



The State of Cybersecurity in Quebec: Practices, Incidents, and Business Resilience

Analysis of Data from Statistics Canada's Canadian Survey of Cyber Security and Cybercrime (CSCSC 2021 and 2023)



Benoît Dupont & Jessica Roy
IMC2 – Université de Montréal

June 2026

With the financial support of



Contents

Introduction	1
Methodology.....	3
Chapter 1. Evolution of the Cybersecurity Posture of Quebec Businesses Between 2021 and 2023.....	5
Profile of Cyberattacks Experienced	5
Overview of the Evolution of Cybersecurity Practices.....	7
Cybersecurity Expertise Available In-House	7
Technical Measures and Risk Management Activities.....	10
Relationships with External Partners and Responses to Cyberattacks.....	15
Chapter 2. The Cybersecurity Posture of Quebec Businesses in the Canadian Context.....	19
Comparative Victimization.....	19
Cybersecurity Measures and Practices	21
Cybersecurity Specialists and Recruitment	21
Organization-Wide Cybersecurity Awareness: Quebec Lags Behind	24
Frequency and Regularity of Reporting to Senior Management: Two Distinct Governance Profiles	24
Self-Assessment of Preparedness and the Risk of Overconfidence	25
Risk Management and Internal Measures	26
Collaboration and Partnership Practices	28
Chapter 3. Cybersecurity Practices and Cyber Resilience: A Multivariate Analysis	31
Sample Profile and Distribution of Variables	31
Determinants of Cyber Victimization: What Actually Protects Organizations.....	33
Determinants of Recovery Costs: Governance as a Protective Factor.....	35
Determinants of Service Disruptions: The Limits of Predictability	39
Summary: Cybersecurity as an Investment in Human Capital.....	42

INTRODUCTION

Knowledge about the state of cybersecurity in businesses in developed countries generally depends on surveys produced by vendors of technical solutions and advisory services, who take advantage of the visibility generated by media coverage of these studies' findings to increase their recognition among potential clients. Some of these surveys are repeated annually and are eagerly awaited by the industry, such as the Ponemon Institute and IBM study on the cost of data breaches, which makes it possible to benchmark financial impacts, causes, and the effectiveness of mitigation measures worldwide.¹ While some of these surveys have become essential references in cybersecurity, most of them suffer from methodological weaknesses that limit their usefulness: the samples from which the data are collected are very limited in size and never representative, response rates are low and introduce selection biases, and the nature of the questions more often stems from the commercial objectives of the company sponsoring these studies than from a concern to rigorously measure organizations' exposure to cyber risks and the maturity of their security practices.²

Studies conducted by public government statistical agencies can offset these weaknesses, but few countries have sufficient resources to establish a national cybersecurity data collection program, particularly because of the costs involved and the technical expertise required. Fortunately, our country has such a program through Statistics Canada's Canadian Survey of Cyber Security and Cybercrime (CSCSC), funded since 2018 by Public Safety Canada. Because of the generous size of its sample — more than 10,000 businesses in each wave — its regularity — the survey is administered every two years — the obligation for businesses to participate in the survey under federal laws, which guarantees response rates of more than 70%, and the relative stability of its questionnaire from one wave to the next, this survey is probably one of the most representative sources worldwide on business cybersecurity practices and the issues businesses face.

Although each wave is the subject of a detailed report by Statistics Canada, the results often remain presented at a very high level and rarely make full use of the richness of the data collected.³ In addition, the published results concern only Canada as a whole, whereas significant variations may occur from one province to another, as specific regulatory frameworks are adopted that redefine organizations' obligations and incentives with respect to cybersecurity. This is, for example, what occurred in Quebec in 2021 with the adoption of Law 25, which modernized the laws governing the protection of personal information and, in particular, strengthened requirements for businesses in the event of confidentiality incidents that often result from cyberattacks. This law came into force gradually between September 2022

¹ Ponemon Institute (2025). *Cost of a Data Breach Report 2025: The AI Oversight Gap*. IBM, Armonk, NY.

² Anne-Marie Côté, Mathieu Bérubé, & Benoît Dupont (2016). "Cybercrime Statistics and Digital Threats: How Security Organizations Measure Cybercrime." *Réseaux*, 3–4(197–198), 203–224.

³ See, for example, Statistics Canada (2024), *The Daily*, "The Impact of Cybercrime on Canadian Businesses, 2023," October 21; or Statistics Canada (2020), *The Daily*, "About One-Fifth of Canadian Businesses Were Impacted by Cyber Security Incidents in 2019," October 20.

and September 2024, forcing businesses in the province to comply with stricter obligations regarding governance, transparency, and cybersecurity.

This report stems from the convergence between the availability of data of unusually high quality in Canada, on the one hand, and the desire to better understand the specific features of the cybersecurity posture of Quebec businesses in an evolving legislative context, on the other. Through Statistics Canada's secure data access program, we were able to work with the confidential microdata files from the CSCSC in order to extract the subgroup of businesses established in Quebec. This allowed us to conduct more in-depth comparative analyses than those available in Statistics Canada's public documents. More specifically, this approach was intended to achieve three objectives:

1. Develop a dynamic portrait of the cybersecurity posture of Quebec businesses between 2021 and 2023 and identify what changes Law 25 may have brought about during these first two years of implementation;
2. Compare Quebec businesses' exposure to cyber risks and their cybersecurity practices with those of their counterparts in the rest of Canada, in order to highlight any specific features and challenges requiring particular attention;
3. Try to use these extremely detailed data to identify the cybersecurity measures or practices that improve the cyber resilience of Quebec businesses by protecting them from cyberattacks and reducing their recovery times and costs.

