

From blueprints to breaches

Digital transformation is reshaping
cyber risk across construction
and infrastructure projects



Three things to takeaway:

1 Why adoption of digital systems is expanding the cyber attack surface in the construction sector

2 How cyber incidents can now disrupt physical construction operations

3 Why cyber resilience must extend across supply chains and operational systems

Introduction

Digital transformation is reshaping the construction sector, but risk governance has not consistently kept pace. As organizations adopt connected technologies and digitise project delivery, new exposures emerge across corporate systems and operational environments leading to digital disruption with real-world consequences.

Large construction projects rely on complex supply chains, tightly managed timelines and interconnected digital tools, creating significant cyber vulnerabilities. Legacy systems, rapidly deployed digital solutions and poorly secured third-party connections can introduce weaknesses that threat actors are increasingly able to exploit. To this evolving backdrop, regulators are placing greater emphasis on robust cyber risk management across information technology (IT) systems, operational technology (OT)¹ and third-party suppliers.

As digitalization continues to accelerate, construction and infrastructure companies face growing cyber and digital risks. High uptime requirements and dependence on multiple contractors and suppliers make the sector a particularly attractive target for ransomware and extortion attackers. Meanwhile, rising geopolitical tensions have fed a sharp rise in disruptive cyber activity targeting critical infrastructure and related sectors.

Convergence threats are also increasing. Threat actors are exploiting poorly secured legacy systems and the growing integration between IT and OT environments to maximize disruption or financial/geopolitical gain. Disruption to critical systems and/or suppliers can lead to project downtime, contractual disputes, safety concerns, and wider financial, regulatory and/or reputational consequences.

Figure 1: Top three digital risks posed to the construction sector according to Control Risks experts²



¹ Operational Technology: hardware and software that detects or causes a change in the physical world, through the direct monitoring and control of physical devices, industrial equipment/processes, and infrastructure.
² Based on a survey of Control Risks' senior Digital Risks experts across cyber threat intelligence, cyber advisory and incident response functions.

Adoption of digital solutions and emerging technologies increase cyber exposure in construction

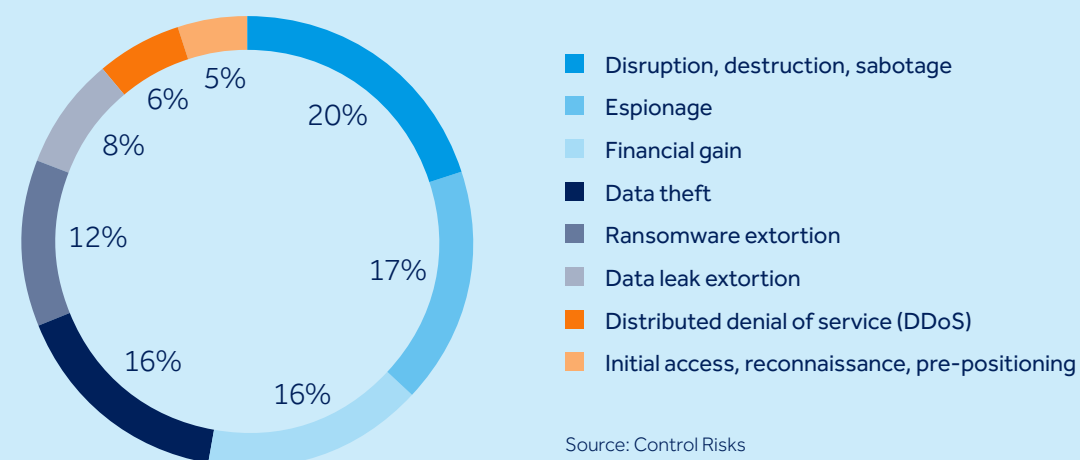
The construction sector has accelerated efforts to digitalize operations in recent years. Organizations are increasingly integrating emerging technologies such as Artificial Intelligence (AI), Internet of Things (IoT) devices³ and sector-specific tools, including Building Information Modelling (BIM).

