
CYBERSECURITY
IS THE NEW
INFRASTRUCTURE
ccn

Table of Content

François Guay

INTRODUCTION

Cyber risk is no longer a future concern. The market has already written the rules. Cyber maturity now determines who gets insured, contracted, and allowed to operate.

There are moments when a discipline evolves. And there are moments when it becomes something else entirely.

We are at that moment with cybersecurity.

For years, it has been treated as a technical function, important but secondary to growth and operations. That framing no longer holds. What we are seeing now is a structural shift. Cybersecurity is no longer just protecting systems. It is determining who gets to participate.

At the Canadian Cybersecurity Network, this shift is visible across our community of over 46,000 members, spanning enterprises, governments, insurers, legal experts, and technology leaders. The signals are consistent. Insurance coverage is being granted or denied based on cyber maturity. Supply chains are enforcing security as a condition of partnership. Regulatory frameworks are embedding cyber readiness into market access. Organizations are increasingly judged not only on what they deliver, but on whether they can be trusted to operate.

Cybersecurity has become infrastructure. It now underpins access to markets, capital, contracts, and growth. Like all infrastructure, it is invisible until it is missing. When it is, the consequences are immediate. Organizations are delayed, restricted, or excluded, often without fully understanding why.

This report does not describe the cybersecurity landscape. It defines the shift underway.

The contributors to this brief represent key control points in today's economy: legal, insurance, enterprise security, operational technology, and supply chains. Together, they reveal a clear reality. Cyber maturity is being used, explicitly and implicitly, to grant or deny access.

That is the shift.

Cybersecurity is no longer a support function. It is the foundation of participation in the modern economy.

Those who recognize it early will reduce risk, move faster, compete more effectively, and lead.

François Guay
Founder, Canadian Cybersecurity Network

Cybersecurity Is the New Infrastructure

Why Digital Trust Now Determines Who Gets to Compete

Infrastructure has always defined who gets to participate. Roads enabled commerce. Ports moved goods. Energy grids powered growth.Today, a new layer of infrastructure is emerging; intangible, yet critical. Cybersecurity.

In an economy shaped by AI, automation, cloud platforms, and real-time data exchange, cybersecurity maturity is no longer just a technical requirement. It is a gatekeeping standard.Those who meet it gain access.

Those who can't are quietly excluded.

This transformation is being driven not just by technology, but by how risk is evaluated and trust is granted:

- Cyber insurers are declining or restricting coverage for firms without proven controls, making insurance a business eligibility test, not just a risk product.
- Procurement and supply chain leaders are embedding security into contract requirements, creating access tiers defined by trust posture.
- OT operators are refusing to integrate vendors without demonstrated resilience, recognizing that digital interdependence equals shared risk.
- Lawyers and breach responders are advising companies pre-incident, because readiness now defines the outcome.
- Governments are conditioning funding and procurement on real cybersecurity posture, not declarations.

This report is not about cyber risk alone. It's about business access.It brings together five frontline experts, a cyber insurer, a breach lawyer, a CISO, an OT strategist, and a supply chain risk lead, to examine how cybersecurity has evolved from back-office cost center to front-door qualifier.

Their collective message is clear:

Cybersecurity is now infrastructure.

It enables access to capital, contracts, markets, and continuity.

And like any infrastructure, its presence, or absence, decides who moves forward.

This is the shift boards and executives must grasp:
Digital trust isn't soft. It's structural.

And it's deciding who gets to compete.

Market Shift:

Cybersecurity as a Condition of Business

A structural shift is underway. Cybersecurity is no longer a technical function or a back office control. It has become a condition of doing business.

Across industries, organizations are encountering the same reality from different directions. Insurers are tightening underwriting requirements and declining coverage where basic controls are not in place. Legal expectations are expanding, with greater scrutiny on governance, accountability, and duty of care. Supply chains are enforcing security standards as a prerequisite for participation. In operational technology environments, cyber risk is now directly tied to physical safety and continuity. At the enterprise level, CISOs are no longer measured solely on protection, but on their ability to enable business operations under increasing risk pressure.

These are not isolated developments. They are converging into a single market force.