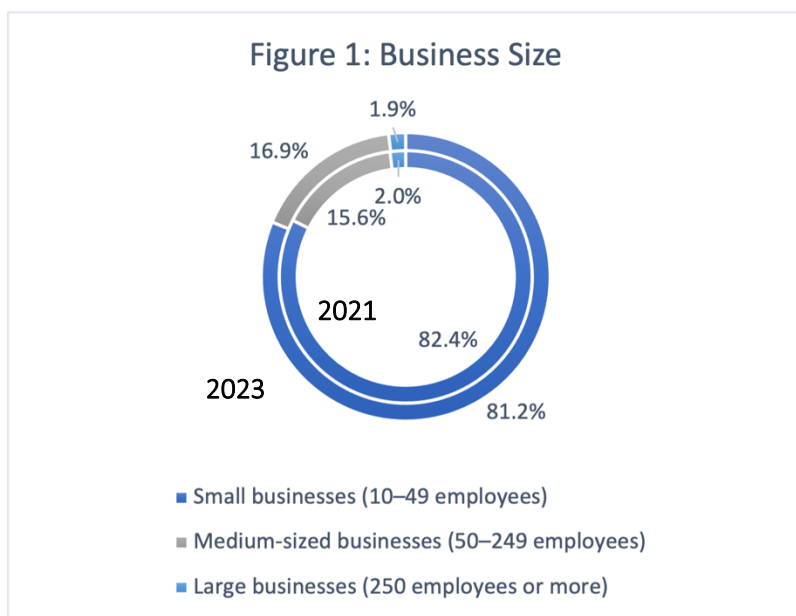
These three objectives are addressed successively in the three chapters that make up this report, following a methodological section that specifies the nature of the data used and how they were processed.

The findings of this study are numerous and concern highly diverse aspects of business cybersecurity, but the main ones can be summarized as follows: between 2021 and 2023, Quebec businesses absorbed a doubling of incident costs and applied the new requirements of Law 25 by strengthening their governance through the systematic involvement of senior management, formal policies, or more frequent use of external experts. However, none of these mechanisms demonstrated a measurable effect on their cybersecurity. Moreover, the multivariate analyses are unequivocal: the only variable that consistently reduces victimization, recovery costs, and service interruptions is the presence of employees specialized in cybersecurity. Unfortunately, this is precisely the resource that is stagnating in Quebec. Quebec's cyber resilience therefore rests on an as-yet unresolved tension: the need to strengthen formal compliance with legislative requirements while increasing investments in specialized human capital whose availability is limited.

METHODOLOGY

This study is based on the two most recent waves of the Canadian Survey of Cyber Security and Cybercrime (CSCSC), conducted by Statistics Canada on behalf of Public Safety Canada.⁴ Administered through an electronic questionnaire to Canadian businesses with 10 or more employees, the CSCSC measures the incidence of the cyber risks faced by businesses as well as the practices implemented to prevent incidents and mitigate their consequences. The target population consists of businesses listed in Statistics Canada's Business Register, covering virtually all sectors defined under the North American Industry Classification System (NAICS 2022). The sample is stratified by industry and business size: small (10 to 49 employees), medium-sized (50 to 249 employees), and large (250 employees or more). The 2023 wave, for which data collection took place from January to March 2024 and covered the 2023 calendar year, was officially released on October 21, 2024. It includes approximately 12,000 businesses across Canada, including roughly 2,800 in Quebec, with a response rate of 71%. Calibration survey weights are associated with the data to produce estimates representative of the target population. Comparability between the 2021 and 2023 waves is ensured through the harmonization of sampling strata and imputation procedures, making it possible to attribute the documented changes to substantive developments rather than to survey design artifacts. The combination of a sample of this size, such a high response rate, and such rigorous methodological standards makes this survey one of the most reliable and representative sources worldwide on business cybersecurity.

The composition of the sample by business size is representative of the Quebec economy, and the very small differences observed result from the weighting applied during data extraction.



⁴ Adapted from Statistics Canada, *Canadian Survey of Cyber Security and Cybercrime (CSCSC)*, 2021 and 2023. This adaptation does not constitute an endorsement of this publication by Statistics Canada.

The analysis is structured into three sections. The first compares the practices reported by Quebec businesses and their evolution between 2021 and 2023 using contingency tables and Mann-Whitney tests for continuous variables. The second performs a similar comparison between Quebec and the rest of Canada for 2023. The third section presents multivariate analyses to assess the effect of risk management measures and practices on exposure to cyberattacks and recovery capabilities (speed of recovery and associated costs). These analyses rely on three binary logistic regression models for dichotomous variables (results expressed as odds ratios) and two generalized linear models with a Gamma distribution for continuous variables (results expressed as mean ratios), selected because of the asymmetric distribution of the latter.

The descriptive analyses presented in Sections 1 and 2 use the survey weights. The multivariate analyses in Section 3, conducted using the unweighted data, should be interpreted as associations observed within the sample rather than as estimates that can be generalized to the entire population.

Statistical analyses make it possible to determine whether a difference between two groups (such as Quebec businesses in 2021 and those in 2023) is genuine or simply due to chance. However, they do not, by themselves, indicate whether that difference is meaningful. In a survey covering tens of thousands of businesses, even a very small difference may be found to be statistically significant simply because the sample is very large. To distinguish what is statistically detectable from what is substantively meaningful, the results presented in this report are accompanied by a measure indicating the strength of the observed association—that is, the extent to which two variables vary together. These levels of association are based on eta squared (η^2), a measure commonly used in the social sciences to quantify the strength of statistical associations between categorical variables. This measure ranges from 0 to 1: the closer it is to 1, the stronger the relationship. Values close to 0 indicate that the two variables are essentially independent of one another. To facilitate interpretation, the resulting values are systematically translated into six levels of association strength, presented in the table below: negligible, weak, modest, moderate, strong, and very strong. These descriptors are used throughout the report to characterize the magnitude of the changes and differences documented.