Digitalization offers clear benefits including improved safety oversight, enhanced compliance monitoring, business process automation and more efficient project delivery. For example, technologies like BIM can be used by construction contractors to collaborate remotely on the same project, ensuring that all participating parties share the same up-to-date view of key information such as building drawings and models.

However, the integration of new digital systems also expands cyber attack surfaces and introduces new forms of risk from a range of attackers. While cloud-based remote collaboration can streamline coordination, cloud-based infrastructure is regularly targeted by cybercriminals and nation-state actors seeking to steal sensitive data or identify access routes to broader corporate IT infrastructure.

The same patterns of insecurity are also applicable for other technologies increasingly integrated into construction operations. For example, a 2025 report identified a 410% year-on-year increase in IoT malware activity targeting the construction sector.⁴ The continued use of legacy systems, highly complex supply chains and strict project delivery timelines further complicate cyber risk management.

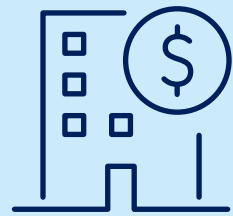
Figure 2: Objectives of cyber incidents targeting the construction sector and adjacent critical infrastructure sectors (share of significant incidents, 2023-26)



³ The internet of things (IoT), or machine-to-machine (M2M) communication, describes the billions of items and gadgets that are connected to the internet and that communicate with each other with little or no human intervention. Such items include domestic white goods, cars, credit cards, lifts and CCTV cameras.

⁴ <https://www.zscaler.com/resources/industry-reports/threatlabz-mobile-iot-ot-report.pdf>

Recent industry data highlights the scale of this transformation:



56%

of investors in construction are looking to allocate more funds for AI adoption.⁵



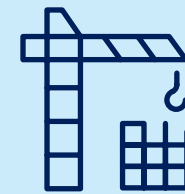
61%

of industry leaders report strategically prioritizing technology and innovation for investment.⁶



34%

of professionals reported being engaged in early pilot testing of AI implementation, with another 14.5% reporting regular use of AI across one or multiple business processes.⁷



USD \$17.72bn

The global BIM construction market was valued at USD 4.38bn in 2024 and is expected to grow to USD 17.72bn by 2034.⁸



In the construction sector, cyber attacks no longer simply compromise the confidentiality of information; they disrupt delivery, stall operations, strain supply chains and expose how quickly digital dependency can become operational risk. As the sector continues to embrace digitalization and automation, the reality of the threats and risks emanating from the digital space are becoming increasingly existential.

Partner in Digital Risks
Control Risks



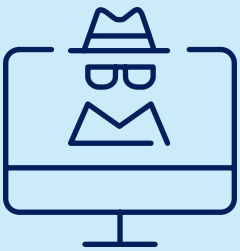
⁵ <https://www.rics.org/news-insights/artificial-intelligence-in-construction-report#>

⁶ <https://kpmg.com/dk/en/insights/market-trends/global-construction-survey.html>

⁷ <https://www.rics.org/news-insights/artificial-intelligence-in-construction-report#>

⁸ <https://finance.yahoo.com/news/bim-construction-industry-research-report-125300365.html>

Extortion and geopolitical tensions drive disruption risks for construction and infrastructure



79%

of Control Risks' experts see ransomware as the threat most likely to significantly impact construction sector organizations

The construction sector is particularly vulnerable to operational disruption. Projects typically run on tight timelines and rely on complex supply chains, meaning delays can quickly lead to escalating costs and contractual consequences. These characteristics make the sector an attractive target for ransomware and extortion actors, who frequently exploit organizations' sensitivity to operational disruption to increase pressure to pay ransom demands.

A 2023 survey examining data resilience in the construction sector found that 77% of respondents tolerate no more than five days without access to project documentation before experiencing severe operational impacts.⁹

In 2025, ransomware incidents resulted in an average of 24 days of downtime.¹⁰ In construction, such disruption has the potential to cause significant delays, impact on third-party subcontractors and suppliers, and generate long-term reputational damage.

