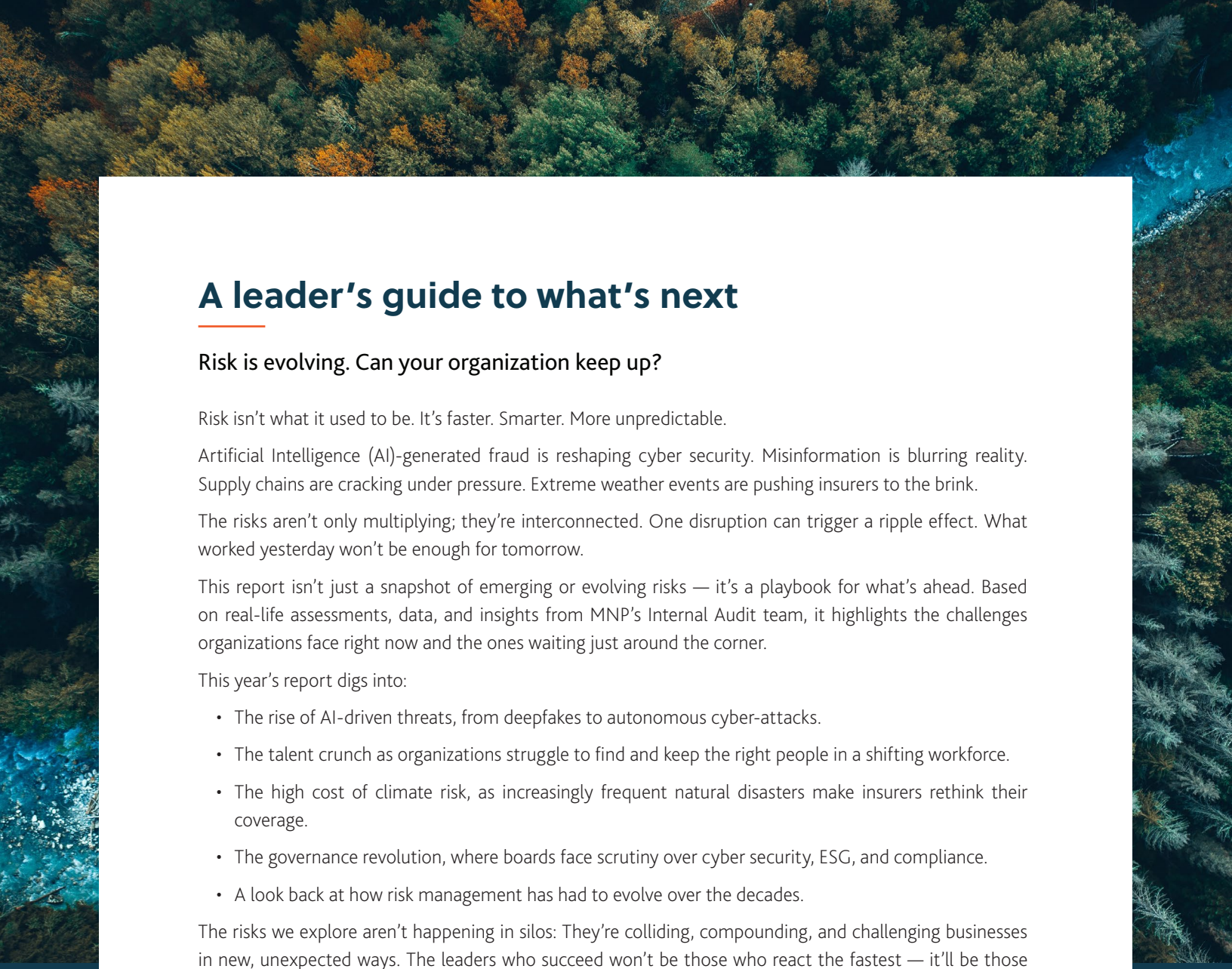
MNP Risk Trends: 2026 and Beyond

Risk intelligence in a world of unprecedented uncertainty and change

MNP.ca

Table of Contents



A leader's guide to what's next

Risk is evolving. Can your organization keep up?

Risk isn't what it used to be. It's faster. Smarter. More unpredictable.

Artificial Intelligence (AI)-generated fraud is reshaping cyber security. Misinformation is blurring reality. Supply chains are cracking under pressure. Extreme weather events are pushing insurers to the brink.

The risks aren't only multiplying; they're interconnected. One disruption can trigger a ripple effect. What worked yesterday won't be enough for tomorrow.

This report isn't just a snapshot of emerging or evolving risks — it's a playbook for what's ahead. Based on real-life assessments, data, and insights from MNP's Internal Audit team, it highlights the challenges organizations face right now and the ones waiting just around the corner.

This year's report digs into:

- The rise of AI-driven threats, from deepfakes to autonomous cyber-attacks.
- The talent crunch as organizations struggle to find and keep the right people in a shifting workforce.
- The high cost of climate risk, as increasingly frequent natural disasters make insurers rethink their coverage.
- The governance revolution, where boards face scrutiny over cyber security, ESG, and compliance.
- A look back at how risk management has had to evolve over the decades.

The risks we explore aren't happening in silos: They're colliding, compounding, and challenging businesses in new, unexpected ways. The leaders who succeed won't be those who react the fastest — it'll be those who are best prepared.

At MNP, we work alongside Canadian organizations and governments, helping them to stay ahead of emerging risks while turning uncertainty into opportunity.

This report isn't about fear, it's about foresight.

Let's take a look.

MNP Internal Audit Services Team

Relentless uncertainty:
Why risk management must evolve

Uncertainty isn't a passing storm — it's the reality we now live in.

Canada's risk landscape has completely transformed over the past few decades. In response, it demands a shift in how organizations approach risk management. From a shaky economy, tariffs, and geopolitical tensions to cyberthreats and climate disasters, the challenges Canadian businesses are now facing are not only relentless, but ruthless.

Enterprise Risk Management (ERM) gained traction in the early 2000s as businesses integrated digital technologies into operations and corporate scandals seemed to be hitting the headlines regularly. The 2010s saw an explosion of interconnected systems that muddied the risk landscape and ushered in the need for a more dynamic approach: think smartphones, Internet of Things (IoT), and cloud computing.

And along came the 2020s

The 2020s brought seismic shifts. The COVID-19 pandemic forced organizations to accelerate digital transformations, manage supply chain disruptions, and manage a remote workforce. Again, risk became more complex and, suddenly, uncertainty was the rule, not the exception.

The forces impacting risk management continue to shift and expand. Artificial intelligence (AI) is reshaping how business is done in nearly every industry. Amid generational shifts in inflation, trade disruptions, and shifts in global markets, it seems more and more like the pandemic-driven economic instability was just the opening salvo.

Climate change is driving natural disasters at an increased rate with Canada experiencing its 10 worst disasters on record in the last decade, according to the Insurance Bureau of Canada. These events have resulted in $30 billion in cumulative insured losses in the last 10 years (up from the previous decade's annual average of $2.2 billion).

Meanwhile, social and economic pressures are intensifying. A 2024 report from Food Banks Canada found that one in four Canadians now lives below the poverty line, which is more than double the official estimate from Statistics Canada. The housing crisis, driven by population growth and increasing rent prices, is adding even more pressure.

At the same time, businesses are facing a growing wave of cyber security threats, with 65 percent of Canadian business leaders saying cyber risks are a top concern, according to Travelers Canada Risk Index. Nearly one in three organizations have already experienced a cyberattack. Medium-sized businesses have found themselves particularly vulnerable compared to their smaller counterparts.

Scenario planning has become essential

Clearly, there are troubled waters ahead. But they are still navigable, provided your organization commits to abandoning reactive approaches in favour of continuous scenario planning and agile risk management. This agility becomes especially important as we experience the compounding effects of risk — like tariffs challenging the economic viability of a company at the same time that a cyberattack takes down their systems. The ability to anticipate, adapt, and respond to rapid change in an integrated manner is no longer only a competitive advantage — it's how your business will survive. Thinking through the "what ifs" to anticipate how risk scenarios could play out will allow companies to become nimbler in responding to risks.

Escalating risks your company needs to watch for

Economic downturn: Concerns about a potential recession persist, with factors such as U.S.-imposed tariffs, trade disruption, and global economic uncertainties contribute to a cautious business environment.

Labour shortages: An aging workforce and shifting employee expectations make talent recruitment and retention a challenge.

Cyber security threats: The increasing frequency and sophistication of cyberattacks or deepfakes require robust cyber security measures to protect sensitive data and maintain business continuity.

Inflation: The long-term impacts of inflation continue to impact both operational costs, consumer purchasing power, and global competitiveness.

Supply chain disruptions: Ongoing global supply chain challenges, made worse by factors like U.S. imposed tariffs, geopolitical tensions, and climate change pose risks to inventory management and production timelines.

Regulatory changes: New rules around factors like ESG, AI, trade conflicts, and data security could demand adaptation to new and more stringent standards.

Geopolitical uncertainty: Global political developments disrupt markets and impact business operations.

Technological disruption: Tech advancements need continuous adaptation to stay competitive in a digital economy.

Environmental risks: Businesses need to implement sustainable practices and prepare for potential regulatory and market shifts.

Reputational risks: Maintaining a positive corporate reputation is essential, as mishaps could potentially lead to significant financial and operational consequences.

Warning Signs

- Material changes in markets that are unprecedented and unpredictable
- Foreign governments losing confidence and unable to implement fiscal policy
- Unusual spikes in cyber activity (i.e., phishing and ransomware)
- Extreme trade tariffs and continuous changes that amplify global uncertainty

AI unleashed:
The explosive growth and hidden risks

AI is no longer a futuristic concept — it's here, moving faster than regulations can keep up

Ready or not, AI is here: It's reshaping industries, transforming decision making, and embedding itself into our daily lives, often without us even knowing. It's been a fast evolution, one that comes with unprecedented risks.

By 2026, AI will generate new use cases by the minute, influencing everything from mortgage approvals to university admissions, insurance payouts, and hiring decisions. Yet, while AI promises to help you streamline processes and improve efficiency, its impact gives way to concerns.

Already, fraudsters are leveraging AI to launch sophisticated cyberattacks, deepfake scams, and ransomware campaigns. Overreliance on AI-enabled decision-making raises concerns about transparency, security, and ethical responsibility. Biases within these systems are already well established. Given that many of these biases originate in how AI models are trained, they are not always easy to spot or correct once the issue is identified.

> Overreliance on AI-enabled decision-making raises concerns about transparency, security, and ethical responsibility.

How do Canadians feel about it?

Canadian businesses, workers, and policymakers are engaging AI with optimism and caution. Consider the following:

- A survey by the Peninsula Group found that only 10 percent of small and medium-sized businesses regularly use generative AI platforms like ChatGPT or Gemini. Barriers include data privacy issues, response quality, and legal exposure.
- 51 percent of Canadians worry about AI's potential to spread misinformation and deepfake content, according to a poll by the Canadian Internet Registration Authority.
- In November 2024, Canada launched the Canadian Artificial Intelligence Safety Institute (CAISI) with a $50 million budget to address AI risks and advocate for responsible development.

Risks to watch

Bias and discrimination: AI systems can perpetuate biases, leading to unfair treatment in decision-making, such as hiring, lending, and insurance.

