Construction

Cyber risk exposures and solutions

Construction organizations are a target for cyber criminals with motives of financial gain via theft of confidential information or money. Cyber is a broad risk that organizations face by virtue of their reliance on information technology, connectivity, and automated processes. In an increasingly punitive legal and regulatory environment, and with more frequent contractual requirements for cyber liability insurance, forward-thinking companies are taking proactive steps to explore and transfer cyber risk.

Numerous factors contribute to an organization's cyber risk profile, including: action by employees, system and program errors, security measures, industry, nature and quantity of data collected, political or strategic significance, and reliance on technology.

Cyber risk considerations for construction organizations

- Gathering, maintaining, disseminating or storage of private information
- High dependency on electronic processes or computer networks
- Contingent bodily injury and property damage resulting from cyber incidents
- Increased attention of hackers due to high profile buildings or projects, including government buildings, infrastructure (water and power), and military projects
- Utilization of "the cloud" exposes contractors to liability ranging from data security, network outages, and regulatory compliance issues
- Reliance on or operation of critical infastructure
- Subject to regulatory statutes

  HIPAA risk associated with medical facility construction
- Dependence on vendors, independent contractors or additional service providers
- Vendor held information:
  - Building information modelling (BIM) programs
  - Laptops and portable devices (cellphones, tablets, etc.) to access systems from third-party locations such as job sites or hotels

Potential cyber incidents for construction organizations

- Hacker access to construction data, disrupting not only operationally, but also through the physical destruction of data, servers, and infrastructure, or by threatening the safety of people onsite
- Network interruption resulting in lost business income
- Intentional acts committed by rogue employees
- Ransomware attacks

We're here to empower results

cyber.deal.desk@aon.ca

aon.ca

Empower Results®

Scope of traditional cyber coverage available in the insurance marketplace

Third party coverage elements

- ***Security and privacy:*** Defence costs and damages suffered by others resulting from a failure of computer security, including liability caused by theft or wrongful disclosure of confidential information, unauthorized access, denial of service attack or transmission of a computer virus.
- ***Regulatory defence and fines:*** Defence costs for proceedings brought by a governmental agency in connection with a failure to protect private information and/or a failure of network security.
- ***Media liability:*** Defence costs and damages suffered by others for content-based injuries such as libel, slander, defamation, copyright infringement, trademark infringement, or invasion of privacy.
- ***PCI fines and assessments:*** Defence costs for investigations brought by the Payment Card Industry (PCI) in connection with a failure to protect private information and/or network security.

First party coverage elements

- ***Breach response costs associated with:*** breach notification, including the hiring of outside law firms and public relations consultants, forensic costs, credit monitoring/protection, notification hotline/ call centre, identity theft resources.
- ***Network business interruption:*** Loss of income and extra expense due to network security failure.
- ***Dependent business interruption:*** Reimburses the insured for actual lost net income and extra expense incurred when the insured's service provider's computer system is interrupted/suspended due to a failure of network security.
- ***System failure business interruption:*** Coverage for business interruption due to an unintentional or unplanned system failure not caused by a failure of network security.
- ***Data restoration:*** Costs to restore/recreate data/software resulting from network security failure.
- ***Cyber extortion:*** Reimburses the insured for expenses incurred in the investigation of a threat and any extortion payments made to prevent or resolve the threat.

Aon has successfully negotiated the following key coverage enhancements (subject to market agreement per individual risk)

- Full limits for incident response and costs associated with breach notification
- Broad definition of computer system
- Coverage for cyber terrorism
- Deletion of the unencrypted device exclusion
- No failure to patch exclusion
- Supply chain business interruption coverage
- Cost of spoilage – replacement of materials that are transferred
- Bricking coverage – replacement costs for IoT devices
- Delay in delivery/delay in performance coverage
- Environmental liability coverage

Empower Results®

Our approach

Adopting a risk-based cyber insurance strategy

Aon's cyber capabilities can support organizations in embracing a risk-based approach through:

- ***Cyber assessment:*** An enterprise-wide approach to cyber security risk that provides a detailed view into an organization's unique technology profile and threat landscape, with a focus on facilitating risk quantification and insurability.
- ***Cyber impact analysis:*** A data-driven analytical framework supporting organizations to optimize their resilience strategy through mitigation and transfer. Existing risk financing strategies can also be enhanced through modelling cyber loss scenarios and stress testing current limits.

Cyber innovation

- Our policies, on a case-by-case basis, broaden the scope of cyber coverage to include: property damage arising from a network security breach, business interruption and extra expense coverage as a result of a systems failure, contingent network business interruption for IT vendors and the supply chain, and cyber terrorism coverage.

Our cyber resilience framework

Aon and Stroz Friedberg offer a full range of services to help you approach cyber as an enterprise risk and achieve cyber resilience.

Seek

Don't wait until it happens, seek it out.

Some organizations feel that they don't need to be ready for a cyber incident while others feel they are secure. Our team helps you understand and quantify what's at risk.

- Assess your organization's security posture
- Align with proven security frameworks
- Proactively test and hunt for malicious activity
- Quantify the potential financial damage from a cyber incident
- Provide prioritized action lists to improve your cyber resilience

Shield

Knowing what's at risk from a cyber attack won't help you protect your organization.

Protecting your critical assets is one of the most important decisions you make. Let our team help make it easy.

- Defend your company from the financial loss of a cyber incident
- Understand the risks of your investments
- Develop tailored security policies and standards
- Remediate vulnerabilities
- Provide strategic cyber security guidance and develop a program

Solve

When it's all said and done, you need specialists to help you recover.

Our team of seasoned professionals is extremely effective at helping you recover from an attack. From securing your systems to simplifying claims, we make sure you don't miss a beat.

- Respond defensibly to an attack
- Minimize business interruption
- Use cutting edge forensics
- Deploy the top technical, legal, and law enforcement minds who understand legal, regulatory, and financial consequences
- Help maximize coverage and cost recuperation

AON
Empower Results®

Client story

Stroz Friedberg worked with a global engineering and design consultancy operating across 23 locations, who were concerned about how a cyber incident could impact their critical technology and operations.

To understand the risk profile of the organization, we carried out a detailed cyber security and vulnerability assessment of the client's system architecture. This was accomplished by looking at severe and plausible incident scenarios the engineering consultancy might face and a quantification of the potential financial losses.

Following the cyber risk assessment and quantification, the team was also able to recommend and implement a wide range of cybersecurity optimizations through:

- Penetration and red team testing
- System architecture evaluation and improvement planning
- Board-level workshops and planning
- Review of existing cyber insurance policy compared to the total cost of risk

By approaching cyber as an enterprise risk, the global engineering and design consultancy firm gained a comprehensive understanding of the impact of a cyber incident and were able to address the vulnerabilities in their critical technology and operations.

© 2019 Aon Reed Stenhouse Inc. All rights reserved.

This publication contains general information only and is intended to provide an overview of coverages. The information is not intended to constitute legal or other professional advice. Please refer to insurer's policy wordings for actual terms, conditions, exclusions and limitations on coverage that may apply. For more specific information on how we can assist, please contact Aon Reed Stenhouse Inc.

Empower Results®