Exact costs of extortion incidents vary significantly across victims, depending on factors like the extent to which operational disruption occurs and whether sensitive data has been stolen as part of the incident. However, some indication of costs to constructors comes from a 2020 data theft extortion incident targeting a UK-based entity, wherein recovery and advisory fees totalled GBP 7 million and fines from the UK Information Commissioner totalled GBP 4.4 million.¹¹

⁹ <https://www.construction.com/reports/enhanced-data-resilience-will-help-the-design-and-construction-industry-face-the-risks-that-impact-their-businesses/>
¹⁰ <https://www.totalassure.com/blog/average-ransomware-recovery-time-2025>
¹¹ <https://constructionmanagement.co.uk/poor-cyber-security-cost-interserve-11m-to-clean-up/>





Double extortion operation targets construction, civil engineering company

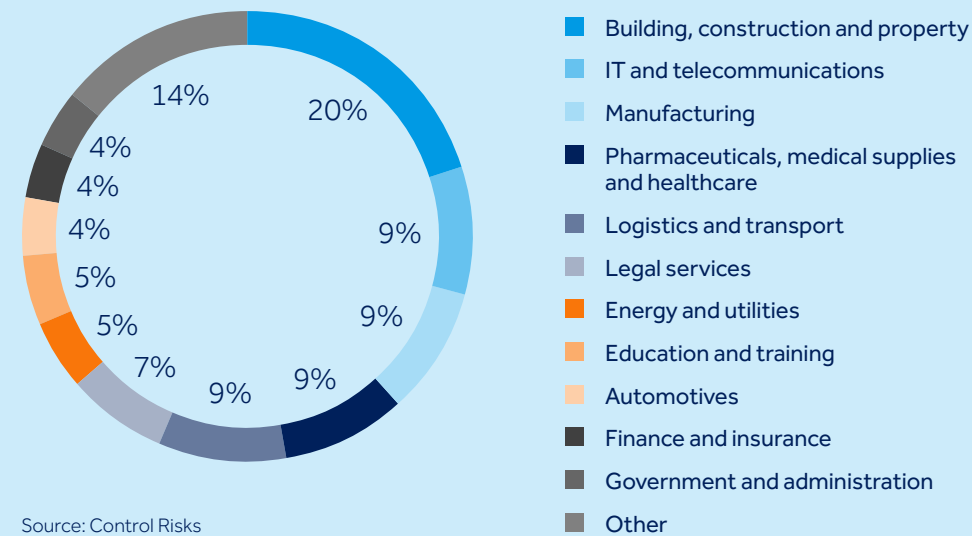
In February 2023, the UK-based construction and civil engineering company Lagan Specialist Contracting Group (Lagan SCG) was targeted in a double extortion operation. The incident was later attributed to Lockbit, a highly sophisticated cybercriminal organization with a long history of high-impact ransomware operations.

The incident resulted in theft of a significant amount of sensitive data relating to employees, including passport numbers and bank details. The stolen dataset was later leaked on the dark web, putting employees at risk of further fraudulent activity. In May 2023, a group action lawsuit was launched with the aim of investigating how the sensitive data breach was allowed to happen and how it affected employee safety.¹²

There is no public record of impact to Lagan SCG from encryption of systems as part of the incident. However, only a few weeks earlier, the same threat actor targeted Royal Mail in a similar incident, causing severe disruption to business operations. Reportedly, Royal Mail spent £10 million on cyber recovery and cyber resilience measures in the wake of this incident, demonstrating the potential financial impact from a successful encryption.

