Marsh

Understanding cyber risk in the construction industry

Cybersecurity in construction

Australian construction companies are not immune to the wave of cyber crime threatening businesses and consumers across the globe.

Indeed, across Australia there has been an increase in the number of incidents of cyber crime, and the construction industry has also been hit[1], with cyber criminals targeting larger building companies and small businesses alike – even consultants, contractors and suppliers.

While some construction companies and contractors have resisted innovating for various reasons, the industry as whole may need to embrace more modern methods as a way to help transform and sustain a future – or to simply survive.[2] But while innovation aids productivity and efficiency, it also brings with it new and rapidly-evolving cyber risks.

There are ways to help minimise the exposure and mitigate the risk, which we examine further in this guide.

[1] July 2021, Australian Financial Review, Cyber criminals increasingly target builders.
[2] November 2022, The Australian Constructors Association, Disrupt or die.

THE CYBER SCENE

Real life impacts and consequences of cyber crime in construction

Supply chain risk is a major concern in an industry where almost everything is connected. The consequences of a cyber event occurring in construction can be significant for everyone connected to a business or project – disrupting operations across the board, and resulting in costly downtime, loss of critical project information, physical damage, financial loss, reputational damage and loss of clients.

While many larger construction firms have increasingly invested in good cyber controls, other smaller operators or contractors may not. And even with improved cybersecurity measures, the risk of damage is still high given that cyber crime is becoming increasingly sophisticated.

Here are some examples

Ransomware attack

What is it? A company's computer systems become infected with ransomware, which encrypts all data and demands payment in exchange for a decryption key.

In 2018, a **Melbourne-based residential building company**[3] twice fell victim to a ransomware attack. The business paid IT consultants to recover the data from backups, and they were also able to crack the encryption that the hackers had set up on a separate system to retrieve the data they had accessed and held at ransom for bitcoin.

According to the **Australian Cyber Security Centre**[4], ransomware attacks were the most destructive cyber crime in Australia over the 2021-222 financial year.

Data theft

What is it? A hacker accesses a company's network and steals sensitive data such as blueprints, financial records, and employee information, resulting in significant delays, financial losses and reputational damage.

