CYBER RISK EXTENDS TO ALL INDUSTRY SECTORS: IMPACTS TO THE CONSTRUCTION INDUSTRY

Gallagher

Insurance | Risk Management | Consulting

Construction

Roger Irvine
Head of Construction
Australia & Asia

Robyn Adcock
Cyber/ Technology
Practice Leader

Cyber risk has evolved to impact organisations of all sizes across multiple industry sectors. Today's threat actors have pivoted to attack vectors that allow them to target key players in the supply chain, where a successful attack on one can impact thousands more. Whether it is a software supplier, email exchange server or a provider of critical infrastructure, the attack surface, and the threat, grow larger by the day. The construction industry is one that falls within the scope of today's cyber threat landscape.

THE EXPANDING CYBER ATTACK SURFACE IN CONSTRUCTION

Construction-related businesses face the same fundamental cyberattacks and threats as other industries but have unique risks that are associated with specific tools they use for managing data, delivering services and systems control. These include:

3D Building Information Modeling (BIM) — Builds digital information models to support efficient decision-making for planning, design, construction, building operations and maintenance.

5D BIM — Provides an enhanced visualisation and project-management platform. In the future, augmented- and virtual-reality technology will be added to allow offices and the worksite to collaborate in real-time.

Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition Systems (SCADA) — Monitors and controls equipment and plant operations.

Drones — Enables job site surveillance, surveying and access to previously inaccessible places.

Autonomous Construction Machinery — Used for the remote navigation of excavators, bulldozers, backhoes and dump trucks for higher utilisation rates and lower operator costs.

Robotics — The deployment of robotics in bricklaying and road paving, to replace highly repetitive, systematic manual processes.

Biometrics — Increasingly used to manage and control construction sites and projects, through access control to secure sites, on-site attendance reporting, health and safety, compliance, and remote management of multiple workforce.

Cloud Technology — The use of vendors to store data on behalf of the business.

Mobile Devices — Allows the highly decentralised construction industry to enhance collaboration at all stages of the construction process, including productivity tracking, report generation, document management, material logistics, inventory management and data analytics.

Internet of Things (IoT) — Provides for remote operation of wearables and machinery, supply replenishment, tracking of tools and equipment and remote usage monitoring.

CYBERATTACKS AND THE FOCUS ON THE CONSTRUCTION INDUSTRY

According to the Australian Cyber Security Centre (ACSC)[1] in the 2020-21 financial period there were over 67,500 cybercrime reports, with losses exceeding $33 billion. Worryingly, ransomware attacks increased almost 15% per cent from the previous financial year. From a construction industry perspective, ransomware attacks can immediately shut down access to important data, leading to critical delays that have a ripple effect through subcontractors and other key players in the construction supply chain. In fact, according to Coveware's Q2 2021 report,[2] the average downtime for ransomware victims was 23 days.

Hackers also favor social engineering schemes to carry out funds transfer fraud where they impersonate senior management and key vendors through Business Email Compromise (BEC) tactics. The criminal's goal is to convince victims to wire funds or provide sensitive information that can be monetised. With the vast amounts of funds that routinely exchange hands throughout the life of construction projects, one can see why this industry would be an attractive target for cybercriminals.

Specifically, cyber risks expose construction businesses to:

- Liability to third parties, such as employees, clients and regulators, arising from computer security failure and breach of private information.
- The costs of dealing with the failure of security or breach of privacy, including notification, ransom payment, forensics, legal services, data restoration and lost income through business interruption.
- Breach of confidential business information, through storing and sharing bid and project data/specifications, owner's processes and project management.
- Unauthorised access and interference with project plant, data and specifications in SCADA and Building Information Modeling (BIM).
- Bodily injury and property damage through the failure of IoT, robotics and remote control of processes and physical security.
- Liability for delay and business interruption caused by unauthorised access to project data and systems.

[1]ACSC Annual Cyber Threat Report - 1 July 2020 to 30 June 2021. Released 15 Sept 2021.

[2]Coveware Q2 2021 Ransomware Blog

TRANSFERRING THE CYBER RISK

Gallagher has worked closely with the cyber insurance market to develop tailored risk transfer solutions for businesses across all industry sectors, including the construction sector. While there is no standard cyber insurance policy, there are some commonly offered coverages that are excellent mechanisms to save bottom line costs in the aftermath of a cyberattack. Other policies, including crime, property, liability, kidnap & ransom and error & omissions, may also offer some limited insurance coverage to cyber exposures. However, a comprehensive stand-alone cyber insurance policy usually affords the most comprehensive coverage for cyber risks while traditional insurance lines are increasingly tightening policy language to exclude cyber risk-related costs.

There are four segments to the cyber insurance risk transfer solution:

1. **Your liability to others**
   - Pays defence costs and damages/settlements that you owe to others as a result of a failure of network security or a breach of private information.
   - Pays defence costs and fines/penalties regarding regulatory actions against you arising from a breach.
   - Pays contractual assessments owed due to noncompliance with PCI (credit card) standards due to a breach.
   - Pays defense costs and settlements arising from professional/media errors and omissions (optional coverage).
   - Pays claims alleging financial loss to third parties (such as your employees or clients).
2. **Your costs of breach response**
   - Pays your costs to engage forensic, legal and PR advisors.
   - Pays your costs of notification of the breach to affected individuals as well as credit monitoring and identity theft monitoring.

3. Your own operational costs after a breach

- Reimburses the ransom in the event of cyber extortion as well as for related forensics. The insurer may deploy vendors whom are expert negotiators with immediate access to cryptocurrency.
- Pays your costs to recover data that has been damaged as a result of a computer security failure.
- Pays your loss of income as a result of business interruption caused by a failure of computer security. This can extend to business interruption losses due to an attack on a an outsourced service provider.

4. Additional services from the insurer

- Provides immediate 24/7 help in the event of a suspected incident at discounted panel rates.
- Free or discounted cyber risk management services during the policy period. These may include employee training, help with technology controls, compliance and incident response planning.

THE STATE OF THE CYBER INSURANCE MARKET

Due to the heightened cyber threat environment, cyber insurance underwriters have responded with a laser focus on data security controls when evaluating risks. Virtually every cyber insurance company will require attestation of at least some preventive controls, which likely include multi-factor authentication (MFA), Remote Desktop Protocol (RDP), data backup practices, segregation of networks, encryption, patch management, Privileged Account Management (PAM), Endpoint Protection, employee training and a host of others. Cyber insurance applications often require ransomware supplemental applications that may involve additional questions around controls specifically designed to prevent or mitigate the effects of ransomware attacks.

Without some of these controls in place, many insurance companies are refusing to quote. Those that do will likely demand significant rate increases. Even those considered to be best in class risks that comply with all underwriting required security controls should brace for potential rate increases, limited capacity and possible coverage restrictions.

Connect With Us

Roger Irvine
Head of Construction
Australia & Asia
T: +61 2 9242 2035
E: roger.irvine@ajg.com.au

Robyn Adcock
Cyber/Tech Practice Leader
Australia
T: +61 414 971 918
E: robyn.adcock@ajg.com.au

We do more than help protect your business. We help build it.

AJG.com.au

Gallagher