MARSH JLT SPECIALTY

Construction Industry:

How technology is reshaping this industry

MARSH

Construction Industry: How technology is reshaping this industry

“A host of new technologies and innovative building techniques and materials are reshaping construction projects, offering the potential for increased efficiency and profitability”.[1]

Against this backdrop of rapid digitisation is a cyber landscape fraught with pitfalls, criminal activity, increasing regulation, and penalties. Those companies which design their IT systems, strategies, and security in line with the evolving business environment have the ability to protect themselves from the potentially terminal consequences of a major cyber event. They also have the ability to differentiate their company in order to remain competitive in a congested sector.

Risk Exposure

It is critical for all businesses to assess their potential exposures; not only the levels of cyber security protection but also the resources available to respond in the event of a breach. In most companies, cyber risks are now being considered at boardroom level. Companies are being asked by internal and external stakeholders to assess both ‘where they are now’ and ‘where they aim to be’ in the future.

Technological advancements continue to assist the industry to become increasingly efficient. They can also make construction companies more attractive targets for cyber criminals and nation-state actors looking to steal data, ransom systems, or otherwise disrupt companies’ operations. Virtually all companies in the construction industry rely on IT networks, software applications, and data to maintain general business activities, from payroll and order processing to marketing and communications.

Two of the key innovations we are seeing that are transforming the construction industry:

1. Building information modelling (BIM), which is an intelligent, three-dimensional (3-D) software modelling technology that gathers data about a project and all its components throughout the project life cycle
2. Blockchain, which is an unchangeable distributed ledger technology designed to ensure the authenticity of each entry in the ledger that can be used in such areas as tracking supply chains and materials, project modelling, and smart contracts.

Historically, the construction industry has not been a target for cyber-attacks as it does not usually hold much sensitive information compared to other industries. However, the construction industry would store personal information such as employee details, bid data and intellectual property, which does increase the risk of regulatory action as the landscape continues to change. This means construction companies should accept responsibility at the most senior levels, should assess how cyber risks can impact their business and their customers, and should take the steps necessary to protect assets and projects.

1 Construction Risk Thought Leadership, International Risk Management Institute, Inc. and Marsh LLC, 2019.

The repercussions could be costly

A recent trend we have observed globally is an uptick in ransomware claims. 2019 statistics suggest an organisation falls victim to ransomware every 14 seconds. Over the course of 2019, severity also increased, with the average ransomware payment almost tripling from USD 12,762 to USD 36,295. Ryuk and Gandcrab comprised close to half of the regional, country and state attacks that occurred. The average Ryuk attack ransom amount was USD 286,557 and many payouts exceeded USD 1 million. The potential impact of ransomware is being considered as insurers develop new underwriting strategies and deliver risk management insights to the business community to help better control this increasing risk.

In light of increasing ransomware attacks, it is important for construction companies to understand their supply chain and how they manage risk and the governance procedures for contractors and sub-contractors which could potentially leave construction companies vulnerable to more cyber-attacks.

Construction companies now more than ever need to prepare for an increase in frequency of attacks across the industry. Greater awareness should be encouraged within the organisation to increase cyber resilience throughout the supply chain. Investment directed towards educating employees is paramount to reduce network vulnerabilities.

Filling the insurance gap for Construction

The cyber insurance market continues to evolve and it is more important than ever for construction companies to understand their current suite of insurance policies. For example, in 2019, we saw the insurance industry react to Silent cyber (or "non-affirmative cyber") notably affecting property and general liability covers. Cyber insurance will continue to evolve to develop protection for gaps created by other lines of insurance.

Cyber insurance is an essential tool for organisations, not only to mitigate cyber risk exposure but also to help organisations recover post-breach.

Cover can extend to:

1st Part Coverages

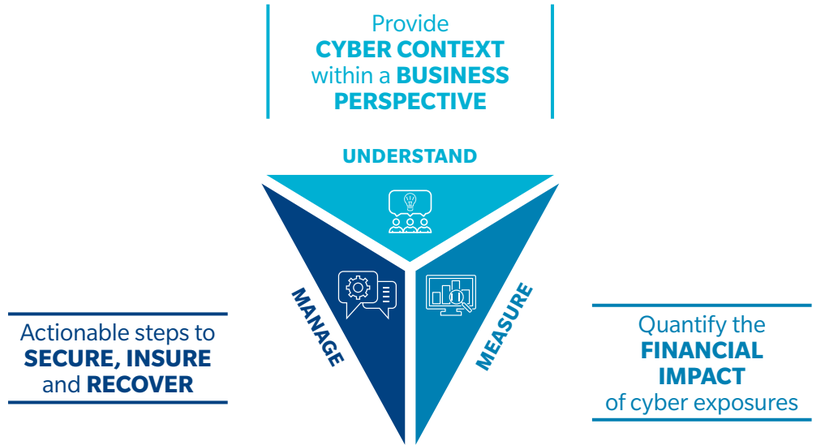
- **Incident response costs** – Immediate access to specialist vendors to minimise the potential financial, regulatory and reputational impact following a cyber-event. This includes the appointment of forensic IT experts, public relations consultants and legal firms
- **Business Interruption/Extra Expense** – 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.

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.

Cyber Risk Management Solutions

Cyber risk can be effectively managed through a program 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's cyber team works with clients to analyse their current state of cyber resilience and stage of maturity, and delivers risk solutions to help clients protect themselves and to help them enable confident risk management.



What makes Marsh different?

Our people are industry leaders and innovators operating at the heart of the cybersecurity eco-system, with experience ranging from measuring and improving organisations' cyber maturity to responding to cyber incidents to designing market leading solutions.

Our global network of cyber experts are available to you in all key markets. We act as one team and actively encourage cross-border collaboration to ensure your access to our expertise and support is not limited by geographic location. The right experts will be in the room to support you, regardless of where you are. We don't just promise a global team, we can deliver one.

Our client experience cuts across industries, allowing us to apply the best learnings in every project we deliver, whilst constantly building on our knowledge-base which our clients will benefit from. Our cyber clients range from the top ASX100 companies to local businesses. As a specialty insurance broker, we have extensive insights on common triggers of organisational failure. This allows us to identify red flags early and develop solutions to address exposures and help you avoid common failure modes.

Our risk based approach is underpinned by quantification and modelling expertise to deliver insights linked to tangible business impacts and we are vendor agnostic. This allows us to present solutions that are supported by very clear financial investment case, with no conflicts of interest.

Our end to end offer allows us to help our clients manage key business risks from their identification through to risk transfer (insurance placement). Few professional services firms are able to offer this full spectrum of services.

Connect with us

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

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

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

GEORGIA O'GRADY
Principal – Cyber
+61 2 8864 8312
georgia.ogrady@marsh.com

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

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

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