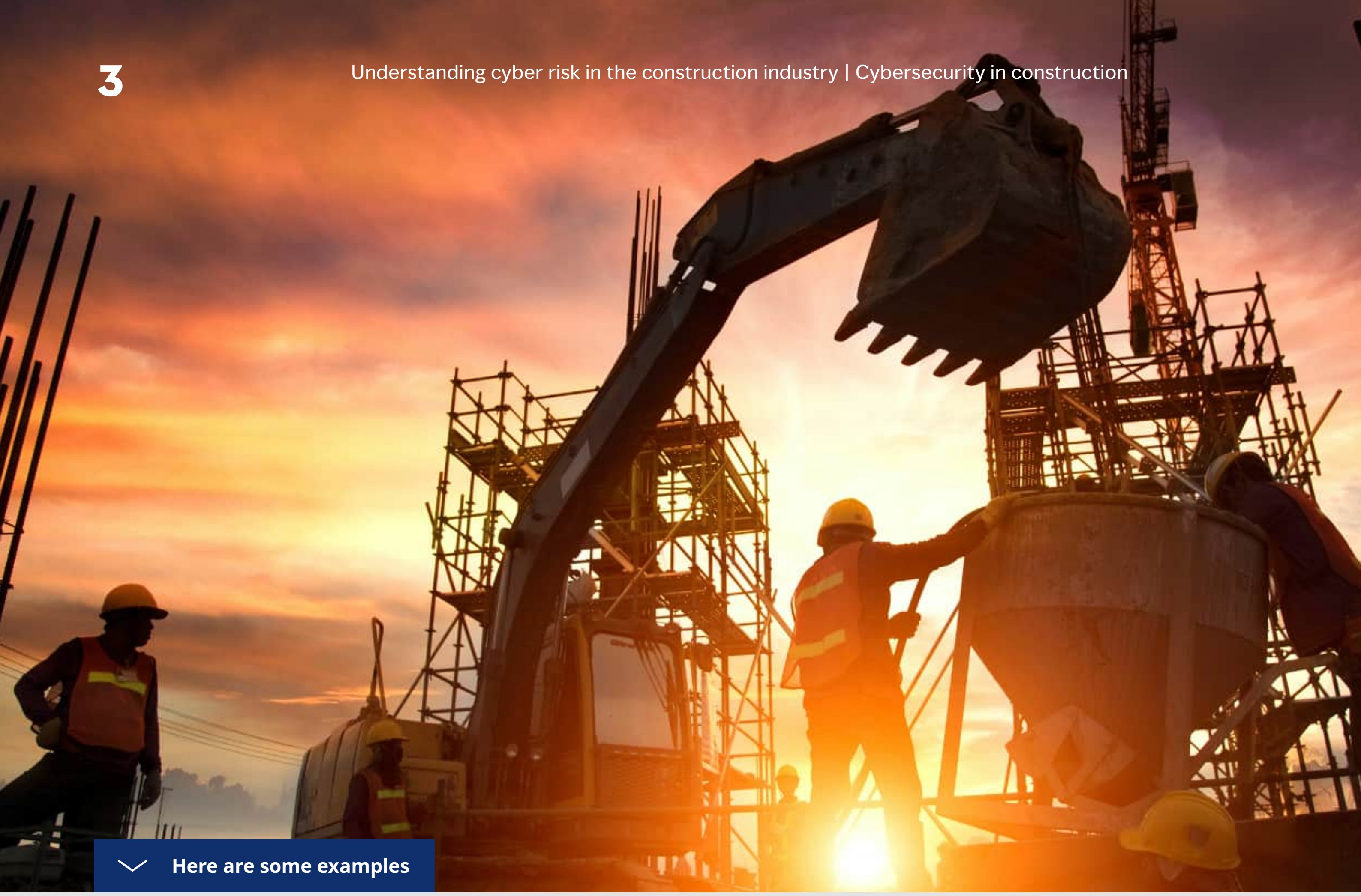
In 2020, **a Canadian construction company**[5] with military and government contracts suffered a ransomware attack, resulting in 60GB of stolen data and the leaking of personal employee records, which included addresses, banking, tax, health and other financial details. Some of the details were publicly published on the internet. Company files were encrypted and a ransom was demanded by hackers.

Phishing scam

What is it? An employee falls for a **phishing (scam) email**, providing confidential login credentials to a hacker. The hacker is then able to gain access to the company's network and potentially steal sensitive information, causing damage or loss.

In 2020, **an Australian logistics company**[6] experienced a phishing attack, targeting employees with emails that appeared to be from a legitimate source. The emails contained malicious links, which when activated by the employees, gave hackers access to the company's systems, encrypting files, rendering them inaccessible, causing system shut downs and disruptions, not only for the company but also for its partners. The incident garnered media attention, impacting the company's reputation, and the company faced significant costs relating to incident response and recovery, as well as legal and regulatory consequences.

[3] July 2018, Australian Financial Review, Cyber criminals increasingly target builders.
[4] November 2022, Australian Cyber Security Centre, ACSC annual cyber threat report, July 2021 to June 2022.
[5] January 2020, Infosecurity Magazine, Major Canadian military contractor compromised in ransomware attack.
[6] February 2020, AFR, Toll faces customer fallout after cyber attack.



Here are some examples

Control system breach

What is it? A hacker accesses and tampers with a company's building automation and security systems, which control things like lighting, HVAC and access, potentially leading to physical injury or damage.

In January 2015, cyber criminals gained control of a blast furnace within **a German steel mill**[7], causing a fire and significant physical damage. It is believed the attackers used phishing emails to trick staff into opening a malicious attachment, which downloaded malware onto the computer. Attackers were then able to access the business's network and other online systems that controlled the plant's operations.

Third-party vendor risk

What is it? This is when a third-party vendor or supplier is hacked, leading to disruption, delay and loss for that vendor, but also other stakeholders in the supply and logistics chain.

