

CYBER RISKS AND INSURANCE SOLUTIONS

IN THE CONSTRUCTION SECTOR



CONTENTS

- ▶ The Construction Cyber Risk Landscape
- ▶ Traditional Construction Insurance Products
- ▶ The Cyber Insurance Market
- ▶ Residual Exposures
- ▶ Marsh Cyber Services

INTRODUCTION

All businesses increasingly face complex computer and information security risks, with cyber and associated malicious activity becoming more prevalent in every sector. The construction industry in particular is going through a period of rapid digitisation, with technology being embraced both for project modelling and daily operations. A survey in 2016 suggests that engineering and construction companies plan to invest 5% of annual revenue each year into digital operations solutions over the next five years¹; the use of building information modelling (BIM) is also now increasingly used across the industry and it is expected that construction equipment and control systems will continue to become increasingly automated.

“...engineering and construction companies plan to invest 5% of annual revenue each year into digital operations solutions...”

Against this backdrop of rapid digitisation comes 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 and to differentiate their company in order to remain competitive in a congested sector.

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 risk is being considered at boardroom level and companies are being asked to assess both where they are now and their future aims.

1. PWC. *Industry 4.0: Building the digital enterprise*, available at: <https://www.pwc.com/gx/en/industries/industries-4.0/landing-page/industry-4.0-building-your-digital-enterprise-april-2016.pdf>, accessed 24 January 2018.



THE CONSTRUCTION CYBER RISK LANDSCAPE

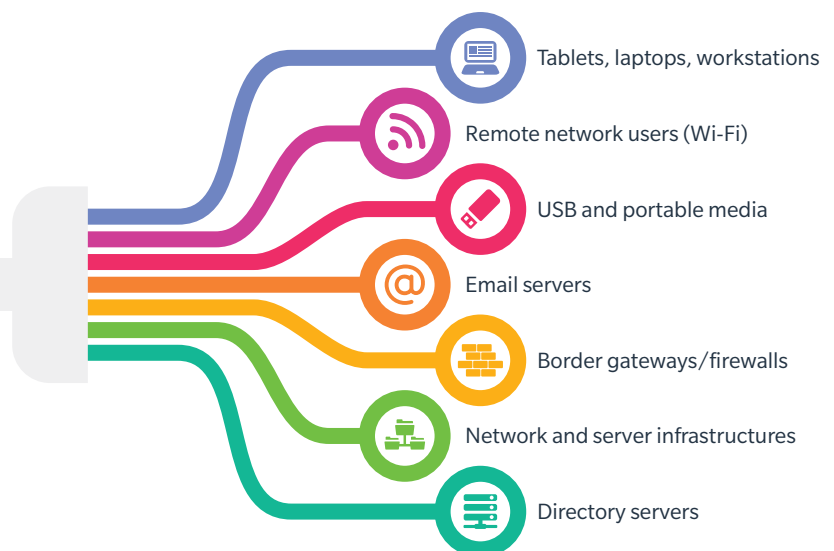
Cyber risk is ever-evolving and every security system is vulnerable. The constantly changing nature of cyber risks means that, whilst provision can be made for known risks, the next attack is likely to have different characteristics.

Some of the most common causes of cyber losses include:

ROOT CAUSE

- **Malicious attacks**
(including crimeware)
- **Inadequate security**
- **System glitches**
- **Employee-related causes:**
 - Carelessness
(lost passwords, stolen laptops, etc.)
 - Mobility (use of unsecured networks)
 - Disgruntled current or former employees

COMMON ACCESS POINTS TO VULNERABILITIES



In analysing the construction industry, we have chosen to separate these risks into:

- General office exposures which occur through the processing of financial and personal data and the reliance on IT systems as the supporting infrastructure to business operations. In the cyber world these are generally termed the “enterprise systems”.
- Project specific exposures relating to the delays, physical damages and liabilities incurred as a result of a cyber-attack. The specific use of IT in executing physical activities is termed “operational technology”.

“...any organisation working in the construction industry relies on IT networks, critical software applications and data...”

GENERAL COMPANY EXPOSURES (ENTERPRISE SYSTEMS RISK)

Like most of the developed business world, any organisation working in the construction industry relies on IT networks, critical software applications and data to maintain communication and general business activities, from payroll, to order processing, to marketing. The broad spectrum of cyber and privacy risks – which pose the potential for significant economic loss and reputational damage – include:

- The theft, loss or unauthorised disclosure of personal information, payment card information, or third party confidential information.
- Cyber-attacks and other non-damage events that result in outages and disruption to critical software applications, data and networks.
- A changing regulatory environment with a proposed² EU Data Protection Regulation introducing higher penalties and the mandatory notification of data breaches.
- The corruption of or inability to access critical data following a targeted hack or computer virus.

