

## Hey! What's New? 2025-94

### IBM Study Finds Data Breach Costs Are Rising Sharply in Canada

An IBM-sponsored article in the latest issue of FEI Canada's *F. A. R.* says that the global average cost of a data breach has fallen for the first time in five years — but not in Canada, where costs continue to climb.

It notes that, “globally, the average cost of a breach dropped slightly to CA\$6.4 million, down from CA\$6.6 million the year before, according to global research by IBM and the Ponemon Institute. In contrast, Canadian organizations are facing higher and more complex breach-related expenses. The study found that the average cost of a data breach in Canada has risen to CA\$6.98 million — a 10.4 percent increase over last year. In the U.S., costs rose 9 percent.”

The IBM report says that “rising expenses stem from a range of factors, including the costs of detecting and containing breaches, regulatory compliance, legal services, and crisis communications.” As well, “Canada is falling behind in adopting AI-powered security tools and addressing gaps in governance, leaving businesses more vulnerable to emerging threats. And one-third of Canadian businesses reported not having access controls on AI systems, positioning them as easy, high-value targets.”

Recovering from a cyberattack isn't just costly — it's also complex, the report points out. “Detecting breaches can take time, and the cleanup often involves teams of professionals, business downtime, and disruptions for both workers and customers.”

While phishing scams remain the most common entry point for cyberattacks, one of the fastest-growing threats is “shadow AI” — the use of unapproved or unsanctioned AI tools by employees. These unmonitored systems often open the door to hackers. “Shadow AI is becoming a major cybersecurity concern for Canadian businesses. These systems often handle sensitive data and connect to external platforms outside the company's control, increasing the risk of exposing personal information and intellectual property. The impact is not just technical but financial. Organizations with high levels of shadow AI reported an average of CA\$967,011 in additional breach-related costs compared to those with limited or no shadow AI.”

Certain sectors face significantly higher costs than others — with health care, finance, and industrial sectors among the hardest hit. “The financial industry reported the highest breach costs at CA\$9.97 million in 2025 — up 7.4% from CA\$9.28 million the year before — underscoring the high value and sensitivity of financial data.”

According to the report, “companies that extensively use AI across their Security Operations Centre (SOC) experience an average breach cost of CA\$5.19 million. That's a significant drop compared to CA\$8.53 million for organizations that haven't adopted these technologies.”

As cyber threats grow more complex, the report urges Canadian organizations to take a more proactive approach to security. The report outlines four key recommendations:

- **Govern and Secure AI Systems:** Create clear policies to regulate AI use, prevent shadow AI, and ensure alignment with privacy regulations.
- **Invest in Security Automation:** Leverage AI-powered tools to detect and contain cyber breaches more quickly and effectively.
- **Integrate AI Security and Governance:** Adopt platforms that combine security with governance to help identify and manage unauthorized AI systems automatically.
- **Expand Employee Training:** Enhance workforce education around cybersecurity to reduce the risk of breaches caused by human error.

Together, the report concludes, “these measures aim to close critical security gaps and help Canadian businesses stay ahead of evolving digital threats.”

For more details and recommendations, download the report at [Cost of a Data Breach Report 2025](#).