¹² <https://www.kpl-databreach.co.uk/lagan-specialist-contracting-group/>

Figure 3: Sectors targeted in ransomware incidents in 2025¹³



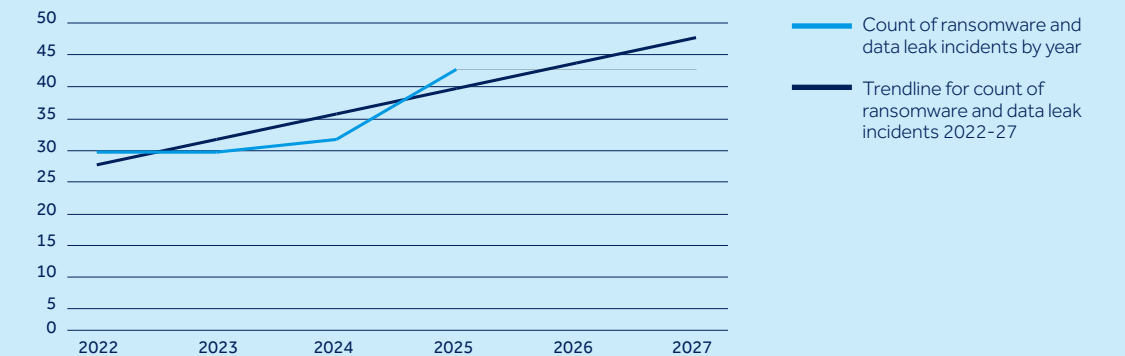
Source: Control Risks

Cybercriminal groups are also exploiting expanding attack surfaces within the sector. As construction firms establish remote connections across networks of contractors and suppliers, for example to facilitate collaborative BIM systems, the number of potential entry points for attackers multiplies.

Similarly, ransomware actors have become more capable of targeting OT infrastructure. A cybersecurity report released in February reported that 119 groups targeted industrial organizations in 2025, representing a 49% year on year increase. Collectively, these groups impacted 526 organizations in the construction sector, with significant operational disruption observed in all cases where ransomware was deployed within OT environments.¹⁴

When deployed within OT infrastructure, ransomware can disrupt industrial control systems (ICS) – specialised software, hardware and network technologies that monitor and control industrial processes – causing shutdowns of physical machinery and limiting or fully removing user control over sensors, built-in safety systems and physical components like valves and pumps.

Figure 4: Ransomware and data leak extortion operations targeting construction and adjacent critical infrastructure sectors (based on significant incidents globally, 2022-25)



Source: Control Risks

¹³ The Control Risks data combines incidents targeting building, construction and property, including real estate, property management and other building and property-associated subsectors. Control Risks' data shows that Building, construction and property was the number one target of ransomware incidents in 2025. While the construction sector has been a primary target of ransomware actors in 2025, this data is also driven by a significant number of incidents against building and property sector entities.

¹⁴ <https://5943619.hs-sites.com/hubfs/312-Year-in-Review/2026/Dragos-2026-OT-Cybersecurity-Report-A-Year-in-Review.pdf?hsCtaAttrib=205683189348>



General contractor targeted in double extortion incident¹⁵

In March 2024, the US-based general contractor Skender Construction was targeted in a double extortion operation by an undisclosed threat actor.

As part of the operation, the threat actor accessed and exfiltrated sensitive data relating to over 1000 individuals. Stolen data reportedly included passport information and social security numbers, likely raising risks of fraud activity targeting affected individuals in the short to medium term.

The threat actor also successfully encrypted IT systems associated with Skender Construction. However, the company had prepared data back-ups to safeguard themselves against operational impact from a data encryption event, enabling it to fully restore systems at speed and limit operational impact of the ransomware incident.

¹⁵ <https://www.constructiondive.com/news/skender-ransomware-attack-chicago-maine/712844/>

Beyond cybercrime, there has been a significant uptick in disruptive cyber events since 2024, linked to state-aligned actors targeting critical national infrastructure (CNI) across Western countries.¹⁶

These incidents are often connected to broader geopolitical tensions, particularly between Russia and NATO members, alongside developments related to the US-Israel-Iran conflict. Cyber attacks increasingly form part of wider hybrid warfare strategies.