Cyber maturity is becoming a gate. It determines who can secure insurance, who can meet contractual obligations, who can operate within critical infrastructure environments, and ultimately, who is allowed to participate in the digital economy.

What makes this shift significant is not the existence of cyber risk, but how it is being enforced. Requirements that were once considered best practices are now being operationalized as entry conditions. Multi factor authentication, incident response readiness, backup integrity, and governance oversight are no longer recommendations. They are being validated, audited, and in many cases, required before business can proceed.

The consequence is clear. Organizations that cannot demonstrate a baseline level of cyber maturity are increasingly facing friction at every point of growth. Contracts are delayed or lost. Insurance coverage is limited or denied. Partnerships are restricted. Expansion into new markets becomes more difficult.

At the same time, organizations that can demonstrate digital trust are gaining a measurable advantage. They move faster through procurement processes. They meet insurer expectations. They are seen as lower risk partners in supply chains and ecosystems that are under pressure to secure themselves.

AI is accelerating this shift. As organizations embed AI into operations and decision making, expectations are expanding beyond security to include governance, control, and accountability. At the same time, boards are being held directly responsible for cyber and technology risk. Maturity is now evaluated not just on controls, but on whether leadership understands and governs these risks.

This is the new operating environment.

Cybersecurity is no longer just about reducing risk. It is about enabling access.

In this context, digital trust is not a brand attribute or a communications message. It is an operational capability, one that is increasingly verified at the moment decisions are made.

The organizations that understand this shift are not treating cybersecurity as a cost center. They are treating it as infrastructure.

Imran Ahmad
Senior partner at Norton Rose Fulbright

Legal Readiness: Why Breach Preparedness Now Determines Who Gets to Do Business

Every major cyber incident reinforces one truth: organizations that fare best are not necessarily those with the most advanced security tools or with the largest IT budgets. They are the ones that engage experts early, such as legal counsel, build breach readiness into their operations, and treat incident response planning as a business function rather than an afterthought.

That distinction is no longer just about surviving a crisis. It is becoming a condition of participation in the digital economy.

From Incident Response to Business Readiness

Too often, legal counsel is brought in after the damage is done, after data has been exfiltrated, after regulators have been notified on a compressed timeline, and after executive teams have made statements they cannot easily walk back. Organizations that invest in breach readiness before an incident occurs operate from a fundamentally different position. They have playbooks that have been tested, communications frameworks that have been rehearsed, and decision-making structures that function under pressure. That preparation does not just reduce legal exposure. It preserves operational continuity, protects relationships, and enables faster recovery.

Legal Readiness as a Market Signal

Regulators, insurers, and enterprise customers are no longer satisfied with vague assurances about cybersecurity. They want evidence of preparedness. They want to see documented incident response plans, tabletop exercises, regulatory awareness across jurisdictions, and governance structures that demonstrate defensible decision-making. Legal readiness has become a signal of organizational maturity. Companies that can demonstrate it are better positioned to secure coverage, win contracts, and satisfy the growing expectations of regulators in Canada, the United States, and the European Union. Those that cannot are finding themselves locked out.

Ransomware and the Pressure on Leadership

Ransomware remains the most disruptive threat facing organizations today, and the legal and business consequences extend far beyond the ransom itself. The pattern is consistent: operational shutdowns lasting weeks, supply chain relationships severed, regulatory investigations triggered, and executive teams forced into high-stakes decisions with incomplete information and no margin for error. The organizations that navigate these events most effectively are the ones that have already mapped their legal obligations, established privilege structures, and prepared their leadership to make informed decisions under crisis conditions. Without that foundation, every choice becomes riskier and more costly.

Privilege, Governance, and Trust

Legal strategy is not peripheral to cyber maturity. Privilege protocols protect the integrity of investigations. Governance structures ensure accountability. Documentation practices create defensible records that stand up to regulatory scrutiny, litigation, and insurer review. These are not abstract legal concepts. They are the mechanisms that allow organizations to respond credibly, recover efficiently, and maintain the trust of customers, partners, and stakeholders.

Enabling Growth, Not Just Managing Risk

Organizations that have invested in legal and breach response readiness consistently realize practical benefits beyond crisis management. They secure cyber insurance more easily and on better terms. They meet procurement and supply chain security requirements without scrambling. They reduce regulatory friction across multiple jurisdictions. And they maintain the trust that underpins every business relationship.