In June 2017, the **NotPetya Ranswomware Attack**[8], which targeted businesses primarily in the Ukraine, quickly spread globally affecting various organisations and industries, including **a French Construction business**. The attack crippled logistic supply chains across the globe, with damage estimates ranging in billions of dollars. Once infected, NotPetya rendered systems entirely inoperable. Many businesses lost critical data and systems, leading to severe challenges. The hackers demanded ransoms, which some victims did pay.

Financial impacts

The exact quantification of the total costs of cyber crime on Australian businesses and their consumers is difficult to establish because it relies upon self-reported data – the reality is that many victims are not reporting crimes.

However, we do know that Australians are losing more money than ever before to cyber crime. In 2022, Australian consumers lost a record $3.1 billion to scams – an 80% increase from the previous year, according to the Australian Competition and Consumer Commission.[9]

For Australian businesses in the 2021-22 financial year, the estimated cost was approximately $98 million, with medium-sized businesses (those with between 20 and 199 employees) being hardest hit.[10]

[7] January 2015, WIRED, A cyberattack has caused confirmed physical damage for the second time ever.
[8] June 2017, NY times, Cyberattack hits Ukraine then spreads internationally.
[9] 17 April 2023, Australian Competition and Consumer Commission, media release, ACCC calls for united front as scammers steal over $3bn from Australians.
[10] November 2022, Australian Cyber Security Centre, ACSC annual cyber threat report, July 2021 to June 2022.

A CYBER APPROACH

The brand damage that accompanies a cyber incident can be significant and hard to remediate without proper foresight and preparation, affecting your reputation with clients, and your bottom line.

To avoid this, companies should consider implementing a double-pronged approach that incorporates a comprehensive risk management program and insurance.

1. Re-assess your risk management

Regardless of whether you're a small business or a large multinational company, it's important you establish business-wide risk management processes that include both staff training and education, as well as cyber incident response planning.

Develop an incident response plan to capture your business's position and plan of action for various scenarios that might arise before, during and after an event. This could include the following:

- Risk management plan
- A ransomware playbook outlining actions and procedures for handling incidents – consider actions across all departments
- A policy to guide your decision-making and approval authority and processes for various scenarios, for example, in which situations you would pay a ransom
- An outline of your communications approach with stakeholders, regulators and the broader public
- Remediation actions and team functions
- Rules for engaging outside expertise – legal counsel, cybersecurity experts and forensic consultants etc
- An outline of the critical factors to enhance the likelihood of insurance under your insurance policies – working with your insurer, requirements, processes etc.

On a business-wide level, you should also establish a risk program and procedures to guide employees. This can include the following:

- Ongoing cyber education for employees
- Cyber risk program
- Adopting least privilege principles so employees only have the access they need
- Multi-factor authentication and complex passwords for all employees and third parties (eg subcontractors), and rotating passwords regularly
- Rules for housing sensitive site data for project engagements separately
- Procedures for ensuring secure and regular back-ups of systems to external data centres
- Monitoring and responding to regulatory obligations
- Testing, monitoring and reporting mechanisms
- Documenting rules for working with trusted vendors and suppliers.

2. Cyber insurance is key for risk transfer

General construction and business insurance policies do not typically include coverage for cyber incidents – even if they do not explicitly exclude such events in the policy wording – which is why it is even more important to speak with a broker who understands your business and can advise on the right insurance package.

While cyber insurance is primarily intended to provide bottom line protection in the form of financial support, it can also provide access to cybersecurity expertise and services that will work with you in the event of an incident. This removes the need for you to establish separate contracts with other providers.

There are additional benefits that come with a cyber insurance policy. For example, you can access immediate a 24/7 incident response service, including expert ransom negotiators. Cyber insurance can also cover your business for costs for business interruption, legal or PR services, restoration and repair of IT systems and data, third-party liability, and even cover the ransom (where it is legal to pay one), as well as penalties and fines.

CHECKPOINT

A ransomware scenario – would you be prepared?