Privacy violations: AI-powered tools can collect and analyze vast amounts of individual and corporate data, raising serious privacy concerns.

Cyber security threats: Deepfake scams and AI-driven malware are already being used by cybercriminals to threaten businesses and individuals.

Job displacement: While AI creates efficiencies, it also automates roles, which can lead to workforce disruptions, skill gaps, and potential societal inequity.

Lack of understanding: Many AI models are complex and even developers have said they don't fully understand how or why they work. Users should, therefore, remain skeptical about how decisions are made and how much to trust AI.

AI weaponization: Autonomous AI-driven weapons and cyberwarfare tools pose global security threats due to risks of misuse or accidental escalation.

Regulatory uncertainty: Inconsistent or changing AI regulations may create challenges for businesses, leading to compliance risks or stifled innovation. Governments may struggle to stay ahead of the innovation and use of AI, and therefore any regulation enforced could be outdated before it is even approved.

Over-reliance on AI: Allowing AI to make important decisions without human oversight can lead to major failures if the system malfunctions or provides an inaccurate output. If human safety could be impacted, it could have dire consequences.

Intellectual property issues: Questions about the ownership of AI-generated content or innovations, as well as the use of copyrighted data in AI training, may result in legal or ethical challenges.

Ethical concerns and public backlash: If your organization misuses AI for unethical reasons — like mass surveillance, deepfake misinformation, or AI-driven disinformation — it could lead to reputation harm and public opposition to AI platforms.

Warning signs

- Unexplained bias in hiring, pricing, or lending models
- Cyber incidents tied to AI, like phishing attempts, deepfake scams, or security breaches
- Operational disruptions due to a failure in an AI platform that leads to financial or reputational damage
- Allegations of privacy breaches as employees inadvertently or maliciously share private and confidential information

Mitigation strategies

- Improve cyber resilience
- Establish risk management and governance policies for AI usage
- Develop ransomware response protocols, training, and recovery solutions
- Strengthen board oversight
- Conduct regular cyber security and operational risk assessments of external vendors
- Improve workforce training
- Continually test AI models and validate their output
- Develop AI monitoring and compliance protocols

Questions to consider:

- Do your third-party contracts specifically state what AI use is acceptable and what is not?
- What public disclosure of AI use should be made to maintain public trust?
- What are the most relevant risk scenarios that could occur when using AI?
- Are you already using AI for high-risk decisions? Should you modify or stop this use?
- How do you know the output from AI is accurate or even reasonable?

Cyber security 2.0: Managing the high-stakes risks of the digital future

Keep pace or risk being left defenseless

Here's the thing about cyberthreats: You're never more vulnerable than when you think you've finally figured it out. Cyber security is a perennial talking point — but peace of mind is a moving target. What seemed secure yesterday could be compromised today. Today's best practices will be woefully inadequate to address the AI-driven threats that are just around the corner.

The reality is cybercriminals are no longer just targeting data, they are targeting trust.

Imagine logging on to a virtual meeting, only to realize later the person you spoke to wasn't real. Instead, it was a deepfake impersonation. With AI-driven fraud on the rise, Canadians now must ask themselves an unsettling question: How do you know who, or what, to trust?

From ransomware attacks that hold your business hostage to phishing emails that bypass traditional security systems, digital threats are smarter than ever. We are entering a new era — cyber security 2.0 — a world where continuous vigilance, proactive defenses, and advanced threat detection are more critical than ever.

Alarming trends in cyberthreats

The numbers tell a concerning story:

- Communications Security Establishment Canada (CSEC) warns that China's cyber program is the most sophisticated and active state-sponsored threat to Canada, targeting businesses, government institutions, and essential infrastructure.
- Canadian households lost more than $500 million to cyber fraud in a single year — yet law enforcement estimates that only 10 percent of cybercrimes were reported, according to a report from the Auditor General of Canada.
- Cyber-attacks are decreasing in numbers but increasing in success rates, says a study from CDW Canada. Cyber security is a key priority for 43 percent of businesses, which dedicate between five to 15 percent of their IT budgets to their defenses.
- The same study found that 82 percent of businesses now have cyber insurance, up from 59 percent in 2021.
- The 2024 federal budget allocated $917.4 million over five years to strengthen intelligence and cyber operations and implement a Canadian Armed Forces Cyber Command to fight growing cyberthreats.

Risks to watch

Ransomware evolution: Fraudsters use advanced encryption and extortion techniques to target critical infrastructure and demand higher ransoms.

Supply chain attacks: Cybercriminals infiltrate organizations through third-party vendors or suppliers to exploit weaknesses in interconnected systems.

AI-powered cybercrime: Hackers use AI to automate attacks, create deepfakes, and develop sophisticated phishing campaigns that are harder to detect.

IoT vulnerabilities: As IoT devices become more commonplace, their lack of standard security protocols makes them attractive targets for attackers looking for weak entry points.

Insider threats: Both malicious and unintentional insider actions remain a big concern, amplified by remote work environments and inadequate monitoring.

Cloud security risks: Misconfigured cloud environments and multi-cloud complexity can lead to data leaks and unauthorized access.

Critical infrastructure attacks: Cyberattacks on energy grids, healthcare systems, and financial institutions can potentially cause widespread disruption.

Zero-day exploits: Hackers target unpatched vulnerabilities in widely used software before software providers can address the fixes.

Data privacy breaches: Stealing sensitive personal and corporate data for resale or extortion remains one of the most prevalent and damaging risks.

Quantum computing threats: Emerging advancements in quantum computing could one day render traditional encryption useless.

Warning signs

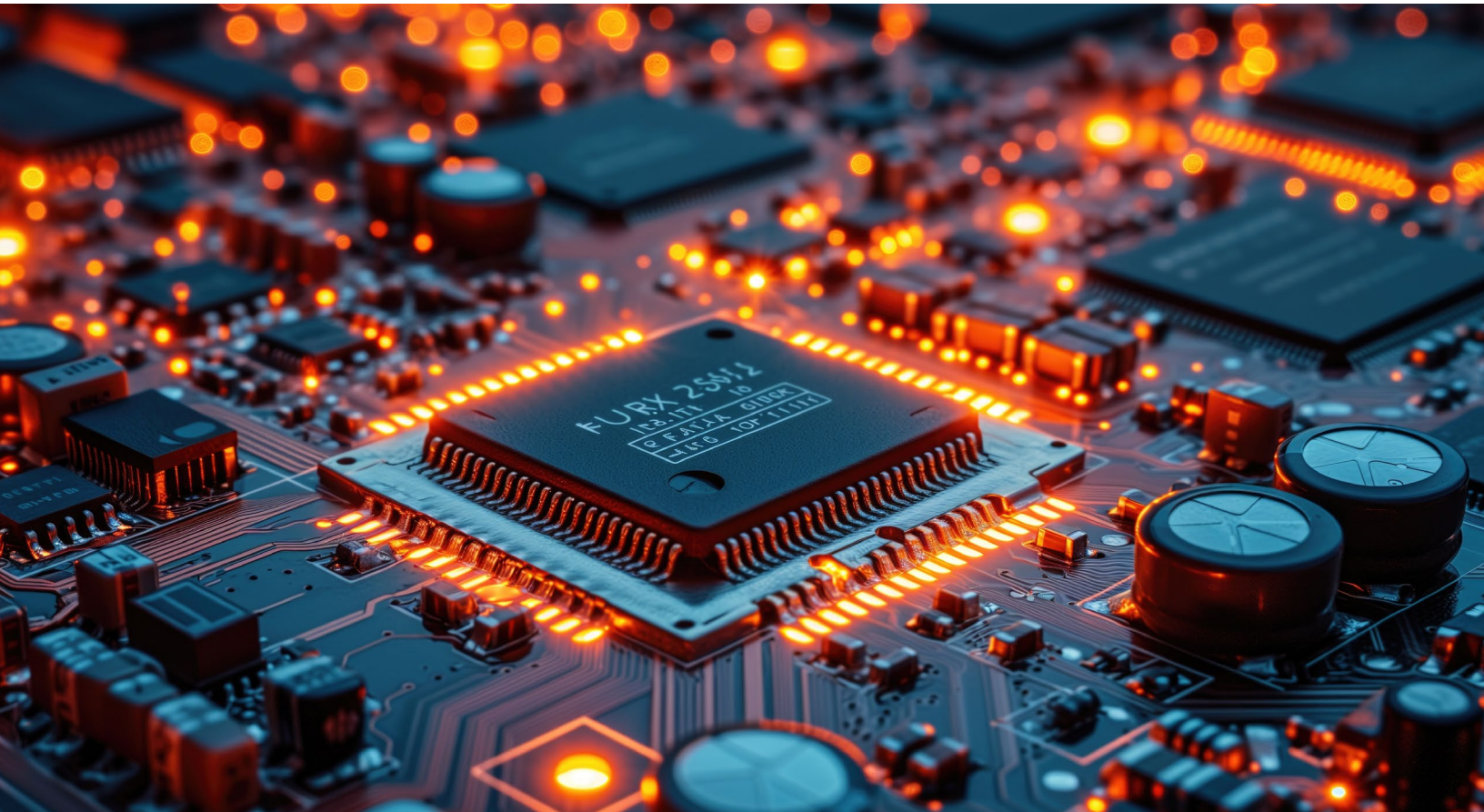
- An increase in phishing attempts, particularly those using AI-generated content
- Unusual logins or access requests from unexpected locations
- Reports of insider leaks or suspicious employee activity
- Increased ransomware demands with threats of public data exposure
- New vulnerabilities in widely used software with delayed patches

Mitigation strategies:

- Zero trust security
- Advanced threat detection
- Mandatory multi-factor authentication (MFA)
- Investing in employee training
- Regular patching and system updates
- Third-party risk management
- Cyber incident response plan
- Encryption and backups
- Quantum-resistant encryption

Questions to consider:

- Does your organization consider the level of confidentiality of every planned meeting? Do you apply enhanced security controls to high-risk meetings, like verifying attendees before a virtual call?
- Are your employees required to report any incidents (work or personal) to IT security if their identity or personal information may have been fraudulently compromised?
- How often does your IT security team brainstorm on the newest cyber-crime scenarios? How will they improve controls to mitigate innovative techniques?
- Do you communicate openly with your industry peers to share intel on new cyber-crime techniques to give you lead time in developing effective controls?



ESG risk:
Conquering the future of sustainability and uncertainty

More than a compliance issue, it's a fundamental business challenge

By 2026, it's anticipated that your business will face more scrutiny over sustainability efforts, social impact, and governance transparency than ever before.

While ESG strategies were initially seen as a pathway to corporate responsibility and long-term resilience, the reality is, it's much more complex.

ESG investments don't always align with shareholder returns, which can lead boards to feel frustrated with policy hurdles (like Bill C-59), shifting regulations, and rising costs. The net-zero transition — a goalpost for many organizations in recent years — has largely slowed due to tighter budgets, complex rules, and compliance hoops. Inconsistent global action has added to the frustration, particularly from high-emitting nations that hinder progress.

Both a risk and an opportunity

In 2024 alone, more than 3.4 million hectares of land were scorched by wildfires, with the Jasper wildfire causing nearly $880 million in insured damages. Events like this are not just environmental disasters, they're also financial ones.

