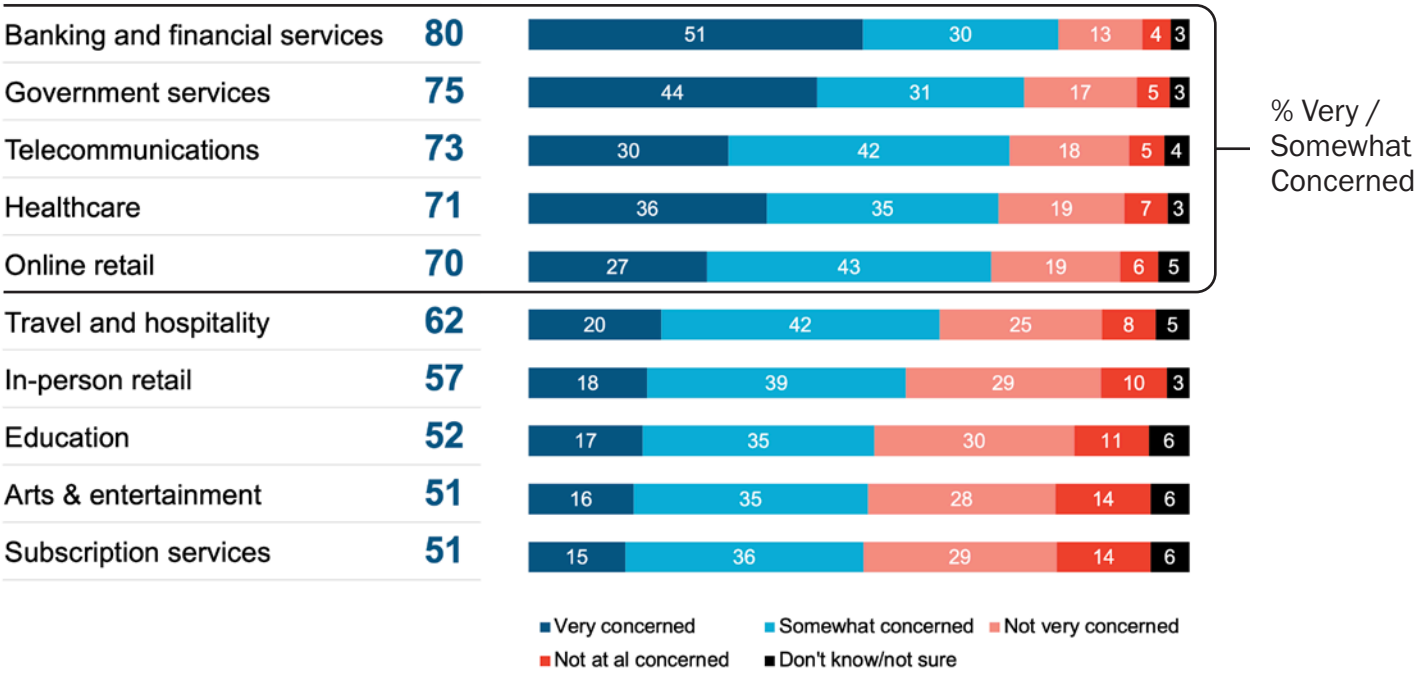
Data breaches are on the rise – and Canadians expect their businesses to be prepared

In a polarized, digital first, and deeply interconnected economy and society, data breaches are on the rise from both a frequency and cost perspective. PwC's 2025 Global Digital Trust Insights survey found that the average cost to an organization of a data breach has risen to $3.32 million per incident. Their increasing frequency has not resulted in increasing acceptance. Canadians are more concerned, more alert, and more judgemental of the enterprises they interact with when it comes to protecting their data. Exclusive research from Navigator reveals that 85% of Canadians are worried about data breaches with 66% reporting increased concern compared to three years ago. For industries handling sensitive information, the concern level is even more acute.

