Specialist Cyber Protection: *For Construction Firms*

Construction firms not a cyber risk? *Think again*.

Construction firms are prime targets with valuable data and information that cybercriminals want:

Protected intellectual property stored and shared online:
Valuable proprietary assets, architectural drawings, blueprints, formulas and equipment specifications for theft, ransom and financial gain.

Employee data kept online, in 3rd party software and in the cloud:
Access to full names, addresses, Social Security numbers, health information and bank details for theft and financial gain.

Access to larger prizes within the same supply chain:
Smaller firms are often targeted because of their supply chain relationships with larger companies.

Valuable information held in new technology and software:
More technology adoption, such as “Building Information Modelling (BIM)”, telematics and project management software means more rich data, sensitive information is accessible online for theft, ransom and financial gain.

High value tools and equipment at risk:
Cybercriminals hack into security systems and CCTV on-site causing property damage and theft.

“Imagine having to explain to a customer, contractor or supplier that their project is delayed or their plans and other sensitive personal data has been stolen or held to ransom.”

How our specialist coverages respond to the threats facing construction firms:

We protect construction firms against their cyber threats by building resilience and minimising risk

01 **Missed Bid** loss coverage
If new business proposals can’t be submitted due to a security breach that interrupts operations

02 3rd party liability for **Bodily Injury** coverage
For bodily injury claims that happen because of a cyber incident

03 Computer system coverage for **Building Information Modeling**
A wide definition that includes problems and issues with BIM, 3rd party hosted websites and design software

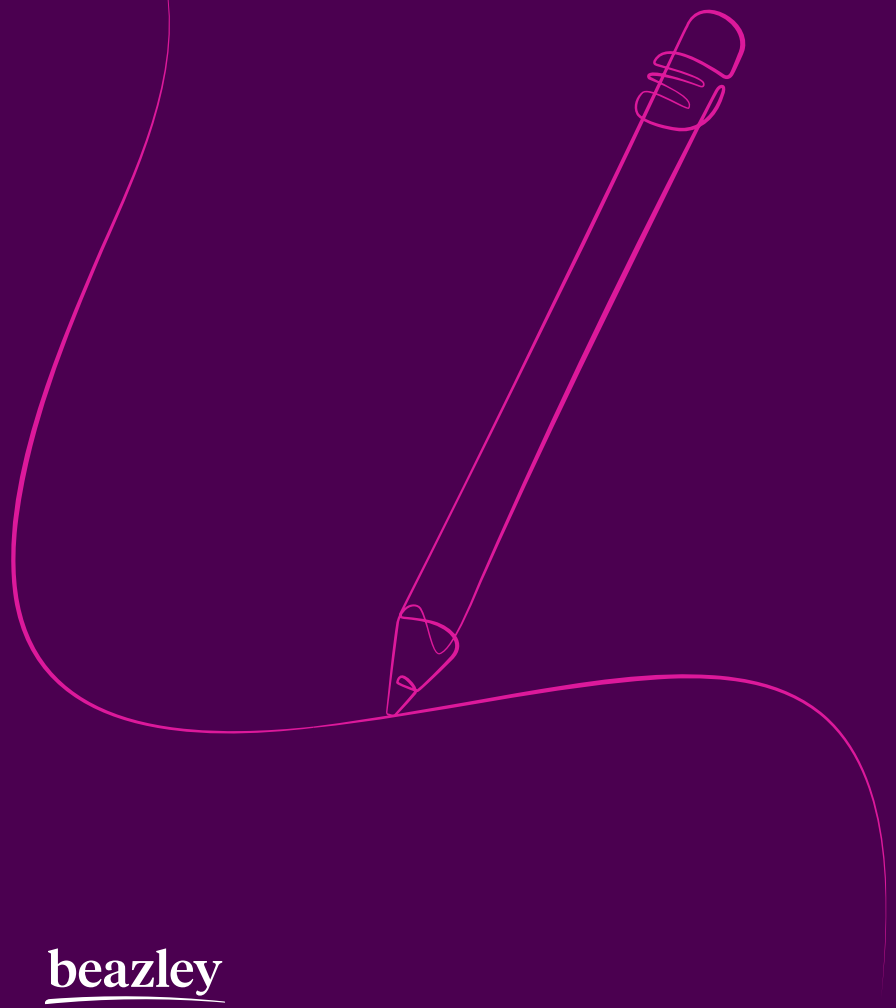
04 Business interruption coverage with a **Qualifying Period**
This incorporates a qualifying period approach instead of a waiting period

05 **Bring Your Own Device** coverage
Included because many contractors and workers utilize their own phones and tablets on-site which increases vulnerabilities

beazley

Claims Case Studies

How our policy supported our client for the duration of the incident



A construction company was the victim of a ransomware attack and the cybercriminals demanded $10M. Without viable backups, the organization had no way to recover and needed assistance.