Strength of Statistical Associations (η^2)
Negligible: $\eta^2 < 0.05$
Weak: $0.05 \leq \eta^2 < 0.10$
Modest: $0.10 \leq \eta^2 < 0.20$
Moderate: $0.20 \leq \eta^2 < 0.30$
Strong: $0.30 \leq \eta^2 < 0.45$

CHAPTER 1. EVOLUTION OF THE CYBERSECURITY POSTURE OF QUEBEC BUSINESSES BETWEEN 2021 AND 2023

Between 2021 and 2023, Quebec businesses operated in a digital environment reshaped by two concurrent developments: the intensification of financially motivated cyber threats, on the one hand, and the gradual implementation of Law 25, on the other. This dual context of escalating threats and a strengthening legislative framework provides the lens through which the data presented in the following sections should be interpreted. The changes observed in Quebec between the two waves of Statistics Canada's CSCSC must therefore distinguish what reflects a reactive adaptation to global threats from what reflects regulatory compliance driven by local legislative requirements, with both dynamics operating simultaneously.

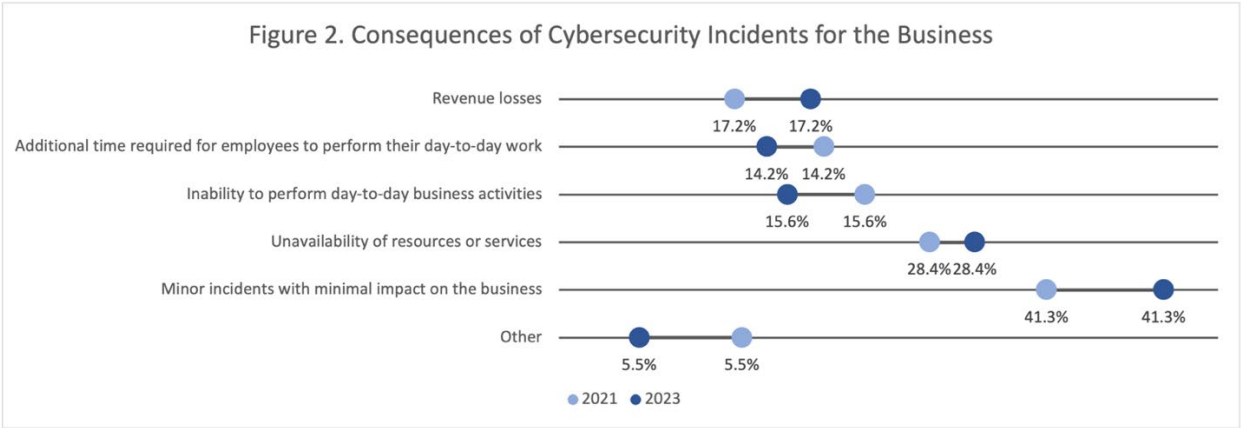
Profile of Cyberattacks Experienced

The proportion of Quebec businesses that experienced at least one cyber incident during the year remained remarkably stable between 2021 and 2023, decreasing slightly from 16.4% to 15.5%. This suggests a degree of equilibrium between the expansion of cyber threats and the gradual maturation of organizational cybersecurity practices. This apparent stability, however, conceals a profound shift in the types of incidents affecting businesses. The most significant change is the sharp increase in financially motivated attacks: the proportion of businesses targeted in attempts to steal money or demand a ransom rose from 19.8% in 2021 to 39.9% in 2023, an increase of 20.1 percentage points—the largest increase observed among all reported threat categories. Cybercriminals are therefore monetizing their attacks with increasing intensity. Conversely, cyber intrusions involving unauthorized or privileged access declined significantly, with the proportion of affected businesses falling from 22.6% to 11.2%. This reduction likely reflects progress in identity and access management, which recorded the largest increase among the technical cybersecurity measures adopted by businesses between the two survey waves. A slight decline was also observed in incidents involving the theft of personal or financial information (-2.3 percentage points, from 27.5% to 25.2%). Although this difference remains statistically modest, it is nevertheless consistent with the expected effects of Law 25 on preventing this type of breach, against which businesses now had a legal incentive to implement more robust protective measures. The remaining differences presented in Table 1 below are negligible and may be attributed to sample weighting.

Table 1. Evolution of the Types of Cybersecurity Incidents Affecting Quebec Businesses Between 2021 and 2023	
Increase	Decrease
- Steal money or demand a ransom (+20.1 percentage points) - Disrupt or deface the organization's web presence (+2.1 percentage points)	- Gain unauthorized or privileged access (-11.4 percentage points) - Other (-3.3 percentage points)

	- Steal personal or financial information (-2.3 percentage points) - No known motive (-1.8 percentage points)
--	---

The consequences experienced by businesses affected by cyberattacks, presented in Figure 2, paint a mixed picture between 2021 and 2023. Two types of operational disruption declined noticeably: the proportion of businesses that had to dedicate additional employee time to enable staff to perform their day-to-day tasks decreased from 18.1% to 14.2%, while the proportion of businesses whose employees were unable to perform their regular duties fell from 20.9% to 15.6%. These declines suggest that Quebec businesses are absorbing cyber incidents more effectively from an operational perspective. In addition, when businesses experienced disruptions affecting the availability of their resources or services, their average downtime was significantly shorter in 2023 than in 2021. At the same time, revenue losses increased from 12.0% to 17.2%, and incidents classified as minor, with minimal impact on the organization, rose from 33.3% to 41.3%. The stability observed in resource unavailability (25.3% to 28.4%, a statistically negligible difference), supplier or customer losses, and reputational damage completes this picture. Overall, cyberattacks in 2023 placed a greater burden on business finances than on operations or stakeholder relationships, which may be interpreted as an indication of increased cyber resilience among Quebec businesses.