And many of Canada's largest companies are still playing catch-up. A review of more than 250 corporate sustainability reports found that most companies are not financially quantifying their climate risks or fully embedding ESG into their strategies.

The question is: Is the risk that companies aren't Bill C-59 compliant, or is the opportunity to rewrite Bill C-59?

The social side of things

The social component of ESG is a business imperative. Organizations face increasing scrutiny over how they engage with people, communities, and society's expectations.

Indigenous rights and reconciliation remain a significant focus in Canada. Businesses operating on or near Indigenous lands need to navigate risks related to land use, cultural preservation, and trust. Beyond compliance, consultation and partnership with Indigenous communities are a baseline expectation, not just from regulators but also from the public.

At the same time, Diversity, Equity, and Inclusion (DEI) efforts are at a crossroads. With the U.S. pulling back from formal DEI commitments, it leaves Canadian organizations with questions about the future of DEI looks like.

That being said, DEI remains a core expectation for businesses, especially among younger workers and customers who want to see authentic progress. Failing to uphold these values can erode your reputation, trust, and limit your access to talent.

Governance is a growing target

As ESG reporting requirements tighten up, the risks of weak governance grow.

Organizations are under pressure to deliver consistent and transparent ESG reporting. Falling short of this, like through omission, misalignment, or greenwashing, can result in regulatory penalties and/or reputational damage.

Meanwhile, boards need to be held more accountable than ever. A lack of ESG oversight or meaningful engagement is inexcusable. Boards need to not only understand emerging risks, but they also need to be actively involved in how those risks are managed.

Additionally, the risk or regulatory and legal liability is on the rise. Whether it's failing to meet climate targets or deliver on diversity metrics, organizations are being held to account. Strong governance structures, with clear accountability, a detailed strategy, and an engaged board, are needed to mitigate operational challenges and financial exposure.

Canadian CEOs seem to be taking ESG more seriously than their global peers, with 29 percent ranking it as a top priority, according to one survey. That being said, the lack of readiness for mandatory ESG disclosures could expose businesses to regulatory, reputational, and operational risks.

Despite these warning signs, there's still a lot of optimism. ESG initiatives have already started driving positive change in Canada, from innovation to sustainability gains. But for these efforts to deliver long-term value, businesses must treat ESG as both an opportunity and a risk. That means building better awareness, improving reporting, and taking proactive steps to align strategy with action.

Risks to watch

Environmental risks

Climate change impacts: Increased frequency of extreme weather events (like wildfires, floods, and heat waves) disrupt operations and supply chains, especially in resource-intensive sectors.

Carbon transition risk: More stringent emissions regulations and carbon pricing could increase operational costs for companies that fail to decarbonize.

Biodiversity loss and resource scarcity: Diminishing natural resources and biodiversity loss create long-term risks for industries that rely on land, water, and energy.

Greenwashing allegations: Companies overstating or misrepresenting ESG efforts face reputational damage, regulatory penalties, and consumer backlash.

Social risks

Indigenous rights and reconciliation: Businesses operating on or near Indigenous lands face risks related to land disputes and community relations, along with growing public and legal scrutiny.

Diversity, equity, and inclusion (DEI): Weak DEI strategies and failing to deliver on those commitments could lead to employee turnover, difficulty attracting talent, and reputational harm.

Labour relations and workforce well-being: Failing to address fair wages, mental health, and working conditions could be a challenge for employers, especially in high-turnover industries.

Governance risks

ESG reporting and compliance: Inaccurate or inconsistent ESG disclosures can result in penalties under evolving national and global reporting standards.

Board accountability: Weak governance practices around ESG priorities, like a lack of board oversight or stakeholder engagement, can lead to shareholder activism or reputational harm.

Regulatory and legal liability: Rising lawsuits and regulatory scrutiny for failing to meet ESG commitments could increase operational risks and financial exposure.

Warning signs

- Regulatory changes that require expanded ESG disclosures and stricter compliance standards
- Stakeholder activism and pressure from investors or advocacy groups on sustainability and social issues
- Legal challenges or lawsuits over unfulfilled ESG commitments, particularly in carbon reduction and DEI
- Boycotts, negative press, or reduced brand loyalty due to perceived ESG failures

Mitigation strategies

- Develop a climate adaption plan
- Strengthen ESG reporting
- Engage with Indigenous communities
- Audit supply chains
- Improve board oversight
- Invest in green innovation
- Prepare for crisis management
- Proactively engage stakeholders
- Monitor legal and regulatory risks

Questions to consider:

- Has your organization established what it is able to publicly disclose to align with Bill C-59 and which disclosures need further verification?
- Since your organization has created formal ESG targets, what have been the greatest risks? What have you changed to mitigate these risks?
- How does your organization rank on relevant ESG-related measures? Do your greatest strengths or weaknesses have the potential to be a competitive advantage or disadvantage?
- How prepared are you to continuously address new ESG-related government regulations and policies? Is monitoring these requirements given to someone as a formal responsibility?

Digital disruption:
The frontier of transformation and technology

Digital transformation isn't slowing down — it's accelerating

As we move into 2026, innovation is no longer waiting for you. And the businesses that move quickly to adopt new technology and services will lead the pack.

But with rapid innovation comes risk. Many emerging digital and AI investments will fail. There will be integration challenges, cyber security threats, employee skill gaps, or regulatory uncertainty. And all the while, the expectations for digital solutions and convenience will continue to rise, forcing your company to rethink how you deliver services.

Canada's digital economy reflects this shift. In 2023, the digital transformation market generated US$84.8 billion, and projections show it'll reach about $492 billion by 2030, as per Grand View Research. That's a staggering 30 percent compound annual growth rate.

This growth signifies that your business must move quickly to innovate, but you must do it strategically and securely.

> There will be integration challenges, cyber security threats, employee skill gaps, or regulatory uncertainty.

The new digital reality

Technology is reshaping how we work, bank, and interact with the world:

- **The digital-first workforce:** The expectation for technology proficiency will become standard, redefining job roles and skill requirements.
- **Fintech companies as established competitors:** Organizations like Neo Financial and EQ Bank are reshaping how Canadians save, spend, and manage their money.
- **Smartphone as digital keys:** By 2026, 87 percent of Canadians expect fully digital public services, says Nortal. This ranges from identity verification and travel to paying bills and accessing secure spaces.
- **AI and automation in the workplace:** Expense reports, scheduling, and data entry will be handled by AI-enabled assistants, freeing employees for higher-value work.

Risks to watch

Resistance to change: Employees and stakeholders may resist new technologies, slowing adoption and productivity.

Integration challenges: Merging new tools with legacy systems can result in delays, compatibility issues, unexpected costs, and operational downtime.

Skill gaps: A lack of technical know-how can lead to poor implementation and a reliance on external advisors.

Unrealistic expectations: Overestimating the immediate benefits of digital transformation can result in budget overruns, failed projects, and disappointment.

Data security and privacy risks: Increased reliance on digital tools and cloud services can expose businesses to cyber security threats, data breaches, and regulatory penalties for non-compliance with data protection laws.

Vendor dependence: Relying too heavily on a single technology provider can create lock-in risks, which limit flexibility and negotiation power.

Regulatory and compliance risks: Businesses failing to meet industry-specific regulations during digital transformation could lead to legal and financial consequences.

Technology obsolescence: A cutting-edge system today could be outdated within a couple of years. You must plan for ongoing updates.

Failure to align with business goals: Digital adoption without a clear business purpose can waste resources and fail to deliver value.

Disruptions to operations: Poorly managed transitions can lead to service interruptions, customer dissatisfaction, and financial losses.

Warning signs

- Delayed implementation timelines and frequent project roadblocks
- Pushback from employees or key stakeholders resisting the technology changes
- Unexpected cyber security breaches due to newly adopted platforms
- Limited options for alternative providers leading to significant vendor dependence
- Regulatory scrutiny or penalties related to digital transformation initiatives
- Digital governance is cumbersome and challenges innovation

Mitigation strategies

- Disciplined change management
- Robust cyber security
- Smart integration planning
- Continuous upskilling and employee training
- Realistic planning and goal setting
- Develop and maintain technology roadmap
- Vendor dependence risk mitigation
- Business continuity planning
- Align digital transformation with business strategy
- Regulatory compliance readiness

Questions to consider:

- How are you enabling innovation and have you removed roadblocks while ensuring value for money from the digital investments you are making?
- How aggressive are your digital transformation plans (in scope, budget, and timeline)? Does your organization, or supporting third parties, have experience doing something of similar size, budget, and scope?
- How will this new digital technology impact the way you do business? Will you need a completely different organizational structure and job descriptions? Do you have the right resources and governance model to deliver value in this new world?
- How much risk will resistance to change (from employees, third parties, or customers) create in relation to this digital transformation?
- How will the digital transformation impact your cyber risk exposure? Are you prepared to manage this?

Future fraud innovation:
Opportunity arriving every second

As digital transformation evolves, so does fraud

Digital transformation moves quickly, but fraudsters move even faster. And the sophistication is only growing. By next year, identity verification, financial transactions, and business operations will be smoother than ever. Imagine boarding a plane without requiring a physical passport — retina scans, digital IDs, and biometric authentication will handle verification in the background.

But with every leap forward in convenience, fraudsters find new ways to exploit emerging technologies. What if contact lenses could mimic someone else's retinas? What if digital ID implants could be copied and used for impersonation? These scenarios may seem far-fetched. But identity fraud, deepfake deception, and synthetic identity schemes are already happening today, and they're only going to get more advanced.

According to Equifax, in the second quarter of 2024, 48.3 percent of all flagged fraudulent credit applications were linked to identity fraud, up from 42.9 percent the previous year. Synthetic identity fraud alone tripled in a year. Meanwhile, Statista found that Canadians lost $123 million to fraud in just the first quarter of 2024, with total losses in 2023 reaching $554 million.

And it's not just individuals who are at risk: A Payments Canada study reported that one in five Canadian businesses experienced payment fraud in the past six months, with large enterprises (26 percent) hit harder than small businesses (16 percent). The most common fraud types were impersonation scams (25 percent), intercepted e-transfers (22 percent), and credit card fraud (20 percent).

Fraud is evolving faster than most defenses. To stay ahead, your business must embrace AI-powered detection, continuous fraud monitoring, and robust security controls — because fraudsters are already doing the same.

The rise of AI-driven fraud

Fraud is no longer about stealing credit card numbers. It's about manipulating trust. AI and deepfake technology have ushered in a new era where criminals can:

- Clone voices and appearances to impersonate executives and approve fraudulent transactions
- Use AI-generated phishing emails and fake invoices to deceive employees
- Use synthetic identities — fake personas built from real and stolen data — to open accounts, take out loans, and commit large-scale fraud
- Create fake online stores, investment platforms, and charity scams to steal money and personal data

Risks to watch

Phishing and social engineering: Increasingly sophisticated phishing emails, text messages, and social engineering trick employees and consumers into revealing sensitive data or making unauthorized transactions.

Business email compromise: Fraudsters impersonate executives or vendors to approve fraudulent payments.

Cyber fraud and ransomware: Criminals encrypt data and demand ransom, often targeting small and medium-sized businesses with fewer resources for cyber security.

Identity theft and synthetic identities: Fraudsters combine real and fake information to create synthetic identities, which are used to commit financial fraud, open fraudulent accounts, or access government benefits.