Legal readiness is no longer a backstop. It is part of the infrastructure that enables companies to compete, grow, and participate in modern digital markets. The question is no longer whether organizations can afford to invest in it. It is whether they can afford not to.

Imran Ahmad is a senior partner at Norton Rose Fulbright and serves as Head of Technology in Canada and Co-Head of Cybersecurity & Data Privacy. He advises boards of directors, senior executives, and in-house legal teams on high-stakes matters at the intersection of technology, cybersecurity, data protection, artificial intelligence, and enterprise risk. You can connect with Imran Linkedin

Patrick Bourk
Vice President, Navacord

How Cyber Insurers Are Setting the New Standard for Cyber Maturity

In today's economy, cybersecurity is no longer a back-office IT function—it is foundational infrastructure. Just as organizations once needed reliable power and transportation to operate, they now require demonstrable cyber maturity to participate in the digital ecosystem. Increasingly, the cyber liability ecosystem (i.e. insurance companies and insurance brokers) are acting as the gatekeepers of this new infrastructure, determining which organizations are "fit" to operate in a connected economy.

From an underwriting perspective, insurers have become de facto assessors of cyber maturity. This shift is driven by hard claims data.

The NetDiligence 2025 Cyber Claims Study shows that ransomware and business email compromise remain the dominant drivers of loss, accounting for the majority of claims and costs, with Canadian incidents averaging approximately US $874,000. More importantly, losses tied to business interruption can increase total claim costs by over 650%, underscoring that resilience—not just prevention—is critical.

As a result, insurers are no longer simply pricing risk—they are actively shaping it. Cyber maturity assessments now go far beyond questionnaires. Underwriters are scrutinizing identity security (e.g., MFA coverage), endpoint detection and response (EDR), privileged access management, and incident response readiness. Importantly, they are also evaluating third-party risk, reflecting the growing reality that supply chain breaches can create systemic losses across entire ecosystems.

This evolution is reinforced in the latest findings from the Canada Cybersecurity Network's State of Cybersecurity in Canada 2026 Report, which underscores a widening gap between digital adoption and cyber readiness. The report highlights that identity has become the primary attack surface, with human-to-machine identity ratios now exceeding 1:80 and a striking 91% of users operating with elevated privileges—dramatically increasing organizational exposure. At the same time, the report points to a surge in AI-enabled attacks and a growing preparedness gap across Canadian organizations. Traditional perimeter defenses are no longer sufficient. The implication is clear: cyber maturity must now be measured by how well organizations manage identity, privilege, and real-time verification—areas that insurers are rapidly incorporating into underwriting expectations.

The practical implication is clear: certain controls are no longer optional. Insurers are insisting on baseline measures such as multi-factor authentication, robust backup and recovery capabilities, continuous monitoring, and tested incident response plans. Organizations unable to demonstrate these controls may face higher premiums, restricted coverage, or exclusion from the cyber insurance market altogether. In effect, lack of cyber maturity can now limit an organization's ability to transact, partner, or even operate in the digital economy.

Cyber insurance is also reshaping business behavior in more subtle ways. Coverage terms increasingly reward proactive risk management—organizations that conduct tabletop exercises, implement zero-trust architectures, and maintain strong governance frameworks are not only more insurable but also more competitive. As regulatory scrutiny intensifies—particularly under guidance such as Guideline B-13 from the Office of the Superintendent of Financial Institutions—insurers are implicitly encouraging organizations to build defensible, auditable security programs that can withstand both attacks and post-breach investigations.

Ultimately, cyber insurers have become critical architects of the digital economy. By defining what "good" looks like in cybersecurity, they are setting the minimum standards for participation. In this sense, cyber maturity is no longer just a technical benchmark—it is a prerequisite for economic inclusion.