	How our solution responded
The policyholder immediately contacted their assigned Beazley Cyber Services Manager, who helped select expert privacy counsel and forensic experts to investigate and determine the scope of the incident.	**Cyber Services: Breach Helpline**
The digital forensics team determined that the cyber criminal did not acquire or access PII; privacy counsel concluded that there were no notification or regulatory reporting obligations as a result of the incident.	**Cyber Services: Digital Forensics, Legal Services**
Beazley arranged for the services of a ransom negotiation firm, who successfully negotiated the ransom down to $5M. Beazley organized payment for the policyholder and in return, the organization received a decryption key for recovery.	**First Party Loss Cyber Extortion**
Without access to project systems, the policyholder needed extra workers, resources and equipment to maintain on-site work.	**First Party Loss: Business Interruption, Data Recovery**
The insured submitted a $3M business interruption and data recovery proof of loss, which later included a further $1M due to additional project delays. The incident resulted in $9M in payments from Beazley to cover these expenses, inclusive of the $5M extortion payment.	**Claims Support**

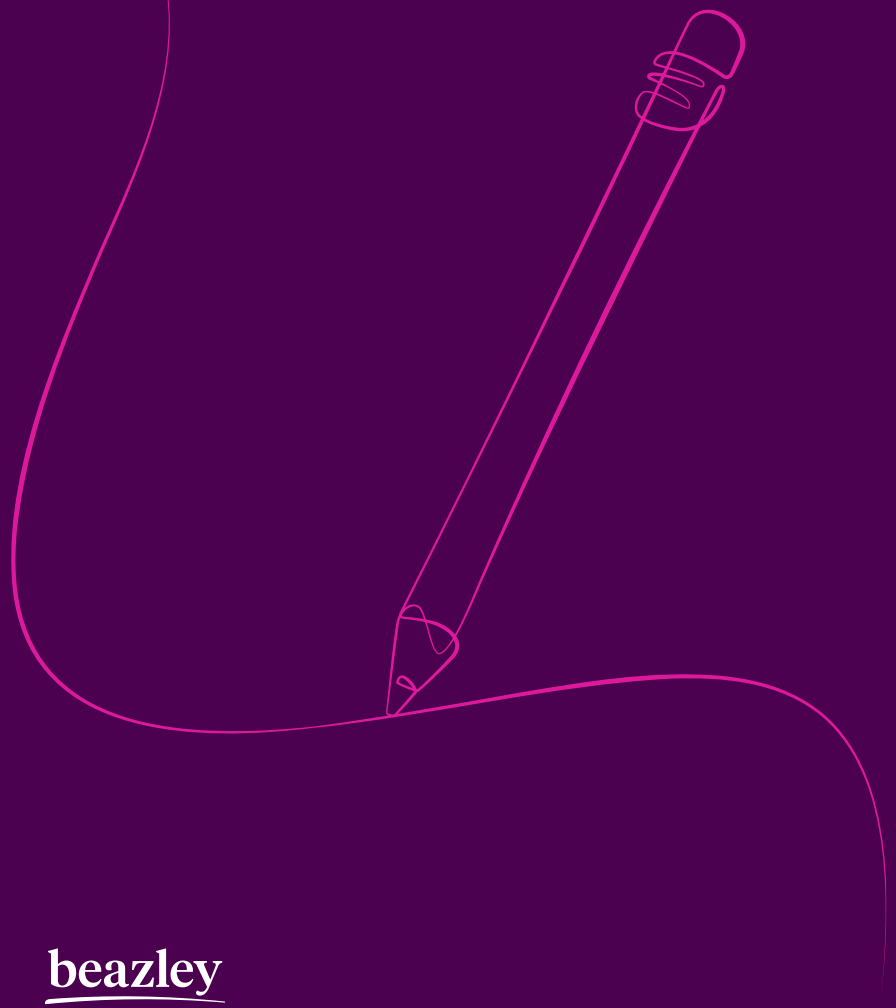
A construction company received an invoice from what they believed to be their existing third-party supplier. The email requested payment regarding a recent materials order and included new wire instructions to an unknown bank account. The construction company, assuming the instructions were valid, sent multiple payments totaling over $1M.