E-commerce and payment scams: Card-not-present fraud, fake online stores, and chargeback scams continue to rise.

Investment scams: Fake high-return investment opportunities, like cryptocurrencies, real estate, and high-yield schemes, mislead victims, especially when the economy is volatile.

Insider fraud: Employees or contractors exploit their access to internal systems or sensitive data for personal gain, often unnoticed until significant losses occur.

Tax and benefit fraud: Fraud related to tax filings and government benefits, like employment insurance and pandemic-related relief programs, remains a concern.

Charity and donation scams: Scammers pretend to be legitimate charities or create fake ones to exploit public generosity, especially during disasters or crises.

Counterfeit goods and intellectual property theft: The distribution of counterfeit products and the unauthorized use of trademarks or copyrights harms businesses and misleads consumers.

Warning signs

- Unusual email requests for urgent payments
- Unexpected spikes in chargebacks, disputed transactions, or customer complaints
- Sudden system shutdowns, ransomware messages, or unauthorized access attempts
- Employees accessing sensitive data outside of the scope of their role
- Reports of fraudulent accounts linked to personal or business information

Mitigation strategies

- Employee training
- AI and machine-learning fraud detection
- Multi-factor authentication
- Secure payment systems
- Vendor verification
- Advanced cyber security
- Data protection through encryption and access controls
- Conduct regular fraud risk assessments and monitor financial activity
- Public awareness campaigns
- Collaborate with law enforcement, industry groups, and regulators

Questions to consider

- Has your code of conduct training and related policies been updated to reflect the current ways technology is being used to commit fraud?
- Are your anti-fraud controls effective at preventing and detecting modern fraud techniques?
- When was the last time your organization conducted a fraud risk assessment?
- Do you have a conflict-of-interest policy that identifies which conflicts of interest are and are not acceptable?

Supply chain 2.0: Navigating the stakes of a hyper-connected future

What risks impact supply chains? More like, what doesn't?

Modern supply chains are complex, deeply interconnected webs where every strand depends on the others.

Whether it's sourcing raw materials, manufacturing, or distribution, risks like digital transformation, geopolitical shifts, labour disputes, and environmental pressures are redefining how goods move across borders. Add in the growing push for sustainable and ethical supply chains, and it's a recipe for unprecedented complexity.

The COVID-19 pandemic in 2020 was an early warning — we learned that supply chains can collapse overnight. Labour, manufacturing, and shipping disruptions triggered shortages across industries, exposing vulnerabilities in single-source suppliers, just-in-time inventory models, and outdated logistics systems.

> The COVID-19 pandemic in 2020 was an early warning — we learned that supply chains can collapse overnight.

Fast forward to 2025, and supply chains are facing fresh challenges. President Trump's unprecedented move to threaten significant tariffs on historic allies significantly changes the landscape for Canadian businesses. It's clear that unquestioned reliance on affordable cross-border trade is no longer a given — and that will pose serious challenges for a domestic economy that has optimized for such a system over the last 30 or more years. Regardless of the ultimate size and duration of tariffs, the ripple effects are certain to be significant and far reaching.

Canada's rail labour disputes in 2024 further reminded us just how fragile supply chains still are. A lockout of more than 9,000 workers at Canadian National Railway and Canadian Pacific Kansas City threatened hundreds of millions of dollars in daily trade, hitting grain exports, chemical manufacturing, and cargo transportation hard. The fertilizer industry alone lost an estimated $55 million to $63 million each day, as per Fertilizer Canada, due to halted rail services, putting Canada's global agricultural trade at risk.

The future of supply chains will belong to those who can evolve, digitize, and prepare for the unexpected.

The reality of the modern supply chain

Supply chain resilience is no longer only about efficiency. It's now about agility, technology, and risk management.

Digital transformation is changing logistics. Leading logistics and retail companies, like UPS and Walmart, leverage data-driven inventory and logistics systems to outmaneuver disruptions. But not all businesses can keep up, which could force smaller businesses out of the market.

Regulatory and ethical pressures are growing. Canada's Supply Chain Act (2024) now requires annual reporting on forced and child labour prevention — a step toward transparency but a challenge for businesses struggling with supplier oversight.

Global governance risks are increasing. Canada's import trading partners are looking at growing governance challenges, making due diligence more important than ever for avoiding unethical suppliers and ensuring regulatory compliance.

Risks to watch

Extreme weather events: Wildfires, floods, and storms are disrupting production facilities and transport infrastructure.

Geopolitical instability: Global geopolitical tensions, like tariffs, trade disputes, and conflicts, affect the availability and cost of raw materials and goods, influencing supply chains.

Labour disruptions: Strikes and labour disputes can lead to interruptions in the movement of goods across the country.

Transportation infrastructure challenges: Congested ports, outdated railways, and highway bottlenecks are increasing shipping delays and costs.

Cyber security threats: Supply chains face more risks of cyber-attacks, like ransomware and data breaches, targeting critical infrastructure and digital systems.

Technological disruptions: Technological advancements and digital transformations introduced complexities and integration challenges within supply chain operations.

Supplier insolvency: Economic uncertainties can lead to financial instability among suppliers, resulting in disruptions due to insolvency or reduced production capabilities.

Commodity shortages: Higher input costs and environmental challenges are making key materials harder to source.

Regulatory changes: Companies now face higher reporting requirements on carbon emissions, ethical labour, and environmental impact.

Pandemic-related disruptions: Lingering impacts of the COVID-19 pandemic continue to affect labour availability and global trade dynamics.

Warning signs

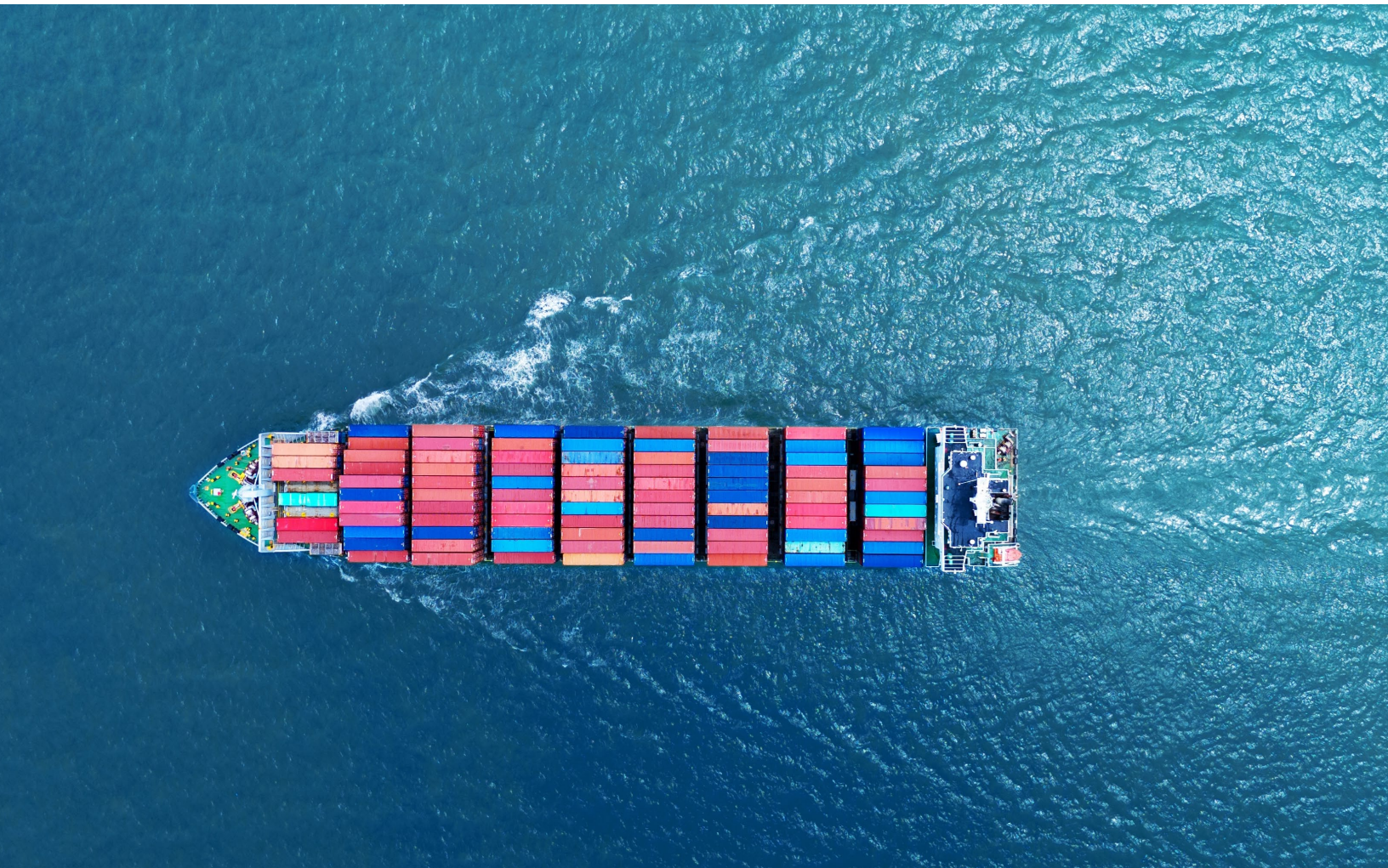
- Increasing lead times or frequent supplier delays
- Sudden spikes in costs due to material shortages or tariffs
- Cyber security breaches or ransomware attacks targeting logistics systems
- Labour disputes, protests, or contract breakdowns in essential industries
- Reports of forced or child labour linked to international suppliers
- Declining infrastructure reliability — like port congestion, rail disruptions, or outdated roads

Mitigation strategies

- Diversify suppliers
- Invest in analytics and digital tools to identify issues and optimize resources
- Strengthening cyber security
- Scenario planning and contingency strategies
- Monitor regulatory landscape
- Build stronger relationships and collaborate with vendors and partners

Questions to consider

- What threats to global trade may impact your business? Are you running risk scenarios to determine how best to be prepared to mitigate risk?
- How well do you know your suppliers and the risks within their business that may directly or indirectly impact you?
- Have you asked your most relied-upon third-party suppliers how they can be prepared to help mitigate risk if and when needed?
- How reliant are your supply chains on digital systems with third-party integrations? Do these third parties have sufficient cyber security controls?
- Is your supply chain agile enough to adapt to unforeseen risks and disruption?



Data value:
Governance and privacy in the digital age

Data is one of the most valuable assets — and one of the most vulnerable

Amid this era of unprecedented digital transformation comes stricter data privacy regulations, rising cyberthreats, and a growing public demand for transparency. As AI, IoT, and blockchain generate massive amounts of data, the challenge isn't just collecting and storing the information — it's governing, protecting, and using it ethically.

The new data dilemma

Standardizing data governance is becoming more and more complex. While initiatives like the Canadian Data Governance Standardization Collaborative aim to set frameworks for managing security and privacy risks, technology continues to evolve faster than regulation. The result? Inconsistent standards across industries, fragmented data management, and increased risks.

> As AI, IoT, and blockchain generate massive amounts of data, the challenge isn't just collecting and storing the information — it's governing, protecting, and using it ethically.