This stability in post-incident impacts is nevertheless accompanied by a concerning economic reality. While the proportion of businesses that incurred recovery costs did not differ significantly between the two survey waves, the average costs borne by those affected more than doubled. Overall, total recovery costs in Quebec increased from \$122.5 million in 2021 to \$315 million in 2023, representing a 2.5-fold increase in just two years. This trend is not unique to Quebec: across Canada, total recovery costs rose from \$600 million to \$1.2 billion over the same period, confirming that the growing monetization of cyber threats is a structural trend. Law 25 may also have contributed to this increase in post-incident costs. Mandatory notification requirements for affected individuals and the Commission d'accès à l'information (CAI), the engagement of legal services, and the mitigation measures required under the regulatory framework all

increase recovery costs. While the available data do not allow the precise impact of these factors to be isolated, it would be imprudent to disregard their potential contribution.

Table 2. Evolution of Aggregate Post-Incident Recovery Costs Incurred by Quebec and Canadian Businesses Between 2021 and 2023		
	2021	2023
Canada	\$600 million	\$1.2 billion
Quebec	\$122.5 million	\$315 million

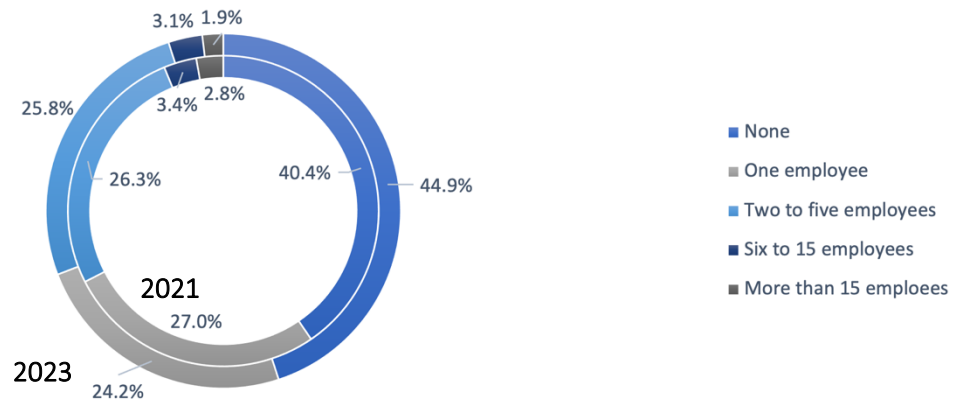
Overview of the Evolution of Cybersecurity Practices

While the previous section documented changes in the exposure of Quebec businesses to cyber threats, this section examines the other side of the equation: how these organizations evolved their defensive posture between 2021 and 2023. The objective is to distinguish changes that reflect a natural adaptation to an increasingly hostile threat landscape—such as investing more because cyber incidents have become more costly—from those that primarily reflect regulatory compliance driven by Law 25. These two dynamics are, of course, not mutually exclusive: they coexist and reinforce one another. However, analyzing them separately is essential for interpreting the long-term sustainability of the observed changes. Adaptations driven primarily by regulatory compliance may stabilize or even decline once legal obligations have been met, whereas deeper changes in organizational culture are more likely to endure. Three main categories of measures are examined: the cybersecurity expertise available within each organization, the implementation of security controls and risk management procedures, and the nature of interactions with external partners.

Cybersecurity Expertise Available In-House

The structure of the human resources dedicated to cybersecurity reveals a persistent tension between growing awareness of cyber risks and an organizational capacity that has been slow to keep pace. The first finding is particularly striking: in 2023, a larger proportion of Quebec businesses (44.9%, compared with 40.4% in 2021) reported having no employees dedicated to cybersecurity-related responsibilities (Figure 3). This means that a substantial share of Quebec's business community continues to face cyber threats without any specialized internal cybersecurity resources.

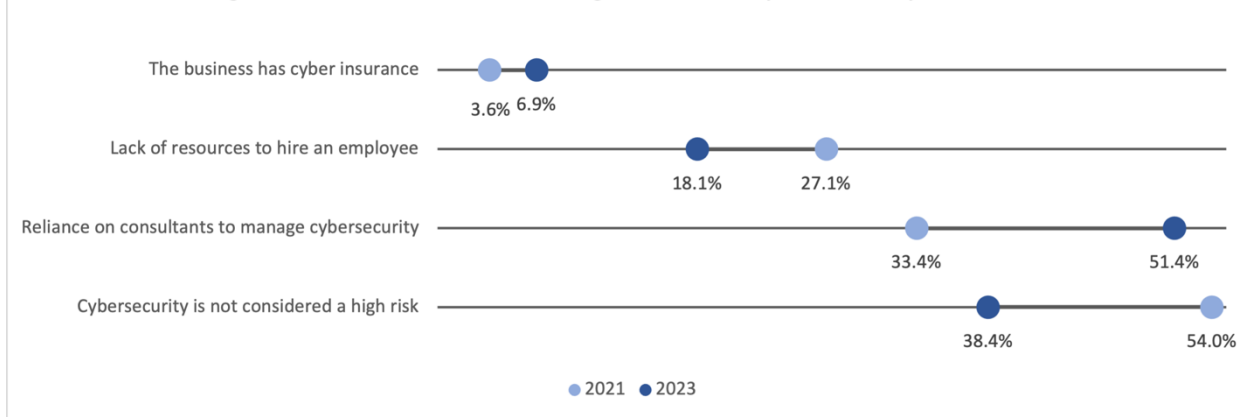
Figure 3. Number of Employees Dedicated to Cybersecurity