CONCERN AROUND DATA BREACHES PER INDUSTRY



Growing concern is stacked on top of an absence of trust, with only 40% of respondents believing that businesses affected by breaches have adequately addressed customer concerns or resolved issues. Is this anxiety fueled by high-profile incidents such as the Canada Revenue Agency and Ticketmaster breaches? Likely in part.

But it's amplified by some of the driving technological changes of the day – changes that are only intensifying.

- **Widespread adoption of artificial intelligence has struck a nerve,** with 70% of Canadians expressing that the technology poses a greater risk compared to just 39% who see it as a valuable tool for preventing breaches.
- **Concern over state-sponsored threats is growing** with 71% of Canadians believing that state-sponsored cyber threats will increase over the next five years and 65% expressing concern that Canadian entities are vulnerable to such breaches.
- **The rise of ransomware extortion poses complex legal, ethical, and financial questions.** While the Government of Canada does not recommend ransom payments, 77% of Canadians agree that it is important to pay ransom (when applicable) to prevent or limit the spread of customer information.

FORGING A PATH FORWARD

Despite these challenges, every business has the opportunity to do right by doing right, showcasing to their customers, employees and stakeholders that they have responded swiftly, with transparency and speed. Specifically:

- **93%** of Canadians emphasized the importance of enhancing security measures, including implementing new systems, conducting staff training, and reviewing policies.
- **92%** believe businesses should offer free credit monitoring and conduct a thorough, transparent investigation.
- **92%** highlighted the importance of notifying clients immediately.

While every scenario brings its own qualities, we remind Canadian organizations to use the following principles in preparation for and response to a breach.

1. **Speed beats perfection, preparation enhances speed**
   As soon as you are aware of a breach, the clock is ticking on your first notification to affected stakeholders. Timely transparency is critical to maintaining trust. Simple and cost-effective preparatory steps can go a long way in building out your crisis and cyber response capabilities.
2. **Lead from the front**
   Activate an integrated crisis response team led by a decisive C-suite leader. Streamline communications by appointing a single spokesperson to manage messaging and maintain consistency.
3. **Develop, practice and implement a crisis management framework**
   It's not a question of if, but when. Prepare for the inevitable with a tailored, practiced crisis communications plan, cyber incident response plan and business continuity plan that leaves guesswork at the door when a breach occurs. Regular exercising of these plans is critical.
4. **Engage with Key Stakeholders**
   Communicate proactively with employees, customers, partners, and regulators. Trust is rebuilt when stakeholders are at the heart of decision-making.

5. Provide tangible support to affected customers

Canadians need to see you work to protect their data. Free credit monitoring, identity theft protection, or the establishment of a dedicated hotline can showcase your commitment to customers and their recovery, reinforcing your organization's accountability.

6. Find and communicate remedial steps

Take immediate action to strengthen your defences. Upgrading systems, conducting audits, and training employees sends a clear message: your organization is serious about preventing future breaches.

7. Leverage external experts

Bring in trusted professionals, like Navigator, PwC, and a legal breach coach to validate your response. Highlighting external expertise reassures stakeholders and demonstrates your commitment to professional recovery.

8. Monitor and manage public sentiment

Track media and social sentiment to gauge public reactions. Use these insights to refine your messaging, ensuring it is empathetic, nuanced, and aligned with stakeholder expectations.

9. Share lessons learned

Be transparent about how you addressed the breach and what improvements have been made. Sharing lessons learned demonstrates accountability and positions your organization as a leader in trust recovery.

10. Conduct a post-crisis response and reputation audit

Evaluate your response, stakeholder sentiment, and reputational risks. Use these insights to refine strategies, rebuild trust, and strengthen your crisis management framework.

Looking to gain deeper insights and better understand how to prepare your organization to effectively respond to and recover from a data breach? Connect with one of our experts today.

Book a consultation by contacting us at **info@navltd.com** or **ca_incident_response@pwc.com**