Regulatory pressure is getting stricter. The 2023 to 2026 Data Strategy for the Canadian Federal Public Service underscores the need for stronger data accountability by requiring businesses to prove they can meet tighter regulations — or face legal and reputational consequences.

Risks to watch

Privacy breaches from AI and third-party vendors: The integration of AI and reliance on third-party vendors without appropriate governance frameworks could lead to increased privacy breaches.

Regulatory non-compliance: Organizations struggle to keep up with evolving privacy laws, leading to potential non-compliance risks and legal penalties.

Cross-border data transfer risks: Data sovereignty laws are tightening, making it harder to store and share data internationally.

Insider threats in remote or hybrid work models: Remote and hybrid work models could result in employees potentially mishandling sensitive data outside secure office environments.

Data breaches from poor security controls: Insufficient cyber security controls could lead to data breaches, compromising personal and organizational information.

Challenges in managing user preferences across channels: Keeping user consent and preference management consistent across multiple platforms poses significant challenges, impacting compliance and user trust.

Emerging legislative impacts on third-party data sets: New laws affecting third-party data increase the risk of non-compliance for businesses that don't have proper governance.

Growing scrutiny on children's privacy: New laws tighten restrictions on data collection from minors.

AI policy and ethical considerations: AI technologies raise concerns about data privacy. Organizations need comprehensive AI policies to address ethical and data privacy implications.

Increased enforcement of privacy regulations: Regulators have increased their enforcement actions, leading to higher penalties for data privacy violations and emphasizing the need for compliance programs.

Warning signs

- Unclear vendor policies on data sharing or security controls
- Delayed response to new privacy regulations or compliance deadlines
- Frequent insider access to sensitive data without justification
- Gaps in cross-border data transfer agreements, leading to legal exposure
- Growing customer complaints about transparency and data misuse
- Regulatory scrutiny of AI decision-making and ethical concerns

Mitigation strategies

- Implement robust data governance frameworks
- Strengthen cyber security measures and data governance-related controls
- Improve employee training and conduct regular compliance training
- Create AI ethics guidelines
- Standardize consent and preference management
- Improve insider threat detection
- Focus on children's data protection
- Monitor evolving legislation
- Prepare for regulatory scrutiny

Questions to consider

- How can organizations ensure compliance with evolving privacy regulations while balancing innovation and operational efficiency?
- What strategies can organizations implement to bridge the gap between establishing privacy awareness and empowering employees to actively manage privacy risks?
- What measures can your company take to address public trust and transparency concerns regarding data usage and protection?
- Have you identified and prioritized your most critical data sets and aligned commensurate safeguards based on the prioritization?

Workforce challenge: The hunt for skilled talent

The fight for top talent is more competitive than ever

As Canada's economy shifts toward technology-driven growth, your organization faces an urgent challenge: finding, developing, and retaining the digital professionals you need to succeed.

Industries are already struggling with chronic skills shortages, shifting workforce expectations, and a growing reliance on AI in recruitment. This issue will only accelerate in the year (and years) ahead. Without strategic action, these trends could stifle innovation, slow productivity, and put businesses at a disadvantage in the global market.

The growing digital divide

The demand for tech talent remains high. Despite high-profile job cuts, Equinix's Global Tech Trends Survey reveals that 70 percent of Canadian businesses cite a shortage of skilled workers as a major barrier to success. The most sought-after skills include cloud computing, AI, cyber security, and data analytics.

However, the workforce isn't keeping up. The Future Skills Centre reports that 90 percent of jobs in the next decade will require digital skills, but only 54 percent of workers currently have them. Canada risks falling behind in the global digital economy without urgent investment in upskilling and reskilling.

The race to recruit and retain

The competition for skilled digital professionals has never been fiercer. Businesses are facing:

Difficulty filling full-time positions: More than 75 percent of organizations report difficulty hiring full-time employees, as per the Society for Human Resource Management's 2024 Talent Trends report.

Specialized skills gaps: Cyber security, AI, and data science roles remain particularly difficult to staff.

Retention struggles: Even with a strong labour market, businesses are struggling to keep top talent.

Canada's aging workforce is compounding this labour crisis. Many skilled professionals are retiring, leaving gaps in knowledge that younger workers are not yet ready to fill.

Meanwhile, skilled trades and essential industries are suffering from declining interest. Despite strong wages and career stability, younger generations increasingly prefer technology-based roles over skilled trades, mining, and manufacturing.

The future is clear: Canada's innovation and productivity will continue to suffer if organizations fail to prioritize talent development.

Still, there does seem to be a glimmer of hope. Canada is taking steps to close this skills gap, like launching the Digital Talent Platform, which connects digital professionals with job opportunities in the public sector. As of publishing, more than 14,000 applications have been received.

Despite these efforts, policy shifts and public sentiment may impact hiring strategies. And consequently, organizations cannot rely only on digital platforms to address talent needs. It's critical that you prepare for potential changes to labour laws, immigration quotas, and funding for workforce development.

AI in recruitment

AI is transforming hiring. Businesses are using AI solutions to:

- Speed up hiring processes by filtering resumes and automating assessments
- Improve candidate experiences with personalized recruitment journeys
- Identify skills-based applicants beyond traditional job titles

However, it's not without risks like:

- Bias in hiring algorithms can unintentionally exclude qualified candidates
- Over-reliance on AI may eliminate strong applicants with non-traditional backgrounds
- Lack of transparency into AI training and decision logic raises compliance and ethical concerns

Additionally, with the rise of AI, transactional jobs have great potential to be replaced by AI and automation, prompting employers to decide whether to reskill their workforce or downsize.

To succeed, your organization must ensure that AI is a tool for efficiency and improved experience, not a barrier to diverse hiring.

Risks to watch

Aging workforce and retirements: Senior employees are leaving, creating knowledge gaps in key industries, like the trades

Chronic skills shortages: The skills gap is widening as organizations struggle to fill key roles, hindering productivity and growth.

Economic uncertainty and wage growth: Plans to curtail wage increases amid a glum economic outlook could potentially affect talent retention and attraction.

Labour shortages in mining: The mining industry faces severe labour shortages amid soaring demand for minerals essential in various technologies.

Temporary foreign worker caps: Employers relying on low-wage foreign labour will be restricted, impacting sectors like hospitality and agriculture.

Labour integration challenges: Canada's labour market struggles to keep up with high immigration, leading to challenges in job creation and integration of new workers.

Demand for reskilling and upskilling: More companies focus on reskilling existing employees because of budget constraints and the need to fill skills gaps.

Skills mismatch due to rapid tech advances: Technology is evolving faster than workers can adapt, necessitating continuous learning and adaptation.

Sector-specific skills shortages: Certain sectors, like construction, utilities, and mining, face specific skills shortages, with downstream effects on productivity.

Public sentiment and policy shifts: Public backlash and electoral pressure lead to policy changes that impact immigration and foreign worker programs, which influence the availability of skilled labor.

Warning signs

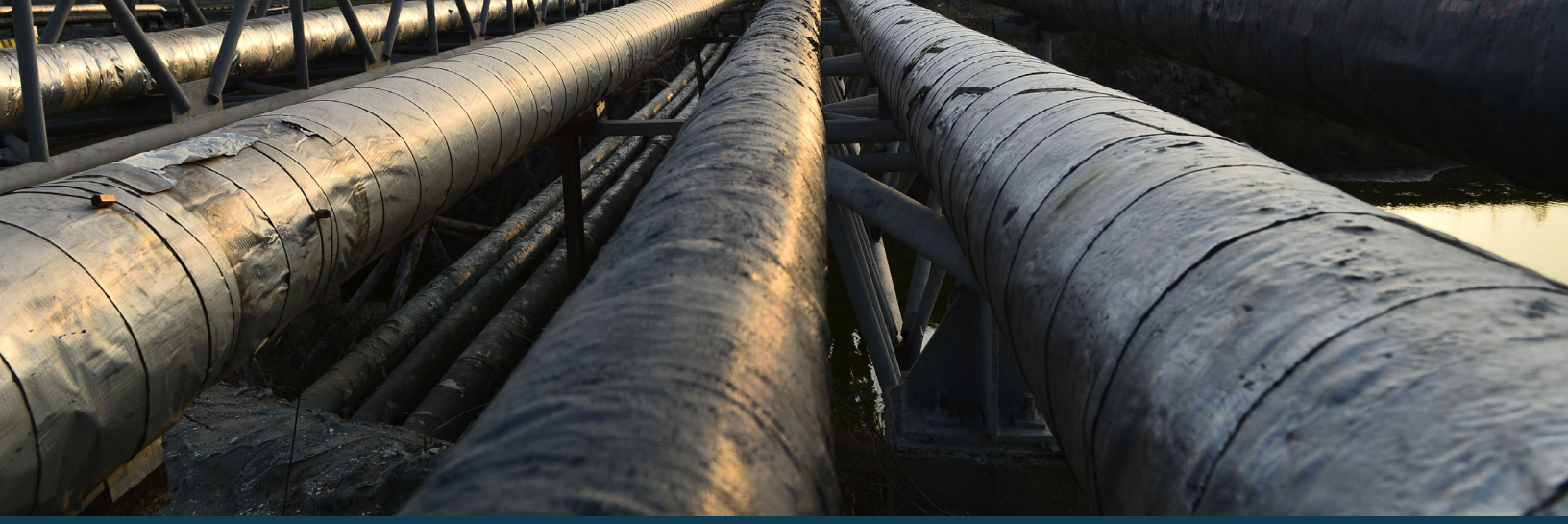
- Inability to source the necessary talent
- Growing skills mismatches between available jobs and workforce expertise
- Delayed hiring times and rising labour costs
- Increasing reliance on contractors and temporary workers
- Declining interest in essential trades and labour-intensive industries

Mitigation strategies

- Invest in reskilling and upskilling
- Expand recruitment pipelines and improve strategies
- Promote careers in skilled trades
- Improve workplace flexibility
- Advocate for public policy support

Questions to consider

- What is the current and projected demand for skilled digital professionals in your organization? How does it compare to the available talent supply and what innovative solutions exist to help you close the gap?
- How are immigration policies and global competition impacting your organization's ability to attract and retain skilled digital talent?
- What role do your education and training programs play in equipping your workforce with relevant digital skills? Do you think your existing programs can meet the needs of the future?
- How might trends like remote work, automation, and economic uncertainty influence the availability and distribution of skilled digital resources within your company?



Strategic convergence:
Tackling the emerging risks of IT and OT Governance

The blurry line between information and operational technology

As Canada's digital infrastructure transforms, the lines between information technology (IT) and operational technology (OT) are blurring. Businesses now rely on integrated systems that connect data-driven insights with real-world operations — further integrating IT and OT. While this convergence unlocks efficiencies, it also creates new vulnerabilities, particularly in the energy, manufacturing, and transportation sectors.

OT systems that were once free from external threats are now prime targets for cybercriminals. Ransomware attacks can halt production, disable power grids, and interrupt transportation networks.

In 2021, the U.S.'s Colonial Pipeline suffered a ransomware attack on the OT side of the business through the virtual private network, which was connected to the IT (or corporate) network. This pipeline carried gasoline and jet fuel to the Southeastern U.S. In the end, Colonial Pipeline paid a $4.4 million ransom to regain control of their OT system.

At the same time, generative AI is reshaping cyber security — offering both defensive advantages and new weapons for attacks. As risks increase, organizations must rethink their governance strategies, balancing innovation with security.