In the event of a cyber incident, your business will reply upon two key measures:

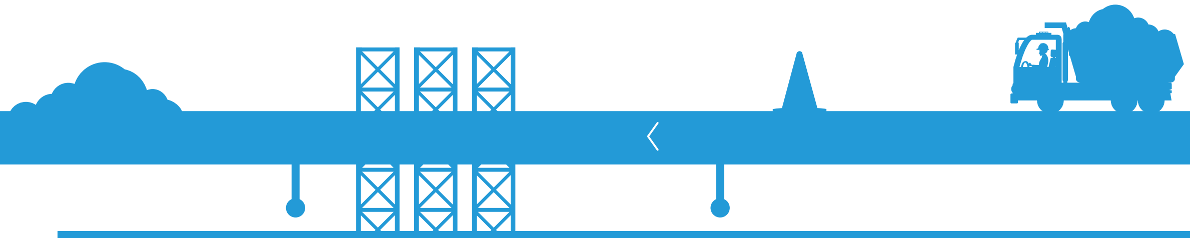
- Your cyber incident response strategy and preparation – a playbook detailing your company's response to different scenarios will save you time in a critical scenario.
- Insurance to transfer the cyber-related risk – some traditional insurance lines broadly exclude cover for cyber-related incidents, while some cyber policies do not always fully cover the costs of property, so it's important to seek advice on how your different insurance policies work together to provide the best coverage for your business.

Consider how the following fictional ransomware scenario could play out for your business at each stage. Would you have the capacity to respond and manage the incident without the appropriate risk program in place?

Breach and incident response →

1. Ransomware attack – the business network is compromised and encrypted
2. Malware is inadvertently enabled – impacting access to critical systems including email and accounting
3. Executives convene with incident response team, and engage legal counsel and PR experts
4. Digital forensic experts confirm backups cannot be accessed

- Drawing upon your incident response plan could save you precious time in a critical scenario – in addition to outlining response procedures, it can also document your company's agreed strategic approach, for example, your agreed policy in relation to paying a ransom.
- Ensure your insurance policies cover costs for specialised cybersecurity relations expertise, such as legal, forensic and media advisors.



← Cyber extortion

5. Ransom negotiators engage threat actor – initial demand of $10m received
6. Following a 7-day negotiation the decision to pay a $4.5m ransom is made following expert sanctions approval

Notes:

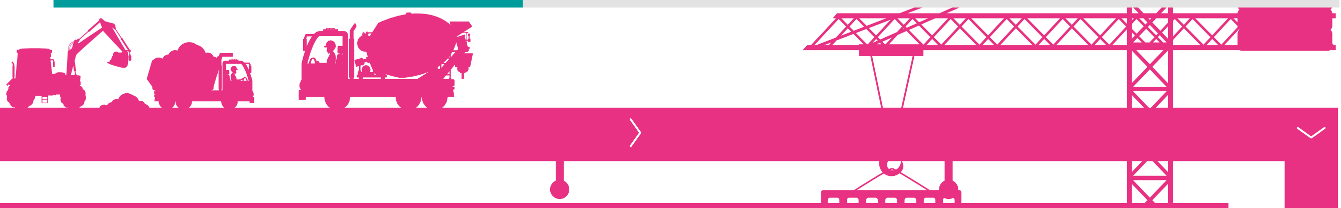
- It's important to understand whether your cyber insurance covers ransoms, and in which circumstances and what reporting, approval procedures and/or processes you need to follow in order to ensure recovery of funds.
- Ensure your insurance policies provide you with access to experienced ransom negotiators.
- Given that many ransoms are demanded in cryptocurrency, it's important you have a basic understanding of cryptocurrencies, or access to counsel who can provide advice and direction, and manage transactions on your behalf.
- It's critical to engage with your insurer before making any payments.

Business interruption and data restoration

7. Inability to access corporate network leads to reduction in business revenue and additional costs to continue working on projects

8. Following ransom payment, decryption process takes 3 weeks

- Deploy your data restoration outlined in your response plan. Regardless of your approach, it is likely to take considerable time and resources to isolate and eradicate the ransomware/malware from your systems – from weeks to months.
- While it's important to restore and protect your systems using secure offline storage backups, it's equally critical that you do not delete key files or notes that might be useful in understanding the cyber criminal's tactics, which can be helpful for either recovery or legal defence.
- Ensure you have adequate insurance to assist with data recovery as well as financial loss due to business interruption.
- Consider whether you need to deploy additional risk management measures, or provide further training to employees.



