MARSH JLT SPECIALTY

OCTOBER 2020

Cyber Risk and Insurance Solutions

Risk in Focus – Professions: Real Estate

MARSH

Contents

Introduction

Cyber incidents are increasing in both volume and severity across all business sectors with the number of cyber threats seen in the first half of 2020 exceeding all of 2019[1]; the real estate industry being no less immune to cyber threats than any other.

The real estate industry has become widely digitised, utilising innovative technologies to transform the traditional home buying and renting experience by enabling features such as virtual open homes, online auctions and digital sale and purchase agreements. The COVID-19 pandemic has also accelerated trends to adopt remote working tools and a further reliance on technology to support business operations.

Online communication methods ranging from negotiation to payment transfers are now industry standards which increases the potential for payment diversion fraud. Furthermore, a wealth of personal information is collected by real estate firms and there is plenty of potential for harm should this information fall into the hands of malicious parties.

1 Vijayan, J. (2020, September 15). More Cyberattacks in the First Half of 2020 Than in All of 2019. Retrieved from https://www.darkreading.com/attacks-breaches/more-cyberattacks-in-the-first-half-of-2020-than-in-all-of-2019/d/d-id/1338926

Real Estate – In the Crosshairs

In addition to the traditional duties associated with handling physical brick and mortar transactions, many real estate businesses are now reliant on digital connectivity for their day-to-day operations (e.g. the integration of third party software or platforms as part of their technology suite) and regularly collect personal information on countless individuals in respect of private viewings and open homes. Even prevention controls such as anti-malware detection and multi-factor authentication for remote access are being circumvented by innovative cyber-criminal organisations with increasingly sophisticated hacking tools.

With an increased digital footprint, the real estate industry is proving to be a consistent target of social engineering (invoice payment fraud) attacks and breaches of personally identifiable information via customer databases. Concerningly these have also been used in follow up attempts at identity fraud. Social media accounts for real estate agents and businesses have also reportedly been hacked in acts of digital vandalism.[2] Day-to-day business activity could also be disrupted if a major system or software service provider were to be impacted by a cyber incident as well.

Recent events highlight the growing consequences of cyber-attacks targeting the real estate industry around the world and in the Pacific region:

- A California property management company had an online database compromised by cyber-criminals which was only been discovered six months after the breach occurred. Stolen data belonging to the company's customers may have included rental applications which contained personally identifiable information such as name, date of birth, social security number, driver's licensing details and a home address – all of which could be used for identity fraud in follow up attacks.[3]
- ASX-listed property valuation firm Landmark White was made aware of a cyber breach in February 2020 forcing the company into a trading halt. The company expects to lose up to $7 million in revenue as a result of the breach and their CEO elected to resign as a result of this breach. The company resumed trading in May with the share price plummeting by 40%.[4]
- The Office 365 network of a real estate agency in New Zealand was compromised resulting in a malicious third party gaining access to internal communications. The fraudster then intercepted an email thread and impersonated an agent to redirect a deposit payment from a buyer. After discovering the lost funds, the buyer subsequently lodged a liability claim on the agency in respect of the diverted funds, in which only a portion was recoverable by the bank.

2 Russell, L. (2020, February 12). New Zealand agent claims Facebook page was hacked. Real Estate Business – News for real estate professionals. https://www.realestatebusiness.com.au/breaking-news/19497-new-zealand-agent-claims-facebook-page-was-hacked

3 https://www.infosecurity-magazine.com:443/profile/sarah-coble/. (2020, April 6). Data Thieves Hit California Property Management Company. Retrieved from https://www.infosecurity-magazine.com/news/data-thieves-hit-wolfeassociates/

4 Cyber attacks on the rise for the real estate industry – Honan. (2020, July 8). Retrieved from https://honan.com.au/news/cyber-attacks-on-the-rise-for-the-real-estate-industry/

Cyber Exposures for the Real Estate Industry

Social Engineering Fraud

Social engineering fraud (also known as 'invoice or payment transfer fraud') refers to techniques used by cyber-criminals to deceive and manipulate victims into diverting funds to fraudulent bank accounts, often posing as what targets believe to be legitimate contacts. Due to the sheer amount of transactions made on a daily basis within the real estate sector, this is a popular method that cyber criminals utilise to steal money and it therefore it creates significant exposure to the real estate industry.

Personal Data

The potential loss of personally identifiable information is another major cyber exposure for the real estate industry. A major data breach of a customer database or mailing list can incur significant first party losses including forensic investigation and data restoration costs, legal support, public relations expenses and the extra time and costs to notify affected individuals and regulatory bodies. Additionally, third party liability claims could eventuate in response to a major privacy breach from the loss of personal data.