> Ransomware attacks can halt production, disable power grids, and interrupt transportation networks.

OT incidents on the rise

Fraudsters are shifting from targeting IT networks to OT environments, where downtime can be crippling. And the growing frequency and cost of ransomware attacks demand enhanced cyber security measures. Organizations must prioritize resilience through improved incident response planning, employee training, and investment in advanced detection technologies.

AI is both a cyber security tool and a threat to your IT and OT systems, particularly generative AI (Gen AI). In fact, the Canadian Internet Registration Authority reported that 70 percent of cyber security professionals expressed concern about potential cyberthreats from Gen AI, particularly when it comes to data gathering by AI tools (61%) and improved phishing tactics (56%).

As these AI-driven threats grow, organizations must adopt smarter monitoring, tighten data controls, and develop ethical AI policies to stay ahead.

Risks to watch

Ransomware attacks: Ransomware remains the top cybercrime threat, directly disrupting critical infrastructure and essential services.

State-sponsored cyberthreats: Nation-state actors are engaging in espionage and intellectual property theft.

Phishing and social engineering: Phishing attacks continue to be prevalent, exploiting human vulnerabilities to gain unauthorized access to systems, impacting both IT and OT.

Legacy system weaknesses: Outdated IT and OT infrastructure poses security risks and hinders the adoption of modern technologies.

Insider threats: Internal hackers continue to pose significant risks to organizational security.

Supply chain vulnerabilities: Risks associated with third-party vendors and supply chains are rising, which could potentially compromise organizational security.

Regulatory compliance challenges: Evolving regulatory requirements demand continuous adjustments to compliance strategies, impacting IT and OT operations.

Advanced persistent threats: Sophisticated, targeted cyberattacks aimed at stealing data or disrupting operations are becoming more prevalent.

IoT vulnerabilities: The growing number of IoT devices expands the attack surface, introducing new security challenges for both IT and OT.

Operational disruptions from cyber incidents: Cyber incidents lead to operational disruptions, affecting productivity and service delivery.

Warning signs

- Critical infrastructure and essential services are unavailable
- Unexplained system outages or sudden data encryption
- Increased phishing attempts and unauthorized access requests
- Reports of insider leaks or suspicious employee activity
- Delays in software updates and security patches
- Malfunctioning or crashing OT systems

Mitigation strategies

- Strengthen cyber defenses
- Upgrade legacy systems
- Improve employee training and conduct regular security training
- Assess supply chain security
- Establish insider threat programs
- Ensure regulatory compliance
- Monitor for advanced persistent threats
- Security measures on IoT devices
- Develop incident response plans
- Security is holistic considering both IT and OT environments

Questions to consider

- How can your organization address the evolving cyber security threats to IT and OT systems as critical infrastructure becomes a prime target for attacks?
- What measures are being taken to harmonize IT and OT governance, given their different operational priorities and security requirements?
- How will Canadian regulations and global standards shape IT/OT governance and strategy in the future?
- What strategies are being implemented to manage the talent and skills gap in IT and OT convergence, particularly in the context of emerging technologies like AI and IoT?

Disinformation everywhere: Unraveling false information in a digital world

A growing threat to democracy

Disinformation — the deliberate spread of false information to mislead and harm others — is one of the great threats facing Canadian society, democracy, and business. As digital platforms dominate communication, false narratives spread faster and more convincingly than ever, eroding trust in institutions and shaping public opinion in dangerous ways.

In 2023, Statistics Canada reported that 59 percent of Canadians expressed deep concern about online misinformation, with 43 percent admitting they struggle to distinguish between fact and fiction. Although this statistic refers to misinformation, this rising concern reflects the public awareness of the disinformation challenges and the urgency to effectively address it.

And the problem isn't just individual misjudgment — it's a systemic challenge that impacts political stability, corporate reputations, and public safety.

Disinformation is a nuisance. But it's also a direct attack on democratic processes. The Survey of Online Harms in Canada 2024 found that 38 percent of Canadians fell for false news at least a few times per month, highlighting the sophistication of misleading content. Foreign interference, AI-generated fake news, and deepfake technology are being weaponized to manipulate public perception, polarize communities, and influence elections.

Impact on business and the economy

The corporate sector is not immune to disinformation, including memes and social media, forgeries, deepfakes, and disinformation-as-a-service platforms. To counter challenges associated with disinformation, Canadian businesses reported adopting solutions like marketing campaigns (to combat the false or misleading information through education), legal action, improving customer outreach, training employees, and implementing new cyber security measures.

Disinformation campaigns can destroy reputations, erode customer trust, and shake markets.

The World Economic Forum's 2024 Global Risks Report identifies disinformation as the most significant short-term global risk. From financial markets to geopolitical conflicts, the ability to distort reality is a tool used by bad actors to destabilize entire industries.

Risks to watch

AI-generated disinformation: AI tools are creating hyper-realistic fake content and spreading it quickly, making it increasingly difficult to separate truth from fiction.

Deepfake technology: Deepfake attacks create highly realistic, but fake, audio and video content, which poses significant risks to public trust and security.

Foreign interference in democratic processes: Foreign hackers may engage in disinformation campaigns that aim to undermine Canadian democracy by exploiting contentious topics.

Misinformation targeting international students: International students in Canada could be subjected to immigration-related misinformation, leading to confusion and potential exploitation.

Disinformation in social media: Social media platforms are hotspots for the spread of disinformation, affecting public perception and discourse.

Manipulation of public opinion through fake news: The deliberate spread of false information, known as fake news, can be to manipulate public opinion on various issues.

International conflicts: In global conflicts, scammers can use sophisticated disinformation campaigns that can target audiences and sway public opinion.

Online harms and hateful content: There's been a rise in hateful content and online harms, often fueled by disinformation, and impacting individual well-being and dividing societies.

Exploitation of conspiracy theories: Conspiracy theories can be synthetically legitimized through disinformation, which could lead to public mistrust in institutions and experts.

Challenges in detecting and combating misinformation: Despite efforts, detecting and combating misinformation remains a challenge and demonstrates the need for tools and strategies to help Canadians identify false information online.

Warning signs

- Surges in viral content spreading unverified claims
- Coordinated disinformation campaigns tied to elections, global events, or targeted at individuals and/or corporations
- AI-generated news articles, videos, and voice recordings mimicking real sources
- Foreign-backed social media accounts amplifying divisive narratives

Mitigation strategies

- Improve public awareness, education, and media literacy
- Develop advanced detection and fact-checking tools
- Stronger regulatory frameworks, accountability, and enforcement
- Advocate for transparent communication
- Promote and work with global partners to verify accurate information

Questions to consider:

- What proactive measures do you have in place to identify and monitor potential sources of disinformation?
- How does your organization respond to disinformation once it has been identified?
- What training or resources do you provide to employees to help them recognize and address disinformation?
- How does your organization plan to strengthen its defenses against disinformation to protect its stakeholders and audience?

An interconnected future: Conquering third-party risks

The growing threat of dependence

Businesses rely on third-party vendors for everything from cloud services and IT back office support to cyber security. But this reliance comes hand-in-hand with risk.

Even though supply chain generally owns the responsibility related to setting up and managing vendors, there is a growing material importance that third parties are playing in the information technology and operational technology space. Many organizations struggle to find the needed technology expertise required to run and maintain systems, so the reliance on third parties continues to grow every year. Some organizations, especially those located in areas outside of major city centres, may see their technology simply stop operating if they are unable to rely on a dependable IT third party.

A single weak link in a supply chain or vendor network could lead to operational interruptions, financial losses, and/or reputational damage. It's not enough that your organization protects itself from cyberthreats, regulatory compliance failures, and operational weaknesses — all your external partners need to ensure they're protected too.

A 2024 report by MNP found there was a sharp increase in Canadian business' reliance on third parties for technology-related services. This trend underscores the importance of regular reviews of third-party agreements, access permissions to ensure the integrity of security controls, as well as stress tests of third-party liability clauses to determine the maximum liability a third party can realistically cover.

Additionally, a 2024 benchmark report from Hyperproof revealed that 62 percent of organizations experienced a supply chain disruption due to cyber security incidents, a 13 percent increase from the previous year.

Over the course of 2024, some Canadian institutions — particularly in the financial sector — faced increasing scrutiny over their third-party risks. The Office of the Superintendent of Financial Institutions (OSFI) raised concerns over concentration risks, warning that excessive reliance on a handful of service providers could create systemic vulnerabilities.

As businesses deepen their dependence on third parties, managing these risks is no longer an option — it's necessary to survive.

Risks to watch

Cyber security breaches: Third-party vendors are a primary source of data breaches.

Regulatory non-compliance: Failing to align with changing regulations, include those of your third party, will result in risks associated with compliance in technology and cyber risk management

Operational disruptions: Dependence on third parties for critical services increases the risk of operational disruptions because of potential vendor failures or insolvencies.

Data privacy violations: The mishandling of sensitive data by your vendors could lead to privacy risk and potential legal repercussions and reputational damage.

Financial instability of vendors: The financial health of third-party vendors directly impacts their service delivery.

Supply chain vulnerabilities: Global trade disruptions demonstrate the fragility of supply chains, with third-party failures potentially impacting product availability and business operations.

Reputational damage: Working with unethical or non-compliant third parties could tarnish an organization's reputation and stakeholder trust.

Legal liabilities: Inadequate third-party risk management exposes organizations to legal challenges, especially when it comes to data breaches and compliance failures.

Strategic misalignment: Partnering with an external vendor whose objectives diverge from your organization's goals can lead to conflicts and inefficiencies.

Over-reliance on key vendors: Concentration risk increases when businesses depend too heavily on a small number of providers.

Warning signs

- Frequent service outages or delays from key vendors
- Regulatory audits highlighting vendor compliance gaps
- Rising cyber security incidents linked to external partners
- Increased legal disputes involving vendor contracts
- Negative media attention around vendor ethics or security failures

Mitigation strategies

- Conduct regular vendor assessments
- Implement a third-party risk management program
- Diversify vendor partnerships
- Improve contracts so they clearly outline compliance and other protections
- Monitor financial health and stability of key vendors

Questions to consider:

- How does your organization assess and vet third-party vendors before engaging with them?
- What mechanisms do you have in place to monitor third-party performance and compliance over time?
- What are your organization's protocols for responding to third-party incidents or breaches?
- How are your third-party contracts structured to include clauses about managing or limiting risk?

Future ready:
Does your organizational design start with your technology and data infrastructure?

Are you ready for the future of work?

The future of work is transforming in front of our very eyes. It's forcing organizations to rethink their organizational structures, leadership approaches, and workforce strategies.

However, as businesses embrace next-generation organizational design, they face critical challenges like talent shortages, cultural resistance, outdated infrastructure, and cyber security threats. Organizations need a clear vision and strategy to navigate these new waters — or risk falling behind the competition.

The risk of disconnection

Many organizations struggle to adapt to change, not because they lack the resources but because they lack a cohesive vision for transformation. Without strong leadership, a commitment to new ideas and innovation, and clear and open communication, new technologies, business models, and structures can feel more burdensome than advantageous.

> Organizations need a clear vision and strategy to navigate these new waters — or risk falling behind the competition.

