RYAN SPECIALTY

FINANCIAL LINES CYBER

Architects & Engineers

Innovative Insurance Solutions for Complex Cyber Risks

RYAN SPECIALTY | FINANCIAL LINES CYBER

Cyber Exposures for Architects & Engineers

The architecture and engineering (A&E) industry is fundamental to the design and construction of buildings and infrastructure. It encompasses a wide range of services, including architectural design, structural engineering and project management. The primary function of the A&E industry is to create safe, functional and aesthetically pleasing structures that meet the needs of clients and communities.

Reliance on Technology

The A&E sector relies heavily on advanced technology to enhance efficiency, accuracy and collaboration.

Key technologies include:

- **Building Information Modeling (BIM)**: This technology allows for the creation of digital representations of physical and functional characteristics of places, facilitating better design, construction and management.
- **Computer-Aided Design (CAD)**: CAD software is used for creating precise drawings and technical illustrations.
- **Project Management Software**: Tools like Primavera and Microsoft Project help manage timelines, resources and budgets.
- **Geographic Information Systems (GIS)**: These systems analyze and visualize spatial data, aiding in site selection and environmental impact assessments.

Cybersecurity Threats

The integration of these technologies has increased the A&E industry's exposure to cyber threats.

Key threats include:

- **Ransomware**: Cybercriminals can disrupt operations by encrypting critical systems, leading to project delays and financial losses.
- **Data Breaches**: Firms handle sensitive client and project information, making them attractive targets for data breaches. Ransomware continues to be a notable concern for the construction sector, evidenced by a 41% year-over-year increase in attacks as of September 2024[1].
- **Phishing and Social Engineering**: These tactics are used to gain unauthorized access to systems by exploiting human vulnerabilities.

Regulatory Exposure

A&E firms must comply with various standards and regulations as applicable to protect data and ensure cybersecurity.

- **General Data Protection Regulation (GDPR)**: In Europe, GDPR mandates the protection of personal data and imposes strict penalties for non-compliance.
- **National Institute of Standards and Technology (NIST) Cybersecurity Framework**: Provides guidelines for improving critical infrastructure cybersecurity in the US.
- **Cybersecurity and Infrastructure Security Agency (CISA) Guidelines**: Offers guidelines and support for protecting critical infrastructure, including A&E services.

[1] ReliaQuest. (2024, November 12). *Report shows ransomware has grown 41% for construction industry.* https://reliaquest.com/blog/report-shows-ransomware-has-grown-41-for-construction-industry/

The Potential Impact of a Cyber Attack

Cyber attacks on A&E firms can have severe consequences:

- **Operational Disruptions**: Attacks can lead to project delays, loss of client trust and operational inefficiencies.
- **Financial Losses**: Firms can incur significant costs due to system downtime, data recovery and regulatory fines.
- **Reputational Damage**: Cyber incidents can erode client trust and damage the firm's reputation.

Illustrative Loss Scenarios

BUSINESS INTERRUPTION

An architecture firm experiences a ransomware attack that encrypts its BIM and CAD systems. As a result, the firm is unable to access critical project files, leading to delays in project timelines and client consultations.

The firm loses an average of $400,000 per day due to the downtime, which lasts for four days. This results in a total financial loss of $1.6 million. Additionally, the firm incurs further costs related to data recovery, system upgrades and enhanced cybersecurity measures to prevent future attacks.

PRIVACY BREACH

An engineering firm suffers a privacy breach when cybercriminals gain unauthorized access to its client database, compromising the sensitive personal and financial information of over 20,000 clients. The firm faces immediate costs for notifying affected clients, providing credit monitoring services and conducting a thorough investigation, totaling $1.5 million.

Additionally, the firm incurs legal fees and regulatory fines amounting to $2.5 million. The breach also damages the firm's reputation, leading to an estimated revenue loss of $1 million over the next year.

THIRD PARTY

An engineering firm experiences a third-party compromise when a vendor responsible for its project management software suffers a breach. The cyber attack disrupts project timelines and exposes sensitive project and personal data. The breach affects more than 50,000 project files, including confidential design and financial information.

The firm incurs immediate costs for notifying affected clients and providing credit monitoring services, totaling $2 million. Additionally, the firm faces legal fees and regulatory fines amounting to $3 million. The breach also results in a decline in new project acquisitions and an estimated revenue loss of $1.5 million over the next year.