Patrick is a lawyer and specialty commercial insurance expert with a passion for helping companies and professionals with their specialty insurance and risk management needs. He is currently the Cyber & Professional Lines Practice Leader for Navacord, Canada's fastest growing insurance brokerage. As a specialty insurance expert, he collaborates with Navacord's 50+ National Broker Partners to build and support the strategic direction of specialty insurance product lines including professional liability and directors' & officers' liability insurance but with an emphasis on cyber liability insurance.
You can connect with Patrick Linkedin

Robert Knoblauch
Global Chief Information Security Officer

Supply chains, AI and the illusion of control in cybersecurity

For years, cybersecurity leaders focused on what they could control: their own networks, systems and people. Asset inventories, vulnerability management and incident response formed the backbone of security programs.

That model no longer reflects reality.

The enterprise perimeter began dissolving nearly two decades ago, as cloud computing and third-party integrations blurred the line between "internal" and "external." Today, organizations operate within deeply interconnected supply chains, where critical services depend on vendors and platforms outside their control.

In this environment, the organization is no longer a single entity—it is an ecosystem.

Therefore, cybersecurity programs must expand accordingly.

Artificial intelligence is accelerating this shift. Agentic AI, capable of autonomous decision-making, is embedding itself into workflows that span multiple organizations. This creates tighter dependencies across disparate suppliers and operational systems—driving efficiency, but also increasing fragility.

When one component fails, the impact is no longer isolated.

Resilience can no longer be tested in isolation either. Organizations should conduct end-to-end business continuity and disaster recovery exercises that include key third parties. These tests expose how failures cascade across systems and where hidden dependencies exist.

Consider a simple example: if an SMS provider fails and one-time passcodes cannot be delivered, authentication workflows break down. Customer-facing applications may become inaccessible. Revenue and trust are immediately at risk.

The question is not whether a vendor will fail, but how prepared you are when it does.

As AI becomes embedded in operations, organizations must also prepare for systems behaving in unintended or compromised ways. This is where "kill switches" become essential. If a vendor is compromised or an AI-driven process produces untrusted outcomes, organizations need the ability to rapidly isolate that component without halting the business.

Visibility is equally critical. Employees are already using AI tools, often outside formal approval. Without understanding what is being used and how data flows through it, organizations are operating with significant blind spots. Policies alone won't solve this. Security controls must be embedded directly into workflows and enforced through technology, not documentation. We all know how many of us actually read the policies.

The reality is clear: organizations no longer control their full operating environment. Supply chains are complex, AI is accelerating interdependence, and the boundary between internal and external risk has effectively disappeared.

The goal is no longer control, it is resilience.

That means testing dependencies, building containment mechanisms, improving visibility, and integrating security into how work actually gets done. Because in a world where saying no to AI is not an option, the organizations that succeed will be those that design for failure—and recover faster than everyone else.

Rob Knoblauch is a seasoned CISO leader with 25+ years of experience in global information security leadership positions. He has developed and implemented global enterprise information security solutions (Endpoint, Network, Data, User, Cloud, IoT) for two of Canada's largest banks, and other financial institutions such as Tangerine Bank, Toronto Stock Exchange and a variety of FI's outside of Canada. You can connect with Robert Linkedin

Tristan Kim
Director, Cyber Risk, Development at KORE Solutions

Four Driving Forces Making OT Cybersecurity the License to Connect and Operate

In today's connected industrial environments, cybersecurity maturity is no longer a supporting capability—it is becoming a condition of participation. Across manufacturing, energy, utilities, and logistics, trust is no longer granted based on reputation or long-standing relationships. It is enforced through technical validation, connection policies, and operational safeguards. What we're seeing on the ground is clear: digital trust is already operating as infrastructure in OT environments—quietly determining who gets to connect, and who does not.

This shift is being driven by four converging drivers that are actively reshaping how industrial environments operate:

DRIVER ONE:

First, the threat landscape has fundamentally changed. Canada's Canadian Centre for Cyber Security continues to identify ransomware and state-sponsored activity as leading risks to critical infrastructure. Industrial environments are no longer peripheral targets—they are part of geopolitical strategy. As connectivity increases, so does exposure. In fact, industry reporting shows that over 70% of industrial organizations have experienced a cyber incident impacting OT systems—evidence that this risk is no longer hypothetical.