Change efforts often fail because there's a lack of backing from the leadership team. Leaders who don't actively drive transformation create uncertainty and resistance within their teams. Employees tend to stick to their familiar routines, reinforcing the need for good communication and effective change management.

When leaders fail to articulate the purpose and benefits of transformation, employees can disengage, which slows (or even halts) new initiatives.

Additionally, the evolution of digital tools means the workforce must continuously upskill and have access to updated systems. But many businesses don't invest in training, leaving their team unprepared for emerging demands.

Even in cases where employees are trained and eager to buy in, outdated digital infrastructure can't support the needs of modern business. Without strategic investment in technology, many will struggle with ongoing inefficiencies, security risks, and lost productivity.

Risks to watch

Talent acquisition and retention challenges: Following a sizable digital transformation project, organizations can struggle to redesign its organizational structure, and to attract and retain skilled professionals, limiting their capacity to execute business priorities.

Inadequate workforce transformation: Resistance to change and inflexible cultures can stop needed workforce transformations, which impacts overall readiness.

Cyber security vulnerabilities: Cyberthreats are a significant risk to organizations undergoing system transformation, leaving many businesses underprepared for potential attacks.

Economic and financial uncertainty: The long-term impact of increases in interest rates and inflation can result in economic uncertainties, putting financial resilience to the test.

Regulatory changes and compliance: Increased regulatory scrutiny requires organizations to adapt quickly or be prepared to face potential legal and financial repercussions.

Technology outpacing workforce skills: Technological changes are outpacing existing skill sets, reinforcing the need for continuous learning and adaptation.

Third-party dependencies: Increased reliance on external vendors can lead to unexpected disruptions and security risks, which impacts the organization's readiness to use the technology implemented during the transformation.

Operational disruptions: Unexpected supply chain breakdowns, economic downturns, or crises can through well-designed organizations into chaos.

Weak risk management frameworks: A lack of comprehensive risk management strategies can leave organizations vulnerable to emerging threats and challenges.

Cultural resistance to change: Organizational cultures that are resistant to change can limit adaptation to new business models and market demands.

Warning signs

- High turnover rates
- Persistent reliance on outdated tools and workflows
- Employees resisting new processes or training
- Frequent cyber security breaches or compliance failures
- Slow adoption of technology due to leadership hesitation
- Regulatory penalties or increased scrutiny from governing bodies

Mitigation strategies

- Invest in talent management and training
- Promote an agile culture
- Strengthen cyber security protections
- Improve financial resilience through diversification
- Ensure compliance with evolving regulations
- Manage third-party risks
- Develop business continuity plans
- Implement a comprehensive risk management program
- Implement change management initiatives

Questions to consider

- How does your organization assess and align both its strategy and workforce capabilities with changing demands, including emerging technologies and market trends?
- What strategies so you have in place to balance flexibility and stability in your organizational structure?
- How does your organization integrate governance and decision-making processes into innovative design frameworks?
- What mechanisms are in place to continuously monitor and adapt your organizational design in response to internal and external changes?

Insurance risk:
The devil is in the details

The fine print has never been more important

Like many other industries, Canada's insurance sector faces unprecedented risks — from the impacts of climate change and rising crime rates to shifting market dynamics and evolving regulations. As insurers, organizations, and policymakers try to find their footing in this new era, it's become critical to read and understand the small print in contracts.

Extreme weather events put immense pressure on the insurance industry, and these are becoming more frequent and costly. Over the past decade, annual insured losses from natural disasters have averaged $2.2 billion, a threefold increase over the rolling 10-year average, as reported by the Insurance Bureau of Canada. The 2024 Jasper wildfire alone resulted in $880 million in insured losses.

In response, insurers are revising risk models, raising premiums in high-risk areas, and tightening up the terms of coverage. Canadian businesses need to prepare for higher costs, increased scrutiny, and potential gaps in coverage.

> Canadian businesses need to prepare for higher costs, increased scrutiny, and potential gaps in coverage.

Shifting market conditions

Despite the challenges above, the insurance market remains resilient. According to CMB Insurance Brokers, a one percent drop in commercial insurance premiums in the third quarter of 2024 indicates more competition among insurers. But, with catastrophes like the Jasper and B.C. wildfires driving up the volume of claims, many companies are opting for stricter underwriting and risk selection processes.

Regulators are also stepping up their scrutiny. The OSFI flagged elevated interest rates, market instability, and climate risks as key concerns for 2024 and 2025. Financial institutions, like banks, must now consider integrating climate risk assessments and strengthening their capital management to stay resilient.

As natural disasters, auto theft, and market volatility converge to shape the future of insurance in Canada, stakeholders need to embrace innovation and collaboration. For insurers, this means enhancing risk modeling, adopting new technology, and proactive regulatory measures will be critical to managing these challenges.

For businesses, this means you must understand the risks and adopt preventive measures which can help mitigate their financial impacts and ensure continued access to affordable insurance coverage.

Risks to watch

For the insured

More frequent and severe natural disasters: Rising claims from wildfires, floods, and storms will lead to a surge in claims.

Geopolitical risks: Global political tensions and conflicts introduce uncertainties that impact market stability and investment strategies.

Medical inflation: Increasing healthcare costs are resulting in more claim expenses, which pushes health insurers to adjust premiums and coverage limits.

Property risks: Higher property values and construction costs, along with natural disasters, increase the volume of claims and make underwriting more complex and expensive.

Liability verdicts: An increase in large liability verdicts, influenced by social inflation, can result in higher claim payouts and adjustments in liability coverage.

For Insurers

Cyber security threats: A rise in cyberattacks, including global tech outages, pose significant challenges and leaves insurers bracing for a wave of claims and reconsidering underwriting standards.

Technology advancements: AI and digital innovations create both opportunities and challenges, but an insurer's technology needs to continuously evolve to stay competitive.

Economic uncertainty: Fluctuations in interest rates and economic conditions impact investment returns, as well as the overall financial stability of insurers.

Talent acquisition and retention: The insurance industry struggles to attract and retain skilled professionals, which in turn impacts operational efficiency and innovation.

Shifting regulations: Evolving regulations require insurers to adapt quickly to maintain compliance or face failures that could potentially lead to legal and financial repercussions.

Warning signs

- Rising reinsurance costs and limited coverage in high-risk areas
- Increasing auto policy surcharges
- Delays in cyber insurance underwriting due to risk concerns
- High employee turnover within insurance companies impacting the efficiency of underwriting and claims processing

Mitigation strategies

- Develop climate risk assessment
- Boost cyber security measures
- Monitor the geopolitical landscape
- Implement ways to control healthcare costs
- Re-evaluate property underwriting practices
- Identify and address liability exposures
- Ensure regulatory compliance
- Invest in advanced technology and training
- Build financial resilience through diversification
- Implement programs to attract, train, and retain skilled employees

Questions to consider

- What types of insurance coverage are essential for your organization based on its industry, operations, and legal requirements?
- How often does your organization review and update its insurance policies to reflect changes in operations, assets, or risk exposure?
- What strategies are in place to reduce potential claims, like implementing risk management programs, employee training, or safety protocols?
- How does your organization stay compliant with policy requirements and regulatory obligations to avoid coverage denials or penalties?

Future-proof resilience: Be bold and agile

Agility is the ultimate competitive advantage

Running a business today means moving fast. To stay ahead, your organization needs to think smarter, move quicker, and stay one step in front of emerging challenges.

Rising costs remain a prominent challenge for Canadian businesses, according to Statistics Canada, with 62.5 percent of businesses anticipating cost-related obstacles in the first quarter of 2025.

And the long-term impact of interest rates and debt costs are also weighing on organizations. These financial pressures limit investments in growth, technology, and workforce development, making financial resilience a priority.

The labour market also remains tight and a significant issue for modern businesses. In fact, the same Statistics Canada survey found that labour cost was the most commonly anticipated input businesses expect to be an obstacle in the second quarter of 2025. Without access to talent, your company risks falling behind on productivity, innovation, and service delivery. Many are turning to automation, upskilling, and new recruitment strategies to help close this gap.

> Without access to talent, your company risks falling behind on productivity, innovation, and service delivery.

While fewer businesses cite supply chain disruptions as a top concern, about 16 percent still anticipate challenges. Delays, inventory shortages, and increasing transportation costs continue to put strain on operations. To stay ahead, you must diversify your suppliers, strengthen logistics, and invest in smarter inventory management.

OSFI has underscored cyberthreats, third-party dependencies, fraud, and technological vulnerabilities as pressing risks for businesses. As we become more and more reliant on digital infrastructure, data breaches, ransomware attacks, and supply chain cyberthreats will continue to test operational resilience.

Despite these challenges, many businesses are cautious but still looking on the bright side. Statistics Canada reported that about three-quarters (73.1%) of businesses are either very optimistic or somewhat optimistic about their outlook over the course of 2025. The proportion of businesses reporting an optimistic future outlook has consistently remained above 70 percent since the second quarter of 2024.

Risks to watch

Business interruptions: Cyber incidents, natural disasters, or supply chain failures could disrupt operations.

Cyber security threats: The increasing frequency and sophistication of cyberattacks pose substantial threats to business continuity.

Natural catastrophes: Floods, wildfires, and storms result in property damage and supply chain disruptions, putting organizational resilience to the test.

Supply chain disruptions: Global and regional supply chain issues could impact the delivery of goods and services.

Regulatory changes: Evolving regulations require businesses to adapt quickly to maintain compliance.

Talent acquisition and retention: Challenges in attracting and retaining skilled workers impact operational efficiency and innovation.

Economic uncertainty: Inflation, interest rates, debt costs, and market volatility will continue to create financial instability for businesses.

Third-party risks: Vendors and suppliers introduce vulnerabilities related to service continuity and compliance.

Technological advancements: Technological changes require continuous adaptation, so businesses need agility to integrate new technologies to stay competitive.

Geopolitical uncertainty: Global tensions introduce uncertainties that could impact market stability and business operations.

Warning signs

- Unplanned operational downtime due to cyberattacks, weather events, or supplier failures
- Higher insurance premiums and regulatory scrutiny linked to climate and compliance risks in some industries, unless organizations adopt more advanced predictive technology
- Delays in hiring for key roles, leading to a slowdown in productivity
- Frequent disruptions in vendor performance or external partner compliance issues
- Reports of delayed cyber security upgrades

Mitigation strategies

- Develop a comprehensive business continuity plan
- Strengthen cyber security measures
- Implement risk management frameworks
- Monitor economic trends
- Diversify talent strategies
- Improve supply chain resilience
- Manage third-party risks
- Monitor regulatory compliance
- Adopt emerging technologies
- Stay informed on geopolitical developments

Questions to consider

- How does your organization foster adaptability and continuous learning among its workforce?
- What systems and strategies are in place to make sure decision-making is agile and informed by real-time data?
- How does your organization cultivate a culture of innovation while maintaining its core values and stability?
- What measures do you take to assess and mitigate risks from external factors, like economic downturns, political instability, or cyber security threats?

The future of governance:
Boards meet evolving risks

The boards of the future need to be as diverse and trained as those they govern

The role of boards of directors is undergoing a seismic shift, fueled by technological advances, economic volatility, regulatory changes, and stakeholder expectations. To remain effective stewards, boards must adapt alongside businesses, expanding their expertise and continuously refining their governance strategies.