Although construction companies are unlikely to be the primary target of such operations, their proximity to CNI, through their role in designing and building physical infrastructure, makes them a credible intentional or collateral victim. For example, a construction firm may be compromised as part of an attack chain targeting a critical infrastructure operator or suffer disruption from a cyber incident directly affecting a supplier or partner.

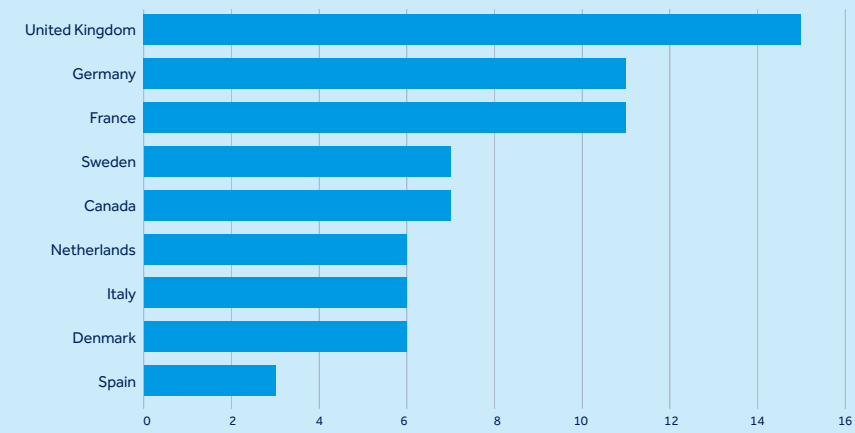


Convergence of construction projects with critical national infrastructure build up is likely to inspire geopolitically motivated or influenced targeting of the sector where it hinders development of critical projects. This is particularly pertinent in states adjacent to geopolitical flashpoints where cyber capable states will look to have economic impact on rivals.”

Global Head of Cyber Threat Intelligence
Control Risks



Figure 5: Number of disruptive incidents by state-aligned groups targeting Canada, Denmark, France, Germany, Italy, the Netherlands, Spain, Sweden and the UK (significant observed incidents, 2022-26)



Source: Control Risks





Pro-Russia cyber activist targets water infrastructure

In 2024, pro-Russia group Z-Pentest carried out a destructive cyber attack against a Danish water utility. After gaining access to control systems, the group manipulated water pressure levels, causing at least three pipes to burst and leaving 500 households without water for several hours.¹⁷

In April 2025, the same actor targeted a Norwegian dam, opening outflow valves and releasing millions of litres of water over a four-hour period before operators regained control over the system. The attack was traced to weak password

protection on a web-accessible control panel and a failure to properly separate OT systems from internet-connected IT systems.¹⁸

Similar incidents have since occurred, including an attempted cyber attack against a Polish water facility.¹⁹ These operations form part of a broader pattern of disruptive cyber activity targeting CNI. Although such attacks have so far primarily targeted utilities and energy sector entities, it is likely that similar tactics could affect adjacent sectors, such as construction, in the future.

¹⁷ <https://www.euronews.com/2025/12/19/denmark-blames-russia-for-cyberattacks-on-water-utility-and-election-websites>

¹⁸ <https://www.reuters.com/technology/norway-spy-chief-blames-russian-hackers-dam-sabotage-april-2025-08-13/>

¹⁹ <https://www.reuters.com/en/poland-foiled-cyberattack-big-citys-water-supply-deputy-pm-says-2025-08-14/>

IT and OT convergence is widening the attack surface and increasing operational risk

As digitalization accelerates, construction companies are increasingly integrating IT systems with OT environments. When implemented effectively, IT/OT convergence can streamline operations by enabling automated communication between systems and improving both project oversight and key processes.

However, this convergence also heightens cyber risk. If systems are not securely integrated, attackers who gain access IT networks may be able to move laterally into OT environments undetected. A 2026 report found that inadequate segmentation between IT and OT systems²⁰ was a contributing factor in 81% of OT incident response cases in 2025.²¹

The risks introduced by architectural insecurities in IT/OT convergence are further compounded by the continued use of legacy systems, the provision of privileged remote access to third parties, and poor cyber security practices, such as credential reuse.