Whilst construction companies are less likely to hold extremely large databases of public/third party personal information, they are likely to store a significant volume of proprietary information including:

- Client data or confidential project information.
- Intellectual property.
- Sensitive commercial material.
- Subcontractors and supply chain management data and/or financials.
- Employee data including health information.

OPERATIONAL TECHNOLOGY

The construction industry is being reshaped by two major trends: contractors are taking on an expanded role in project design, as well as embracing digital technology for both project modelling and daily operations. Information technology has played a major role in construction activities for some time but digitisation is accelerating at an astonishing rate as companies digitise essential functions both internally and across their customer and supply chain.

Technologies such as laser scanning, 3D printing, building information modelling (BIM), and the integration of design and offsite component based assembly are evolving fast. Along with advanced and connected monitoring and control systems, and aspects such as autonomous vehicles and drones, this has led to a common belief that we are in the midst of a fourth industrial revolution, termed Industry 4.0.

2. General Data Protection Regulation (GDPR) effective 25 May 2018.

SUMMARY

All these challenges and more make cyber risk a sophisticated web of complexities which will continue to develop in unpredictable ways in the future.

It is clear from the various reports and literature available that cyber is increasingly being considered as a high risk by all mature companies, and this will have been heightened by the various cyber events of 2017, gaining much press coverage as the clearly significant consequences became widely known. However, it is not always easy for an organisation to assess its level of susceptibility to an event, or the possible effects.

Specialist risk management advice and loss scenario workshops can clarify current exposures and suggest methods to address those identified. However, insurance provides a unique insight into this assessment due to the accessibility to:

- Claims examples and benchmarking data.
- Financial quantification of loss scenarios.
- Insurer assessment of a company's risk rating.



TRADITIONAL CONSTRUCTION INSURANCE PRODUCTS

The rapid evolution of privacy and computer security risks has left many traditional forms of company insurance unable to respond adequately to these exposures, as the following policy limitations demonstrate:

- Property policies typically limit coverage to damage to tangible property resulting from a physical peril; several insurers go further, excluding coverage for any damage to data.
- Business interruption policies do not typically include interruption losses flowing from the unavailability of critical applications, data and networks, unless the root cause is a physical damage event.
- General liability policies traditionally require there to be bodily injury or physical damage to property. Liability claims connected to the transmission of malicious code or the breach of personal information are unlikely to result in allegations required to trigger these policies.
- Professional indemnity policies do not generally provide coverage for the full range of cyber perils and many limit coverage to liability arising from an act, error, or omission of the insured in the course of its professional duties.
- Standard market commercial crime policies do not generally provide coverage for the full range of cyber-crime perils and many limit coverage to theft of assets, fraudulent electronic fund transfers and the cost of recollecting, replicating, or restoring lost or corrupted data.

As a core construction insurance, **construction all risks (CAR)** insurance covers material damage to the contract works during construction. Cover will vary depending on the insurer and the broker but it is certain that some wordings will exclude damage caused by a cyber-attack by one of the applied exclusions described later in this section. In the Marsh Model CAR Wording, there is no reference to cyber or the like and therefore the starting point would be that any loss or damage would be insured under the policy. The same applies to the cover which we negotiate for our clients' core **plant and equipment** coverage. **Third party liability (TPL)** coverage in its basic form would be dependent on bodily injury or damage, whilst our Marsh broadform cover extends to other specified pure financial loss events, such as denial of access or loss of trade.

Most operational property insurers are successfully applying cyber and data exclusions of some kind to their policies and the construction insurance market is looking to follow suit. Many construction insurers will aim to apply these standard insurer exclusions, typically CL380, NMA2912, 2914, or 2915. The impact of these clauses on your cover will vary according to the exclusion and class affected. Marsh's Construction Practice has been able to resist the application of these clauses for our clients to date, we recognise that the conditions of the insurance market may change with time and certainly may react if cyber-attacks become more prominent and prevalent in the construction industry, or in general. We would advise all our clients to carefully review their policy exclusions and, if accepting a form of cyber or electronic data exclusion, to consider how this could affect your business in the event of a loss.

It is important to note that a limitation under your CAR policy will also affect the indemnity under any delay in start up or liquidated damages cover.







In analysing the cover available under traditional construction insurance policies, we have also looked at the available cover for construction insurance classes such as those noted below and would be pleased to discuss with you in more detail:

- Terrorism.
- Marine cargo.
- Professional indemnity.
- Contractors pollution liability.

In making any assessment for the coverage afforded, it is important to recognise the lack of available case law relating to data being regarded as "property" and corrupted data being regarded as "damage". In our analysis we considered only the cyber limitations on traditional insurance products. Obviously there are a plethora of cyber risks which would not be covered by these traditional products, hence why cyber is the most rapidly growing insurance market around the globe.