As risks continue to evolve, some organizations will be left wondering: Should ongoing learning and development be mandatory for board members? Could improving literacy in AI, cyber risk, and sustainability improve decision-making and strategic foresight?

Gain a competitive advantage

Board diversity is no longer an ethical imperative — it's an asset. Canadian Securities Administrators (CSA) report that women now hold 29 percent of board seats among Canada's largest publicly traded companies. New Institutional Shareholder Services guidelines require at least one racially or ethnically diverse board member for S&P / TSE Composite Index companies.

While progress is being made, it's worth reiterating the importance of diverse perspectives at the leadership level for fostering innovation, resilience, and public trust. Boards need to expand their traditional focus on the financial stability of an organization and management's ability to deliver on the strategic plan. Directors and management who encourage agility and innovation will be valued and instrumental in challenging the organization to be more progressive in the face of global and economic uncertainty.

> Could improving literacy in AI, cyber risk, and sustainability improve decision-making and strategic foresight?

Boards are also facing more regulatory inspection. The CSA has proposed National Instrument 51-107 to standardize climate-related disclosures. If it proceeds, companies will be expected to proactively integrate climate risk into governance or face penalties and reputational damage.

Additionally, proxy advisor firms like Glass Lewis have signaled that poor cyber oversight may lead to negative recommendations against directors, particularly for organizations that are materially impacted by cyber incidents. Boards need to collaborate with management to improve cyber security measures and make sure they stay resilient in the face of digital threats.

Risks to watch

Shareholder activism: Boards are under greater pressure from activist investors, so they need to be transparent and actively engaged.

Diversity and inclusion: Ongoing regulatory and proxy advisory policy changes underscore the importance of diversity within boards.

Cyber security threats: Rising cyberattacks and ransomware incidents are putting board-level oversight to the test.

Regulatory compliance: Changing regulations, particularly around ESG, are demanding more attention and resources.

Talent development and succession planning: Boards need to focus on assessing current leaders and identifying gaps in their talent pipeline to navigate a changing business environment.

Economic uncertainty: Inflation, interest rates, and volatile financial markets could impact financial stability and require board direction.

Technological integration: New technologies to enhance operations can be both an opportunity and an obstacle and require oversight.

Reputation and brand management: Increased social media scrutiny and consumer expectations mean boards need to handle any crises quickly.

Third-party risks: Managing risks associated with external vendors has become increasingly important to operational resilience.

Warning signs

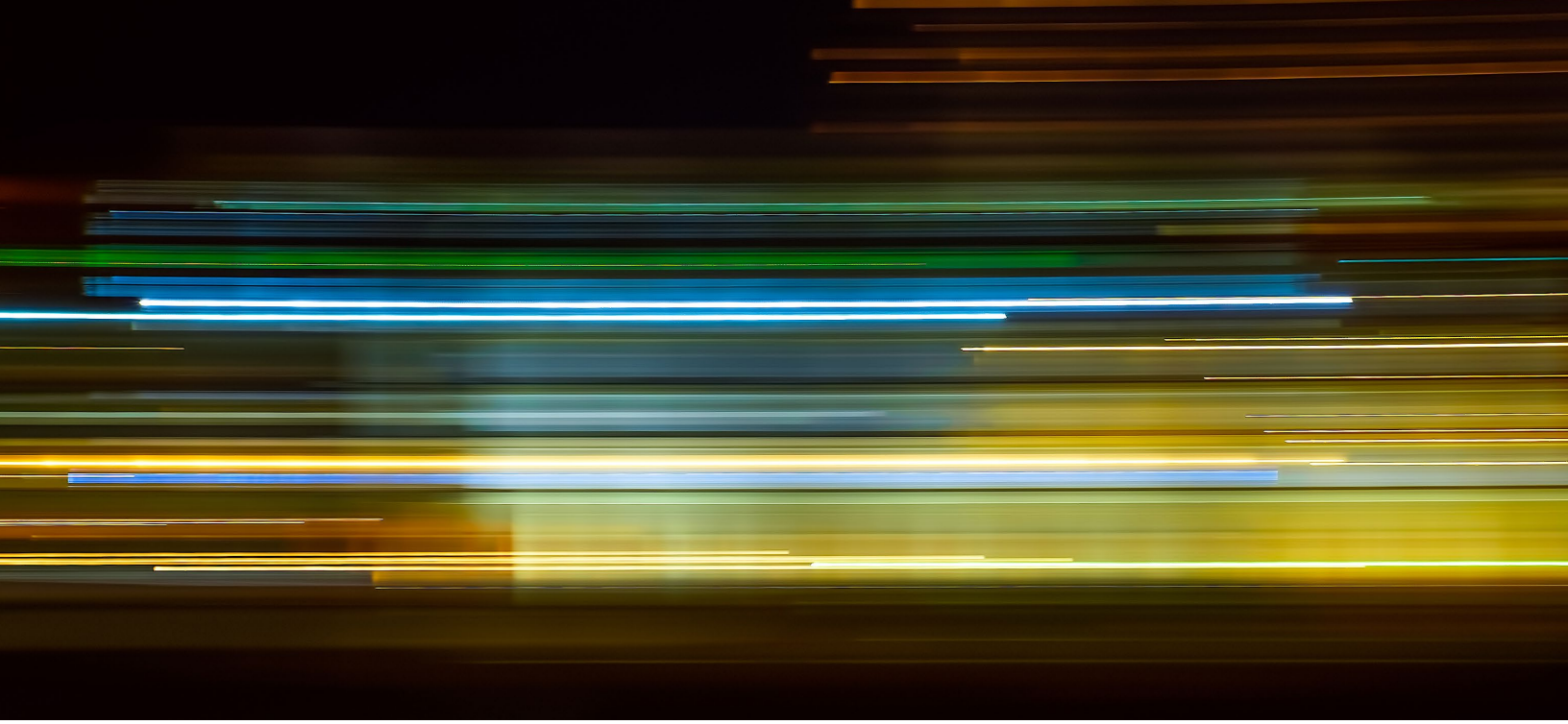
- Shareholder complaints or proxy battles are occurring more frequently
- Cyber incidents escalating in severity because of lack of oversight
- Regulatory audits revealing non-compliance
- Declining investor confidence, reflected in share price fluctuations or public criticism
- Delayed adoption of emerging technologies because of board hesitancy or lack of expertise
- High executive turnover
- Reputation damage from environmental, ethical, or governance missteps

Mitigation strategies

- Implement ongoing governance training
- Maintain transparent communication and proactive investor relations
- Conduct regular cyber risk assessments and training
- Increase diversity
- Stay ahead of ESG and other related regulations
- Monitor economic trends
- Adopt scalable technologies for evolving business needs
- Identify future leaders early and establish executive pipelines
- Align business strategies with sustainability and resilience efforts
- Manage third-party relationships
- Actively manage reputation and brand integrity

Questions to consider

- What processes are in place to ensure your board has the right mix of skills, expertise, and diversity?
- How does your board stay informed about evolving regulatory and governance requirements?
- What governance frameworks or practices does your board use to oversee risk management?
- How does your organization assess and improve the board's performance and accountability?



The next move is yours to make

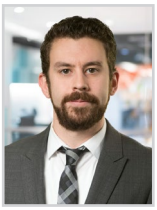
The nature of risk has changed, and so must our response. Today's threats are faster, more complex, and more connected than ever before. But with the right insights and a proactive strategy, your organization can turn uncertainty into opportunity.

The future belongs to those who are ready.

Let's talk about how your organization can stay ahead of what's coming.

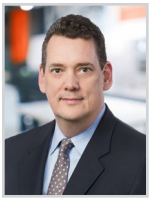
Contributors

Richard Arthurs
Partner | National Leader, Internal Audit



Drew Buhr
Partner | National Cyber Security Assessment Lead, Digital Services

Craig Burkart
Partner | National Leader, Insurance Advisory



Gord Chalk
Partner | Consulting Leader, Energy and Utilities

Caitlin Crowley
Partner | National Enterprise Transformation Leader, Digital

Catharine Dutt
Partner | Enterprise Risk Services

James Dyack
Partner | Valuations and Litigation Support

Johnny Earl
Managing Director, Corporate Finance

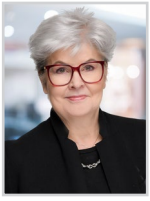
Mariesa Fett
Partner | National Leader, Enterprise Risk Services

Soumya Ghosh
Partner | Digital Services

Denise Gigova
Partner | National Digital Transformation Leader, Digital Services

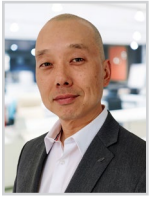
Adriana Gliga-Belavic
Partner | Privacy Leader, Privacy and Data Governance

Wendy Gnenz
Partner | Digital Services

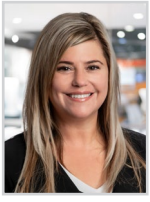


Mary Larson
Partner | Strategy Consulting and Advisory

Chris Law
Partner | Digital Services



Jason J. Lee
Partner | Digital Services



Lisa Majeau-Gordon
Partner | National Leader, Forensics and Litigation Support

Eugene Ng
Partner | Cyber Security Leader, Enterprise Risk Services

Contributors

Cameron Ollenberger
Partner | Enterprise Risk Services

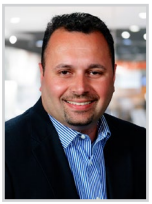
Edward Olson
Partner | ESG Leader, Enterprise Risk Services

Hash Qureshi
Partner | Enterprise Risk Services

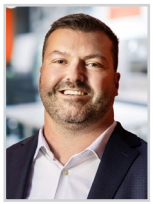
Phil Racco
Partner | Enterprise Risk Services and Third-Party Risk Management

Mark Reynolds
Managing Director, Corporate Finance

Mike Reynolds
Managing Director, Corporate Finance

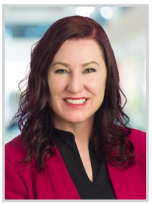


Geoff Rodrigues
Partner | Enterprise Risk Services

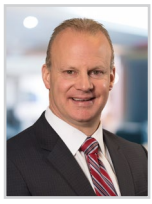


Adam Taylor
Partner | Enterprise Risk Services

Lee Thiessen
Partner | Vice President, Real Estate and Construction



Gina Thornton
Partner | Enterprise Risk Services



Cliff Trollope
Partner | National Leader, Business Resilience Services

Colin Wenngatz
Partner | Data and Analytics

Lanny Westersund
Partner | Consulting Services

Giovanni Worsley
Partner | Property Tax Services

Canada's business advisor

National in scope and local in focus, MNP provides client-focused accounting, consulting, tax, and digital services in more than 150 communities from coast to coast. Founded in Brandon, Manitoba in 1958, we are proud to be born and raised in Canada and committed to the success of Canadian individuals, businesses, and organizations. Our advisors deliver personalized strategies and made-in-Canada solutions to help you reach your full potential — wherever business takes you.

For more information, contact:

Richard Arthurs, FCPA, FCMA, MBA, CFE, CIA, CRMA, QIAL
National Leader, Internal Audit
richard.arthurs@mnp.ca

Mariesa Fett, CPA, CA, ABCP, CRMA, ICD.D
National Enterprise Risk Services Leader
mariesa.fett@mnp.ca

PRAXITY®
A member of the Praxity Global Alliance