DRIVER TWO:

Second, regulatory pressure is catching up. Canada's proposed Bill C-8 signals a clear move toward mandated cybersecurity controls across essential sectors. Once enacted, organizations will need to demonstrate formal cybersecurity programs, incident reporting, and risk mitigation—not just in IT, but across operational environments. This aligns with standards such as IEC 62443 and NIST SP 800-82, reinforcing that OT security must be engineered with safety, uptime, and resilience in mind.

DRIVER THREE:

Third, cyber insurance is tightening in parallel. According to Statistics Canada, cyber incident recovery costs exceeded $1.2 billion in 2023. As losses grow, insurers are demanding stronger proof of risk management—particularly in OT. Organizations that cannot demonstrate visibility into OT assets or effective controls are increasingly facing higher premiums, exclusions, or non-renewals.

DRIVER FOUR:

Fourth, there is a growing supply-demand imbalance. Canada continues to face a shortage of cybersecurity professionals, with an even greater gap in OT. Securing industrial systems requires a hybrid skill set—combining cybersecurity, engineering, and operational reliability—that remains scarce across the market.

These drivers are not theoretical—they are showing up in day-to-day operations. I'm seeing manufacturers delay supplier onboarding until minimum security controls are validated. Suppliers that cannot demonstrate segmentation or monitoring simply don't get connected. Building operators are restricting remote vendor access until automation systems are properly segmented. Insurers are pausing renewals until OT risks are understood. Security is no longer a blocker—it is the gatekeeper of speed. This is no longer just a security investment—it is a prerequisite for revenue participation and ecosystem access.

At a practical level, cybersecurity maturity in OT now means asset visibility, segmentation aligned to zones and conduits, continuous monitoring with OT-aware tools, and incident response designed for safety-critical environments.

The distinction between IT and OT makes this shift unavoidable. If IT "speaks English," OT requires "French." In IT, a breach typically results in financial and reputational loss. In OT, the consequences extend further—into physical damage, environmental impact, service disruption, and risk to human life.

Yet, most organizations still underestimate their exposure—especially in the built environment. Any business operating connected physical systems—HVAC, elevators, access control, or building automation—already carries OT cyber risk. Based on research from Claroty, 75% of building management systems contain known exploitable vulnerabilities, 69% have exposure pathways linked to ransomware, and 51% are directly exposed to the internet without adequate security controls. In many cases, these systems are remotely accessed by third parties, integrated with corporate networks, and owned across fragmented teams. If you have a building, you have an OT environment—whether you realize it or not.

As industrial ecosystems become more interconnected, every partner becomes part of the operational risk surface. The organizations that can demonstrate cybersecurity maturity are moving faster, integrating seamlessly, and earning trust. Those that cannot are encountering friction, delays, or exclusion.

Cybersecurity maturity is no longer a future goal—it is an immediate requirement. Organizations need to understand their OT exposure now, before regulators, insurers, or partners force reactive change. In OT, trust is not negotiated—it is engineered. Digital trust is no longer a concept—it is infrastructure. And like any infrastructure, if you do not meet the standard, you do not get access.

Tristan Kim is a visionary cybersecurity leader and market builder, with over 15 years of experience at the forefront of digital and operational risk. As Head of Security Sales & Business Development at KORE Solutions, Tristan leads the growth of end-to-end cybersecurity strategies across IT and OT environments.
You can connect with Tristan Linkedin

Dmitry Raidman

Cybersecurity entrepreneur, CTO, Cybeats

Cybersecurity as a Supply Chain Requirement

Cybersecurity is no longer just a security team concern. It has become a core supply chain requirement. Yet many procurement processes still treat it as a paperwork exercise, where a vendor submits a SOC 2 Type II report or an ISO 27001 certificate and the conversation moves on. That approach is no longer enough.

These certifications still matter. They can tell you that a company has invested in controls, governance, and formal processes. But they do not automatically prove that the product you are buying is secure, resilient, or supported in a way that will protect your organization over time. In today's environment, trust cannot be based on a document alone. It must be built on evidence, transparency, and the ability to sustain security in practice.

This is where procurement needs to evolve. Zero trust should begin before a contract is signed. Organizations should examine not only what a vendor says about its controls, but how its products are built, what they contain, where they come from, and how the vendor plans to support them after deployment. Provenance, secure development discipline, and operational follow through should all be part of the review.