Businesses in this situation primarily justify their decision in three ways (Figure 4). First, more than one-third believe that cybersecurity does not represent a sufficiently significant risk to justify such an investment. Although this perception appears disconnected from the statistical reality, it is encouraging to note that this complacent position nevertheless declined by 15.6 percentage points between 2021 and 2023. Second, there was a nearly equivalent increase in the proportion of businesses attributing their lack of internal cybersecurity hiring to their reliance on external cybersecurity consulting and service providers, representing one of the most substantial changes observed in this section. Third, the proportion of businesses reporting that they lack the resources to hire a dedicated employee remains high at 18.1%. However, this justification declined by nine percentage points over the two-year period. The adoption of cyber insurance remains below the 10% threshold, although it increased substantially by 6.3 percentage points over the two years, reflecting a moral hazard effect whereby insured organizations alter their behaviour toward risk when they perceive themselves to be protected against potential losses.⁵

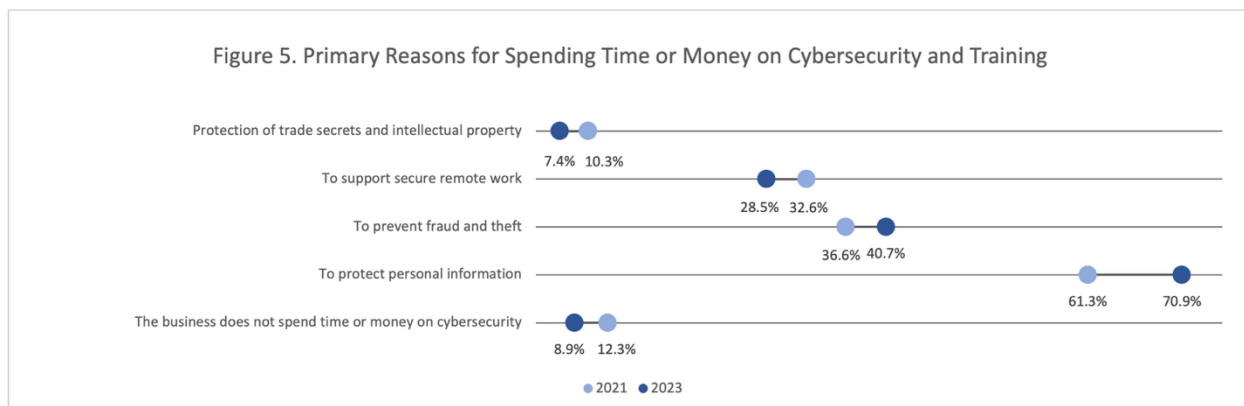
⁵ Steven Shavell (1979). "On Moral Hazard and Insurance." In Georges Dionne & Scott E. Harrington (Eds.), *Foundations of Insurance Economics*. Springer, Dordrecht, pp. 280–301.

Figure 4. Reasons for Not Hiring Dedicated Cybersecurity Personnel



While the recruitment of cybersecurity specialists appears to have stagnated, efforts to provide cybersecurity training to all employees increased from 11.8% in 2021 to 19.1% in 2023. Expressed relative to the 2021 baseline, this increase of 7.3 percentage points represents a 62% relative increase in the number of businesses that strengthened the cybersecurity competencies of their entire workforce. This finding is likely attributable, at least in part, to the obligations introduced by Law 25, whose provisions explicitly require organizations to implement and document employee training and awareness activities relating to the protection of personal information.

The relationship between legislative requirements and reported organizational behaviour is even more evident in the evolution of the motivations cited for cybersecurity spending. The proportion of businesses identifying the protection of employees', suppliers', customers', or partners' personal information as the primary reason for their cybersecurity investments increased from 61.3% to 70.9% between the two survey waves (Figure 5). This increase of 9.6 percentage points is one of the indicators most directly attributable to Law 25 among all the findings analyzed, reflecting the gradual incorporation of statutory privacy protection obligations into the cybersecurity investment strategies of Quebec organizations. Nevertheless, this interpretation should be approached with caution, since the Statistics Canada questionnaire did not include any questions specifically addressing Law 25. Differences between 2021 and 2023 were negligible with respect to motivations such as ensuring secure remote work, protecting the organization's reputation, avoiding downtime and IT outages, preventing fraud and theft, or ensuring business continuity. Likewise, only a negligible increase was observed in the proportion of Quebec businesses that invested in cybersecurity in response to experiencing a cyber incident.