Reputational Harm and Brand Damage

Brand and reputational damage from a cyber incident or data breach can be hugely detrimental to an organisation. Unless managed properly, customers and the wider public can easily lose trust in a brand. Customers may even approach competitors in these circumstances causing a direct loss of the customer and revenue. Data breaches should be handled with strategic care and with support from expert breach counsel. A transparent and professional response to a data breach is crucial for softening the negative impacts on an organisation's reputation.

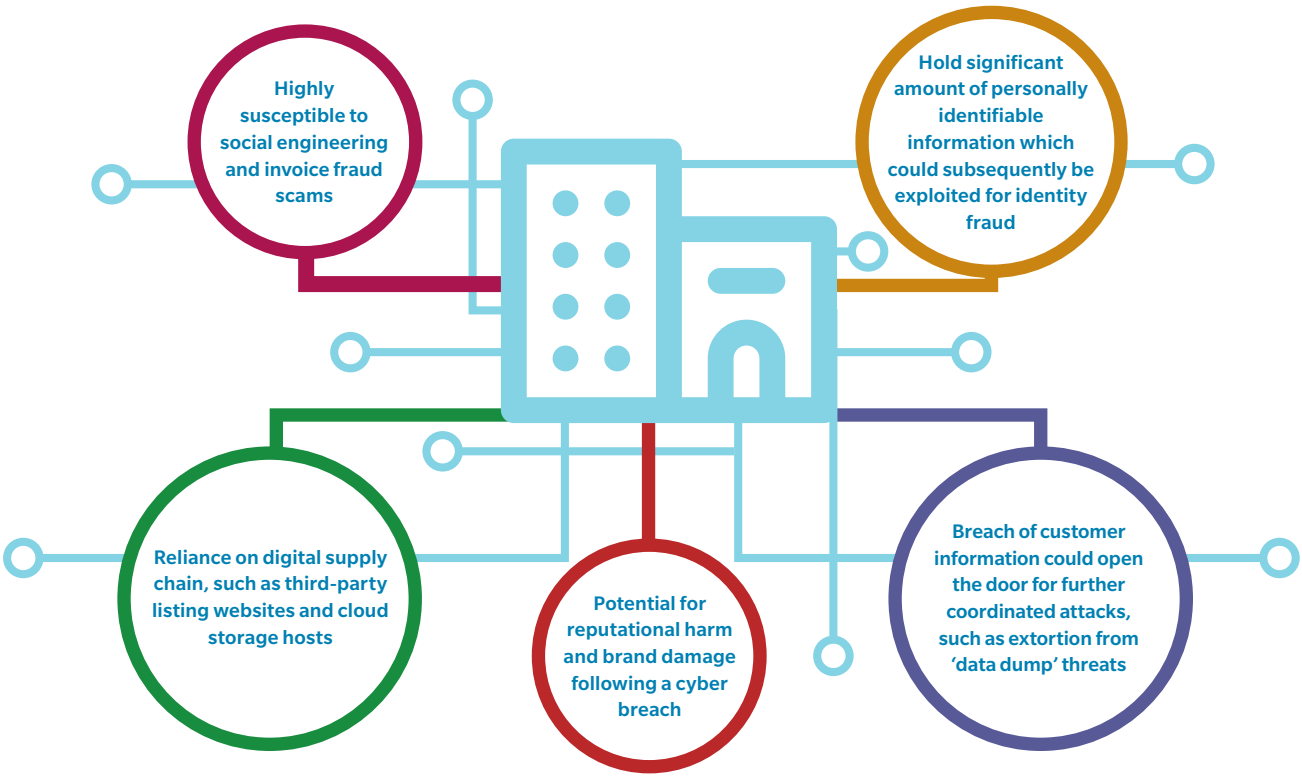
Stricter Privacy Regulations and Legislation

Real estate organisations with large international customer bases may also face exposure to third party claims and regulatory actions for privacy breaches on a mass scale from multiple jurisdictions. In the event of a data breach, companies could find themselves subject to lawsuits based on international privacy legislation which often changes rapidly to meet evolving risks. The European Union's GDPR (General Data Protection Regulation), introduced in 2018, has become a global regulatory model that is seen by many territories around the world as a best practice framework to adopt, including by Australia and New Zealand.

Digital Supply Chain

Given the growing reliance on external cloud software providers to store customer data or host websites and critical platforms, breaches of personal information or the sudden unavailability of emails hosted by a third party provider (which would be outside the control of a modern real estate organisation), will still result in significant unanticipated financial costs. This could be not only from privacy liability claims from any breach of personal data but also from contingent business interruption if day-to-day operations are impacted by a cloud provider being offline.