Software transparency is becoming one of the clearest signals of that discipline. SBOMs give buyers visibility into the components that make up a software product. VEX records help distinguish between theoretical exposure and real impact. Together, they provide a more honest picture of product risk. A vendor that can produce current SBOMs and VEX records is showing more than technical maturity. It is showing repeatability, accountability, and the ability to respond when new issues emerge.

This shift is also being reinforced by regulation. Across sectors and regions, requirements are moving toward greater supply chain visibility and stronger proof of ongoing security. Energy, healthcare, payments, financial services, and digital products sold into the European market are all seeing that direction more clearly. The message is consistent: security claims must be backed by evidence, and that evidence must remain relevant throughout the product life cycle.

At the same time, organizations should not assume that a compliance report alone tells the full story. Recent public scrutiny around questionable compliance audit documentation has exposed the weakness of a checkbox mindset. Buyers need to read reports carefully, confirm scope, review exceptions, and ask deeper questions. In some cases, asking for supporting evidence such as penetration testing results or software transparency artifacts is not excessive. It is responsible.

External security ratings and outside in assessments can also add useful context. If a vendor shows weak external discipline, it may raise valid questions about whether internal practices are consistently followed. These signals are not perfect, but they help teams move beyond trust by assertion.
The bigger point is this: vendor risk does not end at onboarding. Most digital products now depend heavily on open ***source***, and new vulnerabilities, malicious packages, and unsupported components appear constantly. The real measure of a vendor is not whether they passed an audit once. It is whether they can continuously monitor, communicate, and remediate risk over time.

Cybersecurity is no longer a one-time procurement check. It is an ongoing supply chain commitment.

Dmitry Raidman is a cybersecurity entrepreneur, investor, and technology leader with over 20 years of experience in application security, cloud architecture, DevOps, and cyber defense automation. He is the co-founder and CTO of Cybeats, where he leads product innovation in software supply chain security, including SBOM management and vulnerability lifecycle automation.
You can connect with Dmitry Linkedin

Cybersecurity as a Gatekeeper

Insurance as a Gatekeeper

70% of insurers now require evidence of cyber controls before issuing coverage.

61% of organizations report restrictions, delays, or denial in recent applications.

Source: March McLennan, 2025 Cyber Risk Survey

Without demonstrable maturity, organizations are increasingly uninsurable and therefore excluded from contracts that require coverage..

Canada's SME Coverage Gap

18% of Canadian small businesses carried cyber insurance in 2025.

Source: Insurance Bureau of Canada

Low adoption is creating a structural disadvantage, limiting participation in supply chains and larger commercial engagements.

Regulation as Infrastructure

Frameworks such as **CMMC** and **NIS2** now require validated cybersecurity readiness to access defense and critical infrastructure markets.

Source: U.S. Department of Defense, European Commission

Security is no longer a differentiator. It is a prerequisite for market entry.

Trust Filters in the Supply Chain

63% of organizations use cyber insurance as part of vendor risk scoring.

35% of European risk leaders recommend insurance as a vendor qualification requirement.

Source: SecurityScorecard, FERMA

Insurability is becoming a proxy for trust across partner ecosystems.

Sector Standards Are Shifting

Major institutions now require **$5M** cyber coverage from vendors, while manufacturers increasingly request proof of cyber maturity in procurement processes.

Source: Cornell University Procurement, CCN Sector Interviews

Organizations without documented cyber posture are being excluded early in the buying process.

Cyber maturity is now used to grant or deny access.

Across insurance, regulation, and supply chains, cybersecurity is no longer risk management.
It is a control point for revenue, participation, and growth.

"Who lets you in?"

All are now asking the same question:
Can you prove your cyber maturity?

What Leaders Are Missing and What Comes Next

As cybersecurity becomes a condition of access, not just a risk control, organizations are being exposed in ways they do not always see.

