howden

Cyber insurance to protect your business

Cyber Insurance
Construction
& Property

Why is cyber insurance so important to construction & property businesses now?

Construction & property companies of all sizes face a range of cyber risks and these threats are continually evolving and growing in size and complexity. From targeted ransomware and hacking, to phishing, malware, email compromise, and data breaches.

According to a July 2022 "Cyber Readiness" report by Hiscox, construction was rated as the 5th most at-risk industry for cyber-attacks. But despite this, only 28% of firms are prioritizing cyber security in their budgets. Recently hackers have been increasingly targeting mid-sized companies with weak controls these companies make for softer targets, with a wealth of data and more incentive to pay ransoms. There are several aspects to the construction industry that make it more vulnerable to an attack:

- The use of on-site portable and temporary works stations
- A historical lack of focus on cyber security
- Revenue and reputation are dependent upon meeting deliverables, making disruptions particularly costly
- Increasing reliance on technology (e.g. BIM) and the cloud
- Reliance on contractors and subcontractors that may have weaker cyber security controls

In many cases a dedicated cyber policy will be the best solution giving the broadest coverage and providing the technical expertise to identify the origin of a cyber-attack and minimise the subsequent damage to the business and its operations.

Case study: French Construction Company

In 2020 a large French construction company experienced a Maze ransomware attack to its automated data processing system, which compromised employee data (including names, addresses, social security numbers, banking details and drug test results). The attack is thought to have started in their US operations and quickly spread throughout the globe. The company shut down all of its servers to prevent further propagation of the attack. In a "double extortion" attack, the threat actors exfiltrated 200GB of data before encrypting it. They then demanded a ransom of EUR 10m. Even if the company could restore the data from backups, it would still be compelled to pay the ransom to prevent its data from being published.

In this case Cyber Insurance would respond to incident response costs, notification costs, lost revenue and the cyber extortion demand. Howden has drafted bespoke business interruption language for the construction & property industry to address increased costs in excess of normal operating expenses that may be incurred to avoid delays (e.g. cost of overtime, employing sub-contractors or alternative supplicers, night-work, public holidays) and to cover contractual penalties that may be incurred due to delays.

Case study:
UK Commercial Construction firm

A UK Construction firm became the target of a type of cyber-attack called Friday Afternoon Fraud, where attackers take advantage of a firm dealing with and paying a number of contractors or other parties for services rendered.

The scheme culminated in the victim firm transferring £90,000 to a fraudster, but began with a seemingly innocuous email sent to an employee, asking them to update their Office365. The employee clicked on the link and was directed to what looked like the official Office365 site. When prompted, they entered their login credentials. However, this was a phishing email, and due to the construction firm not having multi-factor authentication enabled, the hacker then used the login details to access the employee's email account. From this point forward the fraudster monitored the communications and waited for an opportune moment to strike.

The employee was one of the firm's project managers, and often liaised with subcontractors, who would submit invoices for work performed. A few weeks later, the Managing Director of a subcontractor submitted an invoice to the employee for over £90,000. Spotting this opportunity, the hacker set up a forwarding rule in the project manager's account, ensuring that all emails arriving from the subcontractor were auto forwarded to the hacker instead.

Impersonating the Managing Director, the fraudster informed the victim that their payment details had changed, and requested transfer of the invoice (and all future invoices) to a new account. The project manager forwarded the payment request to the billing team and £90,000 was transferred to the fraudster.

The firm claimed under the cyber crime section of their cyber policy and insurers covered the loss.

How can a cyber policy help?

1 Incident response

The first 24-72 hours following a cyber incident are crucial. A cyber policy gives you 24/7 access to expert support, such as:

- Specialist IT forensics
- Legal assistance to ensure any regulatory notifications are made as necessary
- PR support to minimise reputational damage

2 Cyber extortion/ransom

Hackers can access and lock you out of your files and systems mainly for monetary gain. They can also extract data and threaten to publish sensitive information/ Intellectual Property to extort you. A cyber Insurance policy will indemnify you in the event that payment of a ransom is required, and will provide you with the required expertise to support you including experts with knowledge of hackers, variants of malware and the Dark Web.

3 GDPR/Notification of personal breach

Whether you use and store data on your own premises, or outsource to third party cloud providers, data controllers and processors both have obligations under GDPR (and equivalent legislation worldwide). GDPR also requires you to inform those who have been affected by a breach without undue delay. Depending on the number of data subjects, this can be very costly. A cyber policy can provide you with specialist legal advice to ensure compliance with GDPR and other data privacy laws and regulations following an incident, notification to data subjects if required and credit monitoring assistance.

4 Network security and privacy liability

A cyber policy will provide cover for your legal liability to third parties, covering third party claims and regulatory investigations following the occurrence of a cyber-incident such as:

- Claims because your systems have transmitted harmful malware to the systems of third parties
- Defence costs and damages arising from claims as a result of a data breach (which may often now involve group litigation)
- Claims for defamation, libel, slander arising from your multimedia content

5 Business Interruption and data recovery

An attack such as ransomware or even simple human or operational error can cause system outage/interruption, potentially disrupting your processes, reputation and finances. Cyber policies will cover the loss of income and increased cost of working incurred following an incident, together with the costs incurred to restore your systems and associated data. Howden's bespoke wording tailors this coverage to the specific losses that the construction & property industry may face.

Top risks cyber insurance helps with

1 Ransomware attacks

Ransomware attacks are increasing in frequency and severity, with phishing emails remaining one of the primary methods for delivering an attack. In addition to the costs of the extortion demand itself, associated losses such as system down time and data recovery costs can significantly increase the total expenses incurred. Under a comprehensive cyber policy, the extortion cover will not only cover the payment of the ransom demand; it will also cover the associated forensics expenses, data restoration costs, and even the fees for a ransom negotiator.

2 Data breaches

If a business is hacked, criminals are likely to use stolen confidential data to extort companies or sell on the dark web. Construction companies could be an attractive target for cyber criminals due to personal client data they store on their systems. Data breaches are covered under a cyber-policy whether for notification expenses or a liability claim.

3 Human factor

Whilst there can be a malicious element in some cases, the majority of incidents are non-malicious, arising instead from a lack of awareness, training or sometimes concentration, e.g. accidentally clicking on a malicious link. With many businesses changing to reflect a flexible workplace environment, companies should take preventative measures by ensuring their employees receive training to improve and support their cyber security strategy.

4 Third Party Risk

This threat is presented to businesses through their supply chains and other third party vendors who may have access to systems and data. This is due to them being reliant on those third party vendors having sufficient protection from cyber-attacks or not being a threat themselves. For instance, building information modelling (BIM) creates an online environment where planned building models and projections are displayed. These sorts of common data spaces contain large amounts of information (potentially including client information, trade secrets etc) which cyber criminals may steal.

Why Howden?

Our award-winning cyber team is made up of 25 insurance experts based here in the UK. Working alongside our specialist Construction & Property professional indemnity team we will map out your unique risk profile and implement an insurance programme to help protect your business from cyber related risks.

We make buying and managing your insurance as straightforward as possible; talk in jargon-free language and our team is always available for any queries you have.

If you would like more information about your cyber cover, please get in touch with your usual Howden contact.

howden

One Creechurch Place, London, EC3A 5AF

T +44 (0)20 7623 3806
E info@howdengroup.com

www.howdengroup.co.uk