PLATFORM

FEBRUARY 12, 2025

Cyber Risk: A Compliance Issue for Construction

By David Bowcott & Sadie Perri

WHAT BILL C-8 MEANS FOR CONTRACTORS

Construction projects — and the assets they deliver — are more digitally exposed than ever before. Building automation systems, networked access control, smart meters, IoT sensors, digital twins, cloud-based project management platforms, and remote commissioning tools have become standard across large infrastructure and commercial projects. While these technologies have delivered efficiency and operational insight, they have also expanded the cyber "attack surface" of both construction sites and the operating assets that follow.

During construction, temporary networks, multiple vendors, and frequent system integrations create vulnerabilities that do not exist once an asset is fully operational. Once the project is complete, those same technologies often sit at the heart of energy systems, transportation networks, data centres, and industrial facilities that society depends on. This growing digital footprint is the backdrop against which **Bill C-8** has been introduced — and why cybersecurity is increasingly becoming a construction-phase issue.

WHAT BILL C-8 DOES — AND WHY CONTRACTORS SHOULD CARE

Bill C-8 is federal legislation intended to strengthen cybersecurity protections across Canada's critical infrastructure sectors. It introduces a new **Critical Cyber Systems Protection Act** and expands federal authority under the Telecommunications Act to issue binding cybersecurity directions.

The legislation applies directly to designated operators in sectors such as telecommunications, energy, pipelines, nuclear facilities, federally regulated transportation, and financial market infrastructure. These operators are required to implement cybersecurity programs, manage supply-chain risk, report incidents, and comply with government-issued security directions.

Construction contractors are not designated operators under the legislation. However, they play a central role in designing, building, integrating, and commissioning the physical and digital systems those operators rely on. As a result, cyber risk is increasingly being pushed downstream — not through regulation, but through contracts.

PROJECTS MOST LIKELY TO BE AFFECTED

The projects most exposed to Bill C-8 are those where construction work intersects with **digitally enabled, federally regulated infrastructure.** This includes power generation facilities, substations, pipelines, LNG facilities, rail signaling systems, ports, airports, data centres, telecom infrastructure, and nuclear facilities.

In these environments, contractors often interact directly with control systems, operational technology, commissioning software, and networked building systems. From an owner's perspective, those interactions represent potential cyber vulnerabilities — particularly during construction, when access is broad and systems are in flux.

HOW CONTRACTS ARE LIKELY TO CHANGE

Owners and operators responding to Bill C-8 are already beginning to reflect cyber risk in their construction contracts. Contractors should expect to see fewer standalone "cybersecurity" sections and more integrated risk language woven into existing provisions.

Common themes include clearer definitions of responsibility for contractor-controlled digital systems, expanded subcontractor oversight obligations, incident notification requirements, and restrictions on certain technologies or vendors. Importantly, these clauses are often framed around risk management and cooperation, rather than treating contractors as regulated entities in their own right.

For general contractors, the key issue will be scope discipline — ensuring that cyber obligations are tied to systems and data within their control, and not extended to the owner's operational environment once the asset is live.

CYBER INSURANCE WILL FOLLOW THE RISK

As cyber obligations appear more frequently in construction contracts, insurance requirements are following close behind. On projects tied to critical infrastructure, owners are increasingly asking contractors to carry **Cyber Liability Insurance** alongside traditional builders risk and liability coverage.

These policies are typically designed to respond to incidents arising from the contractor's own digital environment — such as ransomware affecting project systems, unauthorized access to construction data, or costs associated with forensic investigation and system restoration. Limits commonly range from **$2 million to $5 million**, depending on project size and complexity.

However, it is worth acknowledging that publicly reported cyber losses demonstrate how quickly costs can escalate. Incidents such as the Colonial Pipeline ransomware attack, the NotPetya event affecting industrial firms, and breaches impacting major data centre operators illustrate that cyber losses can reach into the hundreds of millions when operational disruption, remediation, and downstream impacts are considered.

For construction contractors, this does not mean cyber insurance limits must mirror worst-case operational losses. But it does underscore the importance of aligning contractual liability with insurable exposure, and resisting open-ended indemnities that far exceed available coverage.

WHAT CONTRACTORS SHOULD BE DOING NOW

Bill C-8 does not impose new regulatory duties on construction firms. What it does do is signal a shift in how cyber risk is viewed across the infrastructure lifecycle — including during design and construction.

Contractors working in affected sectors should take practical steps now: understand which systems they control, how digital access is managed on site, how incidents would be detected and escalated, and whether existing insurance coverage aligns with emerging contractual expectations. Early engagement with legal and insurance advisors can help ensure that cyber provisions are reasonable, scoped, and commercially insurable.

The construction industry has navigated evolving risk landscapes before — from safety regulation to environmental compliance to complex insurance structures. Cybersecurity is simply the next evolution. Bill C-8 makes it clear that for certain projects, cyber risk is no longer something that starts at handover. It begins on the job site.

Questions? Contact:

David Bowcott, Executive Vice President
Construction Industry Group
dbowcott@platforminsurance.com
416-566-5973

Sadie Perri, Senior Vice President
Construction Industry Group
sperri@platforminsurance.com
416-346-6643

ABOUT PLATFORM

PLATFORM is a national, privately owned Canadian brokerage specializing in insurance, surety, sub-default insurance and benefit solutions. We are driven by industry at the heart of everything we do. Our team blends sophisticated expertise with strategic thinking, ensuring that our tailored solutions meet and exceed client expectations.

www.platforminsurance.com

info@platforminsurance.com

416-434-4322

PLATFORM