Marsh

# Cybersecurity in the construction industry

Finding a comprehensive and cost-effective insurance solution

White Paper

# The construction cyber risk landscape

In Asia's increasingly digitalised construction industry, we are witnessing rising corporate financial losses and highly-disruptive impacts from cybersecurity incidents and attacks.

Research on publicly-known ransomware attacks[1] showed that the construction industry was the most common target globally between 2020 and 2021, ranking above manufacturing, finance, and healthcare. A 2022 IBM study also found Asia to be the most targeted among all regions of the world in 2021, accounting for 26% of all cyberattacks on organisations.[2]

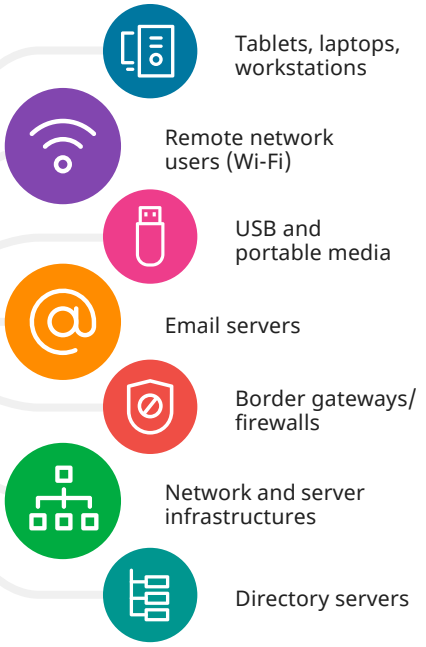
Moreover, companies in the construction industry are typically perceived by cyber criminals as vulnerable as many have high cash flows, while the extensive use of subcontractors and suppliers involving large numbers of high-value payments makes construction businesses an attractive target for spear phishing — a type of email or electronic communications scam targeted at a specific individual, organisation, or business.[3]

At the same time, newer technologies adopted as part of construction companies' core or supporting systems have not been accompanied with the necessary cybersecurity improvements, providing ample access points for cyberattackers or bad actors to exploit and infiltrate. This is not helped by the fact that although 68% are confident about their cyber resilience, nearly half (48%) of the companies in Asia admit that there is still room for improvement when it comes to cyber hygiene practice — as revealed in the 'State of Cyber Resilience' report by Marsh-Microsoft.

## Vulnerable technologies in construction

- BIM (Building Information Modelling) and project management tools that are electronically held, shared and updated
- Automated machinery and robotics
- IoT (Internet of Things) devices / SCADA (Supervisory Control and Data Acquisition) systems
- Information and business critical systems shared with subcontractors and supply chain vendors
- Supporting IT systems (e.g. payroll)
- Critical designs and drawings stored in computer systems

## Access Points




Another factor contributing to increased cyber risk exposure is the construction sector's transient workforce, which often makes controlling access to sensitive or proprietary information difficult. To ensure that the necessary cyber hygiene practices and required steps to safeguard company and client data are taken, construction companies need guidance to implement the key cybersecurity control of vetting and training staff and privileged users (i.e. those with access to data and business critical information).

1 Ransomware statistics: Who is targeted the most? Nordlocker (2021). https://nordlocker.com/ransomware-attack-statistics/
2 IBM (2022). X-Force Threat Intelligence Index 2022 https://www.ibm.com/downloads/cas/ADLMYLAZ
3 National Cyber Security Centre (2023). Cyber security for construction businesses https://www.ncsc.gov.uk/guidance/cyber-security-for-construction-businesses