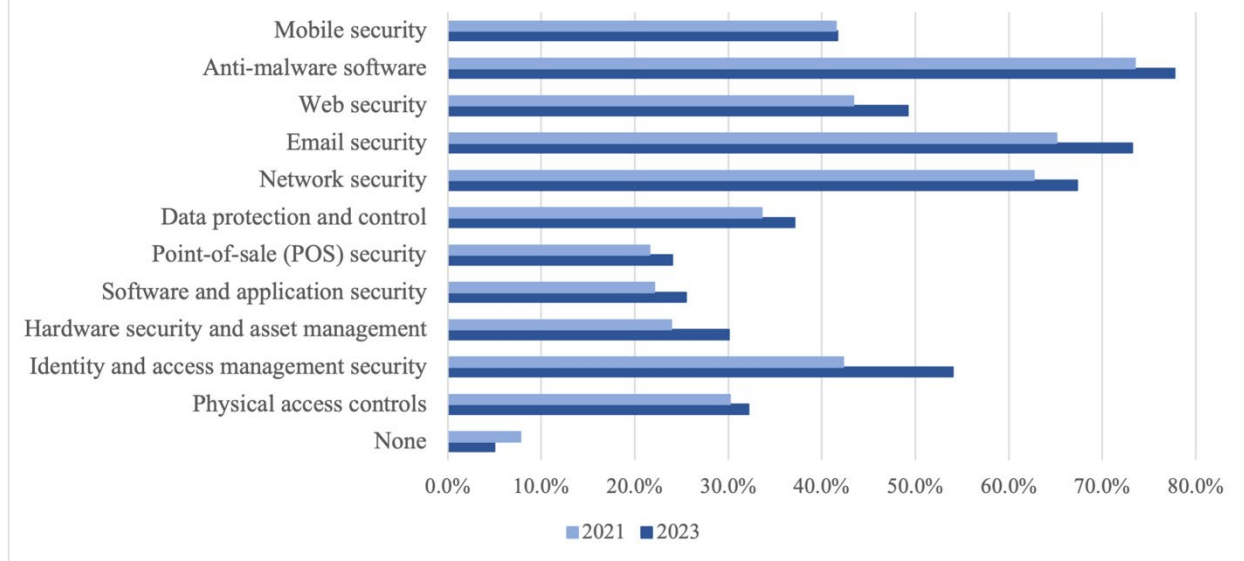


Technical Measures and Risk Management Activities

The practices examined in this section fall into two distinct categories. Technical measures—such as firewalls, encryption technologies, identity and access management solutions, and software patching—constitute the defensive layer deployed at the systems and network levels. They operate largely in an automated manner and serve as the first line of defence against cyberattacks. Risk management activities, by contrast—including formal risk assessments, written policies, the level of senior management involvement, business continuity planning, and disaster recovery planning—reflect an organizational and governance-oriented approach. While these activities do not directly protect information systems, they establish the framework within which security decisions are made, responsibilities are assigned, and resources are allocated.

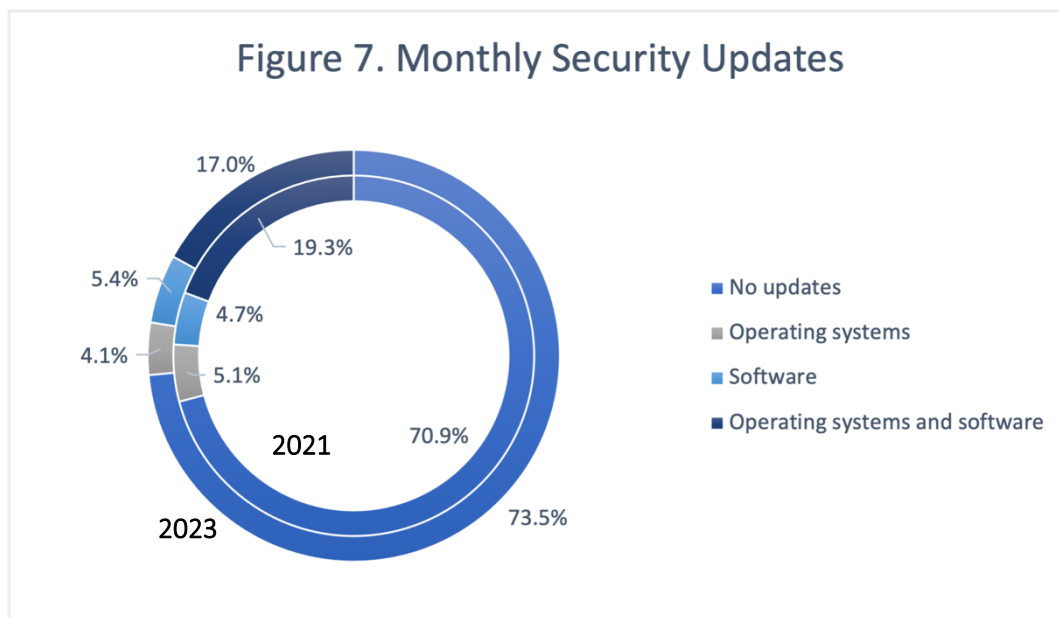
Looking first at the technical cybersecurity measures implemented by Quebec businesses (Figure 6), the overall picture is one of stability between 2021 and 2023, with virtually all observed differences being statistically negligible. Only identity and access management recorded a modest increase, a finding that appears consistent with the previously documented decline in incidents involving unauthorized access. Consequently, despite the intensification of cyber threats and the shift toward financially motivated attacks described earlier, the technical cybersecurity capabilities deployed by Quebec businesses remained virtually unchanged over the reference period.

