MARSH

June 2018

CLIENT ALERT

PAGE UP DATA BREACH

Human resources service provider, PageUp, reported on 23 May 2018 that unusual activity was detected on its IT infrastructure. Following a forensic investigation, it was found that client data may have been compromised and unofficial reports have indicated the breach was caused by the introduction of malware to the company's IT systems. PageUp has confirmed there is no evidence that the threat is still active[1].

Australian company PageUp manages millions of job applications globally and also provides software to collect salary details, bank information, tax file numbers and other sensitive data.

The personal information of thousands of Australians has potentially been compromised, with some local companies confirming that job applicants may have had bank details, tax file numbers, home addresses and birth dates disclosed.

IMMEDIATE STEPS TAKEN

PageUp has notified various data regulators and government organisations of this potential breach. This includes the UK Information Commissioner's Office, the Australian Cyber Security Centre and the OAIC ("OAIC"). The OAIC has confirmed it is working with PageUp to investigate the breach[2].

Some PageUp customers have confirmed they have taken precautionary action and suspended all career portals whilst investigations continue.

CYBER INSURANCE RESPONSE

Given the significant number of individuals whose personal information may have been compromised, the PageUp incident represents the first major data breach since the introduction of the Australian Notifiable Data Breach ("NDB") scheme in February this year. The scheme requires mandatory notification of all eligible data breaches to the OAIC and individuals at risk of serious harm following a breach of their personal information.

For companies that operate outside of Australia and/or hold the personal information of non-Australian citizens, it is critical to also consider the requirements of data privacy legalisation in other relevant jurisdictions. This may include the recently introduced General Data Protection Regulation ("GDPR") that governs the treatment of personal data of data subjects in the European Union. The GDPR in particular contains strict mandatory notification requirements that may apply.

Additionally it is also critical for an organisation to review its third party supplier relationships to establish where notification responsibilities lie in the event of an eligible data breach.

In Australia, even if a business outsources its data storage and/or processing, it may still be subject to the NDB scheme. If a single eligible data breach applies to multiple entities, the NDB scheme only requires one entity to notify the OAIC and the individuals at risk of serious harm. However if the correct process is not followed, then all entities may be held to be in breach of the legislation.

An insurance policy should not act as the primary solution for managing a company's exposure to cyber-attacks or data breaches, however, mitigating cyber risk costs through insurance plays an important role in the overall risk management protocols of a business. There are many costs that can impact a company in the event of a privacy breach by it or a third party supplier and insurance can assist in providing support for some of these costs.

PageUp is a third party provider for businesses. Depending on the terms and conditions of a policy wording, there may be scope for coverage to extend to data breaches that arise from the network of a supplier or a vendor. Items covered may include:

- Notification costs incurred in advising affected individuals
- Increased costs of working that may arise
- IT forensic costs to assess the breach and ensure this has not spread to an insured's system
- Legal costs to notify regulators
- PR costs to assist in reducing potential damage to brand
- Legal defence costs and damages for liability claims arising from affected individuals

We recommend that organisations utilising PageUp services, and that currently purchase cyber insurance, notify their insurers as a precaution. Separate to whether or not cyber insurance is purchased, we also recommend that independent legal advice is sought to determine if notification to a regulator(s) and/or affected individuals is required.

MARSH CONTACT:

If you would like further information, please contact your servicing broker, Kelly Butler or Kristine Salgado.

Kelly Butler
National Cyber Leader, Australia
+61 3 9603 2194
kelly.butler@marsh.com

Kristine Salgado
Managing Principal, FINPRO
+61 3 9603 2871
kristine.salgado@marsh.com

[1] https://www.pageuppeople.com/unauthorised-activity-on-it-system/

[2] https://www.oaic.gov.au/media-and-speeches/statements/statement-on-pageup-people-limited