Threat actors are increasingly intent on targeting OT systems directly. Since 2024, there has been a rise in cyber incidents involving state-linked proxies targeting industrial control systems (ICS) in the utilities sector across Europe and North

America. Cybercriminals are also targeting OT more frequently. One OT cyber security provider reported that 23% of incident response cases handled in 2025 involved ransomware targeting OT systems.²² Meanwhile, many cyber actors are exploiting vulnerabilities in legacy systems. In 2025, 67.5% of exploit attempts involved known vulnerabilities that had existed for some time.²³

With many OT systems relying on older software or hardware that cannot easily be patched, this trend creates significant security concerns. By exploiting unpatched systems, attackers may gain initial access to networks, move between systems and ultimately compromise critical operational environments.

As OT becomes an increasingly attractive target for disruptive cyber attacks, the risk to construction companies grows. In addition to immediate operational impacts and risks to safety on construction sites, such disruptions will also likely result in severe financial losses, contractual disputes long-term reputational damage and even regulatory consequences.

²⁰ Inadequate physical or technical separation between IT systems and OT infrastructure, making it possible for a threat actor to more easily move between systems without detection and conduct malicious activity across both IT and OT infrastructure. For example, an OT system may be configured in a way that allows direct, unsecured communication with enterprise IT systems, such as email servers, enabling a threat actor to use a compromised email server to execute commands on the OT system.

²¹ <https://5943619.hs-sites.com/hubfs/312-Year-in-Review/2026/Dracos-2026-OT-Cybersecurity-Report-A-Year-in-Review.pdf?>

²² <https://5943619.hs-sites.com/hubfs/312-Year-in-Review/2026/Dracos-2026-OT-Cybersecurity-Report-A-Year-in-Review.pdf?>

²³ <https://medium.com/s2wblog/detailed-analysis-of-recent-trends-in-known-exploited-vulnerabilities-c81678a47f39>



Regulatory pressures bring new expectations for cyber risk management

Figure 6: Top 3 drivers of intent to target the construction sector according to Control Risks experts

- 1 Perceived low cybersecurity maturity
- 2 Complex supply chains and third party networks
- 3 Poorly secured smart buildings and systems

Regulators are increasingly taking a broader view of cyber security and CNI protection. Regulatory frameworks such as the European Union's updated Network and Information Systems Directive (NIS2) anticipated updates to equivalent regulations in the UK, and Canada's proposed Critical Cyber Systems Protection Act (CCSPA) introduce new expectations for organizations operating CNI and their supply chains.

These regulatory requirements are likely to cascade through supply chains, including construction companies supporting infrastructure projects.

As a result, organizations across the sector will need to adopt a more structured, risk-led and resilience-focused approach to cyber risk management. This includes strengthening governance, improving IT/OT security practices and ensuring robust incident response planning is in place.

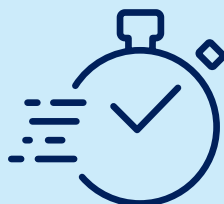


Figure 7: Key components of effective cyber risk management



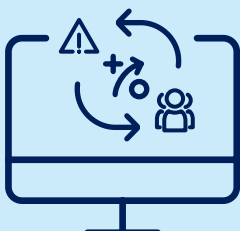
Governance

- Implement comprehensive cyber risk management
- Establish senior oversight and accountability



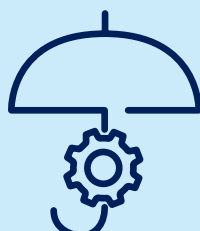
Incident response

- Revise and update incident response and business continuity plans, ensuring compliance with reporting requirements.
- Conduct regular testing against real-world threat scenarios



Supply chain risk management

- Conduct vendor risk assessments
- Include cyber security as part of contracting