# Construction industry cyber incidents and breaches

Although it is commonly believed that large construction companies that generate more revenue are subject to more frequent cyberattack attempts, smaller firms are also vulnerable as they tend to have less robust cybersecurity protocols and controls. These are notable examples of cyber incidents and breaches against the construction industry worldwide in recent years:

| Company | Estimated annual revenue | Type of attack | Description | Impact |
|---|---|---|---|---|
| French construction manufacturing company | US$47.8 billion | Ransomware (NotPetya) | Attack resulted in systems going offline for 17 days. | Loss of around €250 million on sales and of €80 million on operating income. |
| US construction company | US$9 million | Business email compromise (BEC) | Received an invoice via email claiming to come from a client asking for payment to be sent to a different address. | Company sent a check amounting to over US$210,000, believing the invoice to be legitimate. |
| Swiss construction machinery company | US$3.8 billion | Data breach | The company disclosed a security breach with stolen data across all its locations, and refused to pay a ransom amounting to US$6 million. | About 4GB of data consisting of company's operating budgets, order billing documents, and banking statements was subsequently leaked. |
| US construction company | US$50 million | Data breach | The company belatedly discovered that an unauthorised individual may have accessed information relating to its self-insured health plan. | The discovery came after sensitive employee data was leaked. In response, the company took its systems offline and engaged an independent computer forensics firm. |

Common root causes of cyber incidents and breaches include both external and internal factors, such as the following:

**1**

**Malicious attacks** (including ransomware and malware)

**2**

**Inadequate security controls**

**3**

**System glitches**

**4**

**Employee-related causes:**

- Carelessness (lost passwords, stolen laptops etc.)
- Mobility (use of unsecured networks)
- Disgruntled current or former employees

# The impact of cyber risk exposures for construction businesses

Without adequate cybersecurity controls, incidents and breaches typically go undetected for weeks and months and further magnify any negative impact on the victim organisation. The impacts on a construction company can range across operational, people, environmental, financial, and reputational aspects.

**Downtime**
The construction industry is heavily reliant to deliver projects per a timeline. A cyber attack on company software or equipment can lead to project delay and business interruption.

**Breach of intellectual property**
If the company has highly sensitive blue prints or schematics, a breach of these could mean major reputational damage and potential lawsuits.

**Breach of bid data**
Having bid strategies accessed inappropriately can lead to loss of competitive advantage or tender/project.

**Workforce injuries**
If autonomous equipment is overtaken, or physical access restrictions are ineffective, the result can be injury to the workforce and potential third parties.

**Business costs**
The cost of dealing with the failure of security or breach of privacy, including notification, ransom payment, legal services, data restoration and lost income through business interruption.

**Breach of private information**
Liability to third parties, such as employees, clients and regulators, arising from computer security failure.

# Can insurance adequately address cyber risks?

Facing an evolving variety of cyber threats, companies in the construction industry are being challenged by cyber exclusions in traditional insurance policies and a hard market with limited insurer appetite for cyber-triggered property damage, making it even more difficult to calibrate an effective and robust approach towards cyber risk.

As a core construction insurance policy, **Construction All Risks (CAR)** insurance covers all risks of physical loss or damage (except as excluded) to permanent and temporary works during construction. Insurers consistently specify a full exclusion for cyber events for CAR policies under clauses LMA5400 and LMA5401. The extent of the exclusions is summarised below:

| Exclusions[4] | LMA5400 | LMA5401 |
|---|---|---|
| Cyber Act: Loss or damage in connection with unauthorised, malicious or criminal act involving access to or use of an electronic device | Excluded | Excluded |
| Cyber Incident #1: Loss or damage in connection with error or omission involving access to or use of an electronic device | Excluded | Excluded |
| Cyber Incident #2: Loss or damage in connection with the unavailability or failure to access or use an electronic device | Excluded | Excluded |
| Loss or damage in connection with loss of use or reduction in functionality of data | Excluded | Excluded |
| Replacement or restoration of data | Excluded | Excluded |
| Value of data | Excluded | Excluded |
| **Write-Back Scenarios[5]** | **LMA5400** | **LMA5401** |
| Cover for property damage caused by fire or explosion which results from cyber Incident | Yes, subject to Cyber Act or Data exclusions | Excluded |
| Cover for business interruption caused by fire or explosion which results from cyber Incident | Excluded | Excluded |
| Cover for property damage or business interruption if insured peril causes unavailability or failure to use an electronic device | Excluded | Excluded |

The exclusion wordings in clauses LMA5400 and LMA5401 are based on the possible results of cyber risks rather than the causes (e.g. malware or data breaches) and only require 'connections' rather than causation for the exclusions to be in effect. A limitation under your CAR policy will also affect the indemnity under any delay-in-start-up cover (if procured). We have identified the below classes where insurers' views have shifted due to the new cyber landscape:

- Third Party Liability (TPL)
- Plant and Equipment (P&E)
- Terrorism or Political Violence (PV)
- Marine Cargo

4 https://insurance-endorsements.com/lma5400-and-lma5401-cyber-and-data-endorsements/
5 https://insurance-endorsements.com/lma5400-and-lma5401-cyber-and-data-endorsements/

# Closing the cyber risk exposure gap

Given the abundance of cyber risks that would not be covered by traditional insurance products and the lack of case law relating to data being regarded as “property” and corrupted data as “property damage”, companies across industries are recognising the importance of cyber-specific policies in addressing their exposure gaps.

**Most cyber insurance policies provide third party liability coverage as well as first party coverage for loss and damage to non-physical property.** However, there is a wide variation concerning other coverages. Hence, companies procuring cyber insurance need to know whether coverage is provided, and at what level, for aspects such as:

- **Extortion expenses**
- **Data loss and restoration**
- **Incident response costs**
- **Privacy liability**
- **Security failure liability**
- **Business interruption and extra expenses**
- **Credit and identity monitoring**
- **Regulatory actions**

# Discovering your optimal cyber insurance approach

The first step to identify the right insurance approach to mitigating cyber risk is to take the complimentary **Marsh Cyber Self-Assessment** diagnostic — a robust tool to assess their cyber risks and program maturity.

Developed in alignment with the US National Institute of Standards and Technology (NIST) Cybersecurity Framework and supported by advanced data and analytics, the Marsh Cyber Self-Assessment delivers a market-leading analysis of your organisation's cybersecurity controls, technology, and people.

## By mapping your cyber risk exposures, the Marsh Cyber Self-Assessment accurately informs your risk management decisions and enables you to optimise your insurance investments while benefitting from a streamlined cyber insurance application process.

**Key features of Marsh's Cyber Self-Assessment**

- **Complimentary**
  Available at no cost for all organisations, with a free report upon completion of the self-assessment.
- **Secure**
  Easy-to-use web-based interface with industry-leading security protocols such as active directory controls and data encryption in transit at rest.
- **Collaborative**
  Platform allows simultaneous contributions by multiple stakeholders and centralises inputs into a single application, eliminating inefficiencies, redundancies, and errors.
- **Comprehensive**
  Helps you gain a holistic view of your cybersecurity maturity with controls benchmarking against peers, at the same time helping drive stakeholder discussions on resource allocation.
- **Actionable**
  Report includes a risk-scoring mechanism that enables you to proactively address cyber vulnerabilities.
- **Access to experts**
  Connect with Marsh's cyber risk and insurance specialists to understand reports better, tailor a risk and insurance approach, and negotiate with insurers.

## Taking care of your cyber risk transfer and claims management needs

You can rely on a trusted partner to obtain right-sized and competitive risk transfer solutions aligned to your needs and manage your claims in the event of a cyber incident. By leveraging the global presence, multidisciplinary teams, deep technical expertise and bespoke approach of Marsh's Cyber practice, clients can benefit from proprietary wording enhancements with leading cyber insurers and tailored cyber products with catastrophe cover or buy-back cover for specific exclusions under existing policies.

The fluid and constantly evolving nature of the cyber risk landscape also poses a challenge to companies. In particular, losses resulting from new forms of security breaches raises the question of how to determine the different exposures or additional expenditures included under the specific policy language. With the knowledge and expertise of Marsh's claim advisory services, you can have peace of mind when it comes to managing claims should a claim arise.

**To boost your organisation's cyber risk resilience and help your construction business gain a competitive advantage with optimised cyber risk and insurance insights and solutions, contact a Marsh representative or request for your Marsh Cyber Self-Assessment today.**

Marsh

## About Marsh

Marsh is the world's leading insurance broker and risk advisor. With around 40,000 colleagues operating in more than 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 $17 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 mmc.com, follow us on LinkedIn and Twitter or subscribe to BRINK.