These examples are hypothetical scenarios used solely to illustrate potential outcomes.

RFL's Cyber Solution

Ryan Financial Lines' (RFL) policy was created to look at cyber as a peril, considering how data and systems can cause a wide array of operational challenges. Addressing areas such as business interruption, data restoration, computer crime and social engineering, extortion, and privacy breaches, RFL's policy is intended to help support businesses during cyber incidents. It offers a combination of first-party cost reimbursement and third-party defense and regulatory coverage, with a broad definition of data and computer systems.

1ST PARTY

Crisis Response: Intended to help mitigate the costs and expenses to respond to a system event or privacy breach event

Cyber Extortion: Intended to help mitigate the costs and expenses to respond and resolve an extortion demand that threatens to release or destroy data and/or disrupt or damage the computer system

Computer System Interruption: Intended to help mitigate the net income losses and additional operating costs that occur during a business interruption event due to systems and/or data being taken offline in a malicious attack or other operational failure.
Coverage can include:

- Renting, leasing or hiring external equipment to reduce the duration of a material interruption
- Additional operating costs including services, premises, employing contract staff and overtime cost
- Costs to switch service from a named IT vendor to a new provider if the service cannot be restored within the indemnity period (when event is caused by vendor systems)
- Procuring product or services from alternative sources to meet contractual obligations in supplying the insured's customers
- Paying any service credits or contractual penalties that the insured is contractually required to pay as a result of a material interruption

Reputational Damage: Intended to help mitigate the loss of net income due to a reduction in business or the loss of a service contract with a client in the wake of the public being notified of a system event, privacy breach event, or network security event

Fraud and Social Engineering: Intended to help mitigate the direct financial loss from the wrongful transfer of money by fraudulently accessing the computer system or intentionally misleading an authorized person to transfer funds to a third party purporting to be a vendor, client, or employee. This cover also extends to the financial loss arising from the unauthorized access of a client's telecommunication system by a malicious third party

Data and Software Restoration: Intended to help mitigate the costs and expenses to recover corrupt data or software, and potentially even upgrading/replacing affected software applications or equipment

3RD PARTY

Privacy Breach and Other Third-Party Liability:
Intended to help mitigate the defence costs and damages arising from:

- Any unauthorized disclosure or access to personal or confidential corporate data
- Any liability that arises from other cyber events such as the transmission of a malicious code, contract breaches due to a BI event, and unauthorized access to data by a third party

Vendors

In the event of a cyber incident, RFL provides access to a curated loss control vendor panel not affiliated with RFL, intended to assist with breach response and related services. RFL's cyber solution includes breach response options and access to resources that may assist in managing exposure and mitigating the impact of a cyber event.

Privacy Counsel: US

Pierson Ferdinand LLP

Incident reporting:

RFLCyber@pierfed.com

833-737-7444

Alternate counsel options:

McDonald Hopkins LLC

Cipriani & Werner, PC

Mullen Coughlin

Wood Smith Henning & Berman LLP

Privacy Counsel: Intl.

Kennedys Law LLP

Incident reporting:

RyanFinLinesIR@kennedyslaw.com

UK/EMEA- +44 203 137 8749

AUS/APAC- +613 9498 6688

Alternate counsel options:

Weightmans LLP

Pinsent Masons LLP

Forensics: US

CyXcel

S-RM

Kroll

IronGate

CrowdStrike

PNG Cyber

Palo Alto Networks - Unit 42

Data Mining

CyXcel

Consilio

Asceris

Epiq

Notifications

IDX

Epiq

Kroll

Forensics: Intl.

CyXcel

S-RM

Please note that the use of these vendors is subject to the terms, conditions, and reporting requirements outlined in your policy. We reserve the right to amend our vendor panel at any time.

RYAN SPECIALTY | FINANCIAL LINES CYBER

Who We Are

Ryan Financial Lines was formed in March 2024 to offer clients a wide-ranging, single platform of financial lines products. Ryan Financial Lines brings together the Management and Professional Liability talent at Ryan Specialty Underwriting Managers providing greater synergies and efficiencies to further enhance the solutions and services for our clients and carriers. This unified approach brings together our expanding network of expertise of more than 70 teammates based across a number of key territories, including North America, United Kingdom, Europe and Latin America.

ryanfinlines.com

International: RFL-UK-Cyber@ryanfinlines.com | US: RFL-US-Cyber@ryanfinlines.com