Real Estate Industry – Cyber Risk Profile



Filling the Insurance Gap

Cyber insurance can provide critical protection for direct loss and liability arising out of the use of technology and data in day-to-day operations, assisting real estate businesses to mitigate their exposure to cyber risk and successfully recover from a cyber-incident.

Cyber 1st Party Coverages

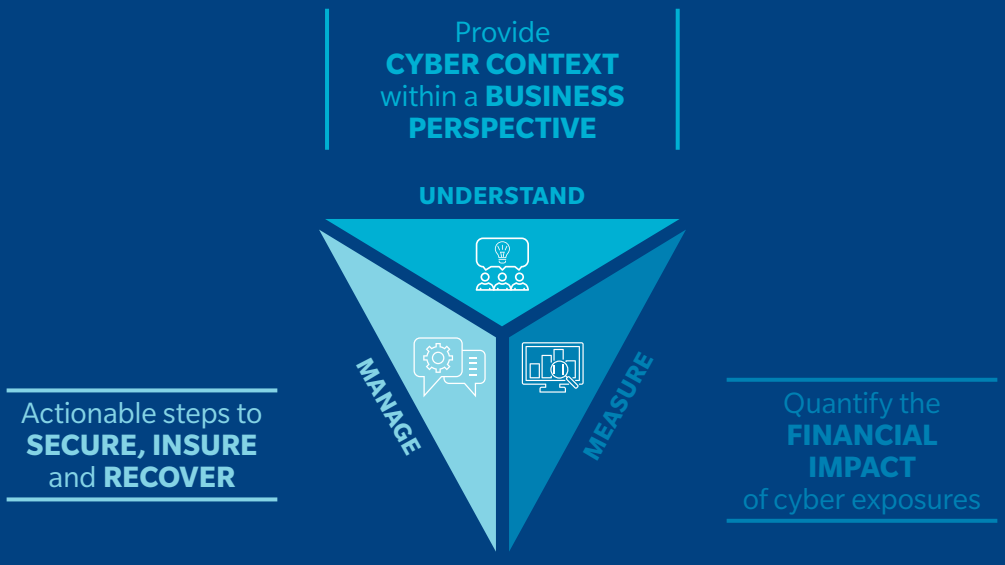
- **Incident Response Costs** – Immediate access to specialist vendors to minimise the potential financial, regulatory and reputational impact following a cyber-event. This includes the appointment of forensic IT experts, public relations consultants and legal firms.
- **Business Interruption/Extra Expense** – Reimbursement for lost profit, including extra expense resulting from a technology failure, computer system outage or cyber-attack. Coverage can be expanded to include contingent business interruption arising out of a cyber-event impacting a critical supplier.
- **Information Asset Protection** – Costs incurred to recreate, restore or recollect data damaged, stolen or corrupted.
- **Privacy notification and credit monitoring** – Provision for costs to comply with privacy breach notification statutes, as well as the provision of credit monitoring protection for affected customers.
- **Extortion** – costs to negotiate a ransom demand, as well as coverage for an extortion payment.

Cyber 3rd Party Coverages

- **Privacy Liability** – Liability for failure to prevent unauthorised access, disclosure or collection of confidential personal information, or to properly notify a privacy breach.
- **Media Liability** – Defence and liability costs for online libel, slander, plagiarism or copyright infringement.
- **Regulatory Defence** – Defence of regulatory actions, including affirmative coverage for certain assessed fines and penalties where permitted by law.

Marsh Cyber Services

Cyber risk can be effectively managed through a programme of continuous improvement and vigilance that combines technology with risk transfer. Cyber risks are not technical problems that firewalls and patches (though important) can solve alone. Marsh delivers risk solutions to help you protect your real estate business and enable confident risk taking. Marsh's approach to cyber risk management is comprehensive and employs techniques that **Understand, Manage** and **Quantify** the unique cyber risks affecting the real estate industry.



Connect with us

To further understand your organisation's cyber and technology liability exposures and which potential risk management or insurance solutions may assist, please contact your Marsh representative, or speak to one of our cyber risk and insurance specialists.

KELLY BUTLER
Cyber Practice Leader – Pacific
+61 3 9603 2194
kelly.butler@marsh.com

NICOLE PALLAVICINI
Principal
+61 2 8864 8323
nicole.pallavicini@marsh.com

JONO SOO
Head of Cyber Specialty – New Zealand
+64 9 928 3092
jono.soo@marsh.com

KRISTINE SALGADO
Managing Principal
+61 3 9603 2871
kristine.salgado@marsh.com

SAMUEL ROGERS
Managing Principal
+61 3 9603 2381
samuel.rogers@marsh.com