Technical mitigations

- Update security controls including network segmentation between IT and OT systems, access control, endpoint detection and response (EDR) tools and updated patching
- Map legacy systems and develop mitigation strategies for systems that do not fall in normal patching cycles



Training and awareness

- Conduct regular employee awareness training
- Encourage employees to report suspicious activity

At the heart of underwriter insights



Kyle Gray
Underwriter Team Lead, Cyber

From a cyber underwriting perspective, construction is highly exposed to operational disruption and financial loss. In Canada, the sector's rapid adoption of interconnected IT systems, operational technology, third party platforms and supply chains which are often spread across multiple active sites and regions creates complexity that can be exploited. A single cyber incident can stall projects, restrict access to critical systems and ripple through contractors and suppliers, resulting in delays, cost overruns, liquidated damages and lost revenue and reputation.

This exposure is growing as cyber risk is increasingly viewed through the lens of operational resilience. Canadian firms are facing rising expectations from clients, lenders, and public sector counterparties around their ability to continue operations through disruption. While regulation is less prescriptive than in

some European markets, guidance from federal bodies such as the Canadian Centre for Cyber Security and evolving requirements tied to critical infrastructure, public procurement and cross border operations are raising the baseline for cyber resilience. For many construction businesses, demonstrating resilience is becoming essential to securing work, particularly on large or infrastructure linked projects.

Cyber incidents are also reflecting this shift. Losses are less about data theft alone and more about downtime – systems locked by ransomware, workflows interrupted and, in some cases, physical operations affected through connected building systems or industrial controls. The distinction between cyber risk and business interruption has effectively disappeared.

Notably, many serious losses still stem from relatively basic issues: identity & access management, legacy systems that cannot be easily patched, trusted third party access, and social engineering. Addressing these fundamental cyber risks can significantly reduce both the severity and duration of disruptions.


Beyond prevention, response capability is critical. The speed at which a firm can contain an incident, make decisions, and restore operations has a direct impact on project disruption and financial loss. Tested incident response plans, clear governance and realistic recovery assumptions are therefore key underwriting considerations.

For brokers and underwriters, conversations are increasingly centered on tangible outcomes rather than abstract threats: how long operations could be down, which projects would be affected, and how quickly work could resume. Ultimately, in the Canadian construction market, cyber risk and operational interruption are inseparable.

Survey

As part of this report, we surveyed 20 senior experts across Control Risks' Digital Risks practice for their views on the key threats, risks and vulnerabilities in the construction and infrastructure sector, from across Control Risks' EMEA, APAC and Americas teams, including London, Berlin, Copenhagen, Hong Kong, New York, Washington, Sydney, and Bogota.

The survey includes answers from experienced consultants, practice leaders and the majority of Partners in CR Threat Intelligence, Cyber Advisory and Incident Response functions. Where we reference data points or citations from "Control Risks' experts", this draws from the qualitative and quantitative findings of the survey.



For more information on this report, visit qbecanada.com or contact us at canadaenquiries@ca.qbe.com

QBE Canada
QBE Services Inc.
6 Adelaide St. E
7th Floor
Toronto
Ontario, M5C 1W4
Canada
+1 416 682 5930

QBEcanada.com

This report was produced by QBE with Control Risks.

QBE European Operations plc ("EO plc") is registered in England (No. 2641728). Its registered office is at 30 Fenchurch Street, London EC3M 3BD. The principal subsidiaries of EO plc are: QBE UK Limited registered in England (No. 01761561) ("QBE UK"). QBE Underwriting Limited registered in England (No. 01035198) ("QUL"). QBE UK and QUL are authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority with their registered offices at 30 Fenchurch Street, London EC3M 3BD. QBE Management Services (UK) Limited (No. 3153567) is an appointed representative of QBE UK and QUL. QBE in Canada operates through QBE Services Inc., which is registered in the Province of Ontario Canada No. 002193827.

 **QBE**
At the heart of it