Figure 6. Cybersecurity Measures Currently Implemented by Quebec Businesses

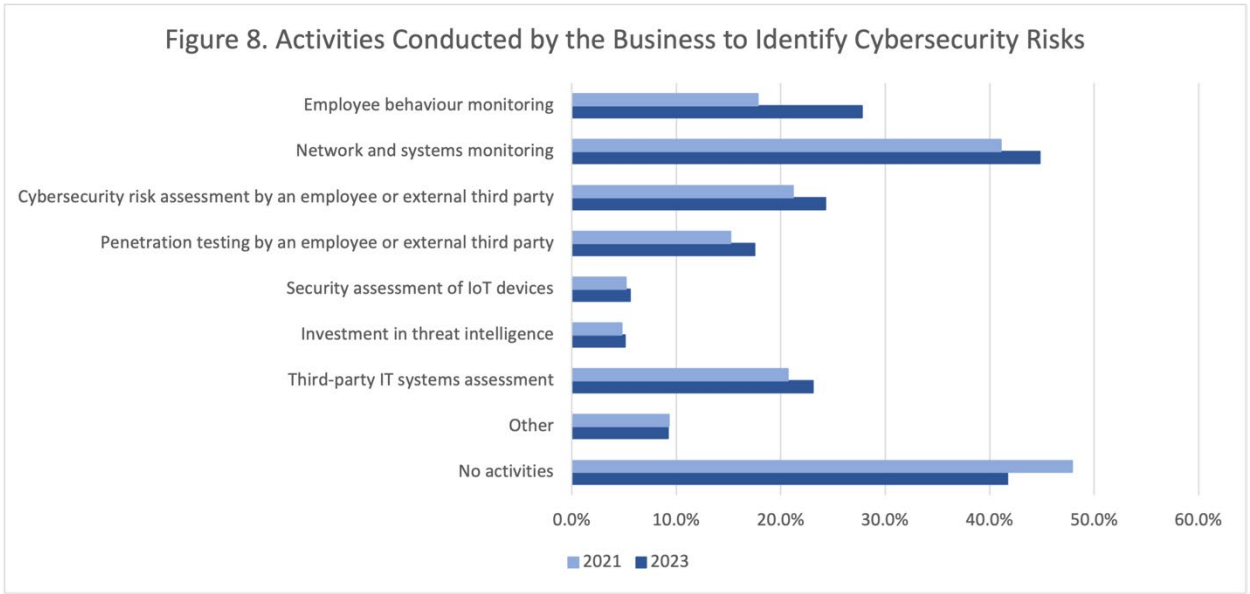


The application of monthly security patches and software updates is one of the most fundamental cyber resilience practices recommended by all major cybersecurity authorities. The findings are nevertheless concerning: more than 73% of Quebec businesses reported applying no security patches or updates on a monthly basis, a figure that remained unchanged between 2021 and 2023 (Figure 7). Neither the escalation of cyber threats, the implementation of Law 25, nor the increased professionalization observed in other dimensions of cybersecurity governance discussed later in this report has led to any measurable improvement in this area. This remains one of the most persistent vulnerabilities in the cybersecurity posture of Quebec businesses.

Figure 7. Monthly Security Updates

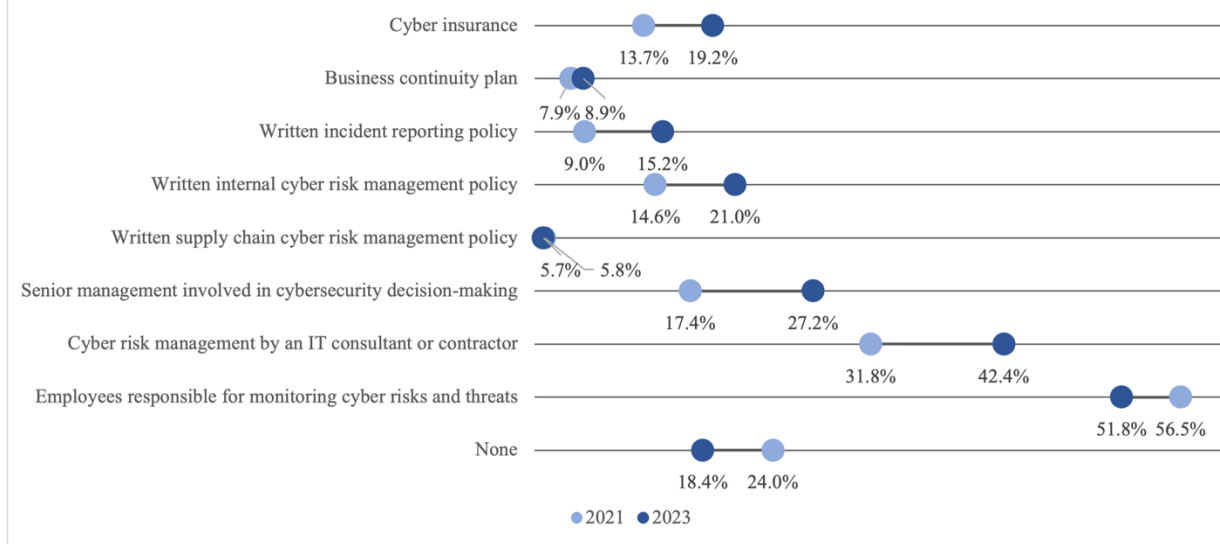


With respect to the activities undertaken to identify cybersecurity risks (Figure 8), all categories of activity increased in 2023. However, these increases were negligible across all categories except for employee behaviour monitoring, which recorded a moderate increase (+10 percentage points), likely reflecting greater awareness of the risks associated with insider threats. It is nevertheless concerning that approximately four out of ten Quebec businesses report conducting no activities whatsoever to identify the cybersecurity risks to which their systems are exposed. This figure remained stable between 2021 and 2023 and is difficult to dismiss. It indicates that a substantial portion of Quebec's business community continues to operate without any systematic assessment of its vulnerabilities, despite the fact that the financial costs of cyber incidents more than doubled over the same period.