THE CYBER INSURANCE MARKET

Cyber insurance is a developing product and the cover available from carriers and brokers varies across the commercial insurance market. Although most policies provide third party liability coverage as well as first party coverage for loss or damage to property, there is a wide variation in other coverages. Clients need to know whether coverage is provided, and at what level, for aspects such as:

						
Extortion expenses	Data loss and restoration	Incident response costs	Transmission of viruses	Business interruption and extra expenses	Credit and identity monitoring	Regulatory actions

“...Marsh has a proprietary product, CyberShield, which provides comprehensive cover for our clients...”

The constantly evolving nature of cyber risk translates into an equally fluid landscape when it comes to claims management. Indeed, the challenge with any loss resulting from new forms of security breaches is to determine the different exposures or additional expenditures which are included under the specific policy language.

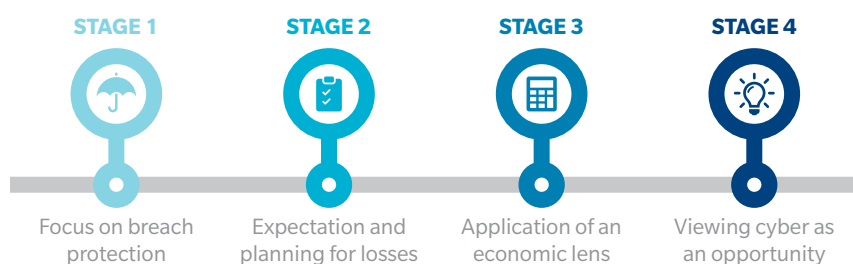
Should you decide to explore the cyber insurance market, Marsh has a proprietary product, CyberShield, which provides comprehensive cover for our clients in respect of all of the above circumstances. In addition we have other Marsh cyber products available which offer catastrophe cover, or buy-back cover for specific exclusions under your existing policies.

RESIDUAL EXPOSURES

Based on our comprehensive construction and cyber Marsh policy forms, we do not believe that the residual exposure to clients in the construction sector is significant. The main identified residual exposure appears to be project delay in start-up or liquidated damages caused by a non-damage cyber event where inaccessibility to systems, or interruption by investigations causes a delay to the operational date of the project. Any company purchasing cyber cover can insure their standard business interruption losses but the cyber market does not currently provide multi-year project cover and the potential to insure this exposure. If there is a client demand for such cover, we would be pleased to investigate it for you.

MARSH CYBER SERVICES

Marsh's cyber team works with our clients to analyse their current stage of cyber resilience and maturity. At a high level, we regard these to be:



Marsh can provide analytical services related to all of the above. These services include existing policy gap analysis studies and loss scenario financial quantification. In addition, we have tools at our disposal to assess your company risk profile in comparison to your peer companies. We work together with NCC Group, a global expert in cyber security and risk mitigation, to enable us to provide our clients with comprehensive and tailored cyber expertise for your business.

If you do decide that you want to explore purchasing cyber insurance, there are many ways to do this. Some clients choose to do so after detailed analysis of both their existing cover and potential exposures; others are happy to purchase off-the-shelf products to provide a degree of immediate blanket protection. The purchase of cyber insurance is growing and the marketplace is developing in response. In most companies, cyber risk is being considered at a boardroom level which means that many risk managers are finding it easier to raise the profile of insurance within their organisation, or are being tasked with a due diligence exercise which ensures that cyber risk management and insurance has been fully assessed and strategically addressed. Insurance provides a tool in this process which can bring a lot more than just risk transfer through:

“...we can provide our clients with comprehensive and tailored cyber expertise for your business...”



HELPING TO DEFINE THE RISK

- Narrows scope to key scenarios you face.
- Provides a source of objective loss data – frequency and impact.
- Helps define your exposure and possible loss.



FORCING FINANCIAL DECISIONS

- Turns the risk into a financial question.
- Enables rational financial choices.
- Provides a catalyst for risk management investment.



ASSISTING IN RISK MANAGEMENT

- Provides a rich source of third party risk benchmark data.
- Challenges expert opinion.
- Provides a large, reliable financial safety net.

For all enquiries relating to cyber risks in the construction sector, please contact Stuart or Richard below:

STUART FREEMAN
Marsh's Construction Practice
+44 20 7357 2854
stuart.freeman@marsh.com

RICHARD BARKER
Financial and Professional Risks (FINPRO) Practice
+44 20 7357 3301
richard.barker@marsh.com

The information contained herein is based on sources we believe reliable and should be understood to be general risk management and insurance information only. The information is not intended to be taken as advice with respect to any individual situation and cannot be relied upon as such.

In the United Kingdom, Marsh Ltd is authorised and regulated by the Financial Conduct Authority.

Copyright © 2018 Marsh Ltd All rights reserved

GRAPHICS NO. 17-1110