, both prior and subsequent to a cyberattack;

(h) provide periodic training to employees on data protection measures; and

(i) provide full and prompt cooperation with the relevant authorities.

If you have any queries, please contact associates, **Wee Yun Zhen** (wyz@lh-ag.com), **Nicole Shieh E-Lyn** (sel@lh-ag.com), **Harvey Ng Yih Xiang** (nyx@lh-ag.com),or their team partner, **G. Vijay Kumar** (vkg@lh-ag.com).

Head Office
Level 6, Menara 1 Dutamas
Solaris Dutamas
No. 1, Jalan Dutamas 1
50480 Kuala Lumpur
Malaysia
Tel: +603 6208 5888
Fax: +603 6201 0122

Johor Office
Suite 21.01
21st Floor, Public Bank Tower
No.19, Jalan Wong Ah Fook
80000 Johor Bahru, Johor
Tel: +607 278 3833
Fax: +607 278 2833

Penang Office
51-12-E, Menara BHL Bank,
Jalan Sultan Ahmad Shah,
10050
Penang
Tel: +604 299 9668
Fax: +604 299 9628

Email
enquiry@lh-ag.com

Published by TMT Practice