Strategic Blind Spots

- **Insurance denial is rising quietly.**
  Coverage is increasingly restricted or denied due to weak controls. Many organizations only discover this at renewal.
- **Vendor trust gaps are multiplying.**
  Suppliers are being screened out of RFPs for lacking cyber insurance or certification, particularly in regulated and cross border supply chains.
- **OT risk remains invisible.**
  Industrial environments often lag in maturity, creating exposure that leadership assumes is already covered.
- **Compliance is no longer enough.**
  Buyers and insurers are demanding proof of operational readiness, not alignment to frameworks.
- **Cyber posture is affecting capital.**
  Early signals show investors and funders incorporating cybersecurity into due diligence, impacting access to financing.

Signals for the Next 12–24 Months

- **AI risk will enter underwriting.**
  Insurers will begin pricing AI related exposure, including decision risk and model behavior.
- **Procurement requirements will tighten.**
  Cyber insurance and security validation will become standard across public and private sector contracts.
- **Investor scrutiny will increase.**
  Cyber maturity will become a factor in valuation and deal approval.
- **Regulation will expand its reach.**
  Frameworks such as CMMC and NIS2 will continue to shape eligibility across sectors.
- **Digital trust will become measurable.**
  Boards will be expected to track and report cyber and trust posture as part of governance.

CCN Signal

The next phase of cybersecurity is not about tools.
It is about permission.
Organizations that can demonstrate trust will move faster, win more, and remain insurable.
Others will not realize they have been excluded until the opportunity is gone.

Leadership Implications

"What leaders must do now to keep their companies insurable, connected, and competitive in a trust-gated economy."

1. Reframe Cybersecurity as Infrastructure
Treat cyber maturity like electricity or logistics, a foundational enabler of operations, access, and credibility.
Board directive: Embed cybersecurity into infrastructure, risk, and business continuity planning.

2. Require Proof, Not Promises
Don't settle for policies or intentions. Demand verifiable controls, tested readiness, and third-party assurance from both internal teams and vendors.
CEO move: Link insurance, contracts, and procurement access to measurable controls.

3. Interrogate the Trust Gaps in Your Supply Chain
Assume at least one vendor is uninsurable, unmonitored, or unable to recover.
Leadership action: Map critical suppliers and require evidence of cybersecurity, not just compliance.

4. Involve Legal and Insurance Before the Crisis
Pre-breach engagement with legal and cyber insurers now shapes response time, recovery cost, and reputational survival.
General counsel & CFO: Review and pre-negotiate breach response expectations and coverage limitations.

5. Make OT and Infrastructure Cyber Risks Board Visible
If your operations depend on physical systems, the board must see the digital attack surface too.
Board request: Quarterly visibility on OT system risks and external connection policies.

6. Align Executive Incentives to Cyber Maturity
Reward readiness. Penalize delay. Treat digital trust as a performance metric.
CEO directive: Tie executive KPIs to specific risk-reduction milestones or posture scores.

7. Know What Disqualifies You
Understand what would prevent your organization from securing insurance, entering a contract, or recovering from breach, before it's tested.

Leadership question: "What would block us from getting insured, onboarded, or trusted today?"

Final Takeaways

The signal is clear: cybersecurity has outgrown its roots as a technical safeguard. It now underpins access, determines trust, and shapes the economic pathways of companies across Canada and beyond. As insurers, regulators, enterprise buyers, and capital providers embed cyber maturity into their decision making, organizations must adjust, or risk exclusion from the markets that matter most.

This is no longer a conversation about vulnerabilities. It is a strategic shift in who gets to operate, grow, and compete.

To close this CCN Insights brief, we offer the following distilled takeaways to guide boardrooms, executive teams, and policymakers in the months ahead:

- Cybersecurity is no longer technical hygiene, it's business infrastructure.
  It now determines access to insurance, capital, contracts, and supply chains.

- Digital trust is being scored, measured, and required, often quietly.
  Organizations are being excluded without realizing it, not for failing, but for falling short.

- Proof of maturity is the new baseline.
  AI adoption and leadership accountability are now part of that proof.

- Boards and CEOs must move beyond checklists to demonstrate operational readiness.
  Those who invest in trust gain speed, resilience, and market access.

- Cyber maturity is now a growth enabler, not just a defensive cost.
  The gatekeepers have changed.
  Insurers, regulators, buyers, and investors are now deciding who gets to compete.

Cybersecurity is the New Infrastructure

A CCN Insights Brief from the Canadian Cybersecurity Network.