Data theft

9. Personal and banking data of employees and customers filtrated and sold on the dark web

10. Subjects are notified of the data breach and offered credit monitoring

- Disseminate formal breach notices to affected parties (eg customers), and communicate regularly.
- Establish a dedicated response team to respond to customer and supplier queries, provide support and manage remediation (as required).
- Ensure your insurance provides cover to remediate costs of breach notification, credit monitoring and identity theft monitoring.

Liabilities, fines and penalties

11. Legal proceedings filed on behalf of data subjects. Information Commissioner's Office investigation commences.

- Check your policies to ensure insurance provides adequate cover for legal costs, settlements, fines and penalties, and public relations support.
- Conduct a whole-business review of your approach that incorporates learnings, and update your cyber incident response plan and overall strategy.

As cybercrime continues to evolve and become more sophisticated, the construction industry needs to prioritise cybersecurity. The consequences of a cyber attack for a construction project could be severe, leading to costly downtime, loss of critical project information, financial loss, and reputational damage.

To safeguard against evolving threats and transfer risk, construction companies ought to implement a two-pronged and proactive approach to cyber risk management. A comprehensive cyber risk management plan is the first step, and should involve regular risk assessments, employee training, the establishment of proper controls, and working with trusted vendors and suppliers. Additionally, it's important to seek advice on incorporating cyber insurance into your overall risk transfer strategy, which can provide critical financial support and access to cybersecurity expertise during an incident.

This is the best way for the Australian construction industry to fortify itself from cyber crime, while continuing to innovate and prosper into the future.

Useful resources

The Australian Cyber Research Centre has excellent guides and tips for businesses looking to increase cyber resilience, including the latest alerts and advisories.

About the author – Kelly Butler

Kelly Butler is the Chief Client Officer and Executive Chair of Cyber Risk for Marsh in the Pacific. She also serves as the Senior Cyber Risk Advisor for some of Marsh's largest clients and sits on Marsh's Global Cyber Board.

Kelly has been a driving force in establishing Marsh's market-leading cyber broking practice. With an insurance career spanning 25 years, she has also worked on all sides of the insurance industry including working with leading global insurers in claims management handling complex casualty, professional indemnity and director and officers matters, crisis management and financial lines broking.

A respected voice and champion of the insurance industry, she is passionate about educating insurers, clients and brokers about better managing and mitigating cyber risk.

About Marsh

Marsh is the world's leading insurance broker and risk advisor. With over 45,000 colleagues operating in 130 countries, Marsh serves commercial and individual clients with data-driven risk solutions and advisory services. Marsh is a business of Marsh McLennan (NYSE: MMC), the world's leading professional services firm in the areas of risk, strategy and people. With annual revenue over $20 billion, Marsh McLennan helps clients navigate an increasingly dynamic and complex environment through four market-leading businesses: Marsh, Guy Carpenter, Mercer and Oliver Wyman.

For more information, visit marshmclennan.com, follow us on LinkedIn and Twitter.

This publication and any recommendations, analysis, or advice provided by Marsh (collectively, the 'Marsh Analysis') are not intended to be taken as advice regarding any individual situation and should not be relied upon as such. This document contains proprietary, confidential information of Marsh and may not be shared with any third party, including other insurance producers, without Marsh's prior written consent. Any statements concerning actuarial, tax, accounting, or legal matters are based solely on our experience as insurance brokers and risk consultants and are not to be relied upon as actuarial, accounting, tax, or legal advice, for which you should consult your own professional advisors. Any modelling, analytics, or projections are subject to inherent uncertainty, and the Marsh Analysis could be materially affected if any underlying assumptions, conditions, information, or factors are inaccurate or incomplete or should change. The information contained herein is based on sources we believe reliable, but we make no representation or warranty as to its accuracy. Except as may be set forth in an agreement between you and Marsh, Marsh shall have no obligation to update the Marsh Analysis and shall have no liability to you or any other party with regard to the Marsh Analysis or to any services provided by a third party to you or Marsh. Marsh makes no representation or warranty concerning the application of policy wordings or the financial condition or solvency of insurers or re-insurers. Marsh makes no assurances regarding the availability, cost, or terms of insurance coverage.