	How our solution responded
The policyholder immediately contacted their assigned Beazley Cyber Services Manager, who reviewed the fraudulent instruction and determined an email compromise was likely. Privacy counsel and forensic services were recommended to investigate further.	**Cyber Services: Breach Helpline**
The investigation confirmed that the fraudulent invoice payments were caused by an email compromise and the investigation concluded that the incident did not result in unauthorized access to PII.	**Cyber Services: Digital Forensics Investigation**
The policyholder recovered $1M of the misdirected funds. Beazley indemnified the remainder of the lost funds and covered the use of privacy counsel and forensic services for the investigation.	**Claims Support**

beazley

Claims Case Studies

How our policy supported our client for the duration of the incident



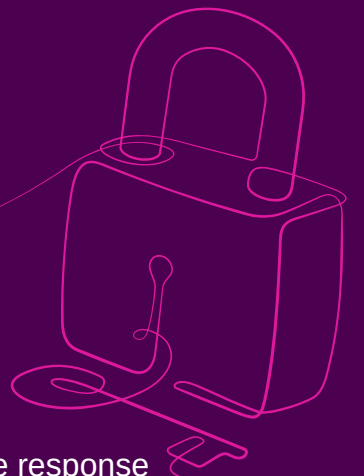
A specialist environmental construction company suffered a ransomware attack that resulted in the theft of sensitive information.

The policyholder immediately contacted their assigned Beazley Cyber Services Manager, who helped select expert privacy counsel and forensic experts to investigate and determine the scope of the incident.	**Cyber Services: Breach Helpline**
The digital forensics team determined that the threat actor exfiltrated sensitive CAD drawings and numerous HR files containing PII; privacy counsel concluded that the unauthorized access to PII triggered individual notification obligations under state law.	**Cyber Services: Digital Forensics, Legal Services**
Privacy counsel drafted notices and Beazley arranged for notification and call center services to support the process.	**Cyber Services: Notification & Call Center**
The exfiltration and potential unauthorized publication of the sensitive CAD drawings by the threat actor posed significant commercial risk. Beazley coordinated for a ransom negotiation firm that was able to settle the ransom event for $3M.	**First Party Loss Cyber Extortion**
Beazley provided coverage for the $3M ransom payment, which resulted in a decryption key and quick recovery, minimizing the overall business interruption loss. Fees incurred by services providers and the notification process were further paid under the policy.	**Claims Support**

How our solution responded

beazley

Reducing Risk:
Cybersecurity advice for construction firms



01 **Incident response planning -** Create a plan that is stress tested regularly. Improve upon the issues raised during testing to improve response times to a cyber incident. *Testing the plan will help minimize damage by creating the appropriate downtime procedures for the business.*

02 **Staff cybersecurity training -** Conduct regular phishing tests to reduce human error. Many cyber incidents happen because someone clicked on something which they shouldn't have. *More than 50% of the claims Beazley received from construction companies could have been stopped by aware and educated staff.*

03 **Backups -** Develop and test backup and recovery plans; keep copies of sensitive or proprietary data in a separate and secure location. Having effective and complete sets of backups can help organizations avoid worst case scenarios. *Keep in mind, recovery often takes much longer than anticipated even with viable back-ups.*

04 **Email security -** Properly configuring spam filters, investing in antivirus protection, and adding multi-factor authentication can help your employees avoid business email compromises, fraudulent instruction losses, and other cyber claims. *Multi-factor authentication can stop nearly all automated cyber-attacks.*

05 **Penetration testing -** Engage a security firm to evaluate your attack surface and assess vulnerabilities; report results to the executive team and recommend future protective actions. *Penetration testing can drive down the costs of an incident significantly*.

06 **Vendor risk management -** Vet suppliers thoroughly, require Cyber Insurance for all service providers, and use standard contracts, questionnaires and forms for uniformity. *Consider who is responsible for notification obligations if the vendor suffers an incident.*

Our clients have access to free risk protection advice and recommended vendors included as standard in their insurance policy.

beazley

Our Cyber Solution for Construction

Key coverages include:

- **Breach response:** Notifications, Forensics, Public Relations Costs, Legal, Crisis Management
- **First party:** Cyber Extortion, Business Interruption, Dependent Business Interruption, Data Recovery
- **Third party:** Data and Network Liability, Regulatory Defense and Penalties, Payment Card Liability
- **eCrime:** Fraudulent Instruction, Funds Transfer Fraud, Telephone Fraud

Construction Appetite