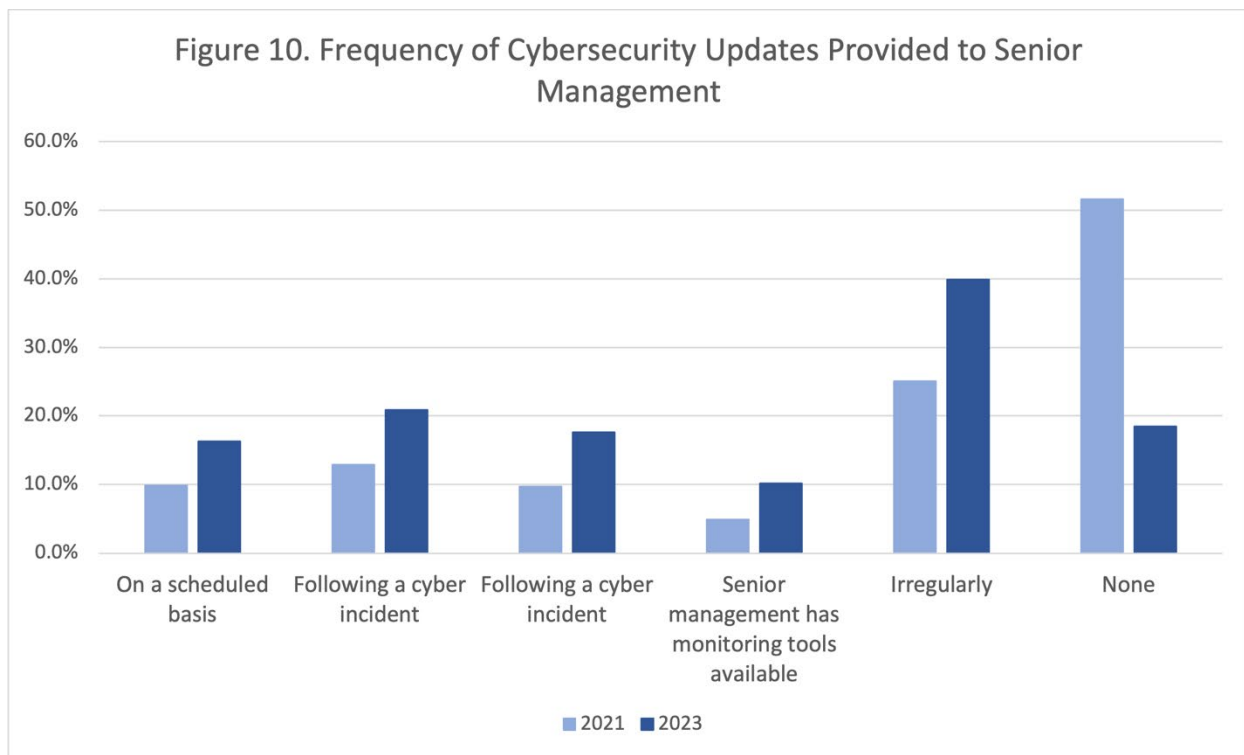


More encouragingly, formal risk management practices improved across most of the dimensions measured by the survey (Figure 9), reflecting, in practice, the governance requirements introduced by Law 25, which mandates the implementation of written policies, internal reporting procedures, and oversight mechanisms. Positive developments include greater senior management involvement in cyber risk decision-making (+9.8 percentage points) and increased reliance on external cybersecurity consultants (+10.6 percentage points), two dimensions that will be examined in greater detail later in this report. Two areas of persistent weakness should nevertheless be highlighted. First, business continuity planning and internal risk monitoring remained stable or declined between the two survey waves, leaving structural gaps that the incentives created by Law 25 have not been sufficient to address. Second, written supply chain cybersecurity risk management policies remain virtually nonexistent (5.8% in 2021 and 5.7% in 2023), representing a significant blind spot at a time when indirect attacks through suppliers and service providers have become an increasingly important vector for compromising information systems.

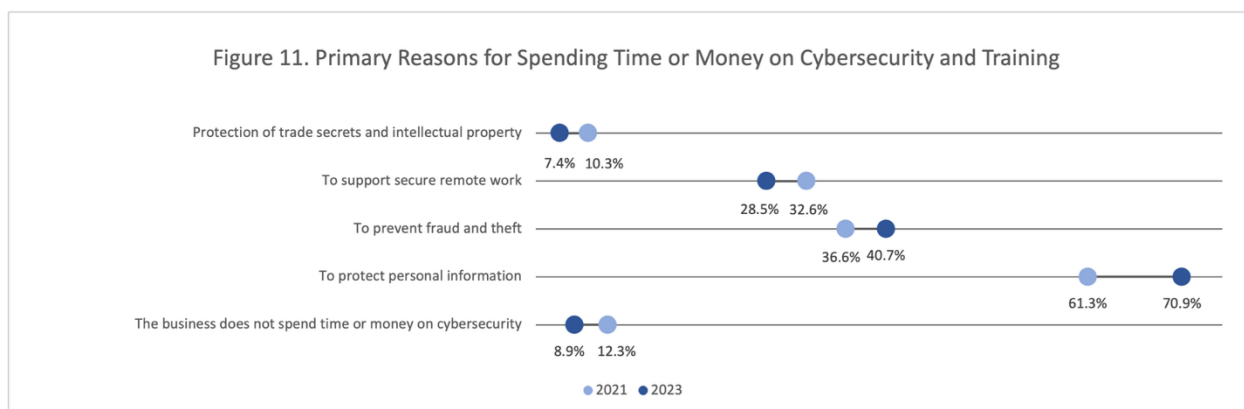
Figure 9. Cybersecurity Risk Management Measures Currently in Place



The most striking—and statistically significant—transformation observed between 2021 and 2023 concerns the increased involvement of senior leadership in cybersecurity governance. The proportion of Quebec businesses whose senior management received no cybersecurity updates fell dramatically from 51.6% to 18.5% between the two survey waves—a reduction of 33 percentage points, representing the strongest association observed in the entire analysis (Figure 10). In just two years, cybersecurity evolved from being a technical issue delegated to IT teams into a core governance concern falling within the responsibility of the highest decision-making bodies of Quebec businesses. This major shift is not coincidental. Law 25 explicitly assigns responsibility for the protection of personal information to the individual with the highest authority within the organization, thereby creating a powerful institutional incentive for cybersecurity-related information to be escalated to senior leadership.

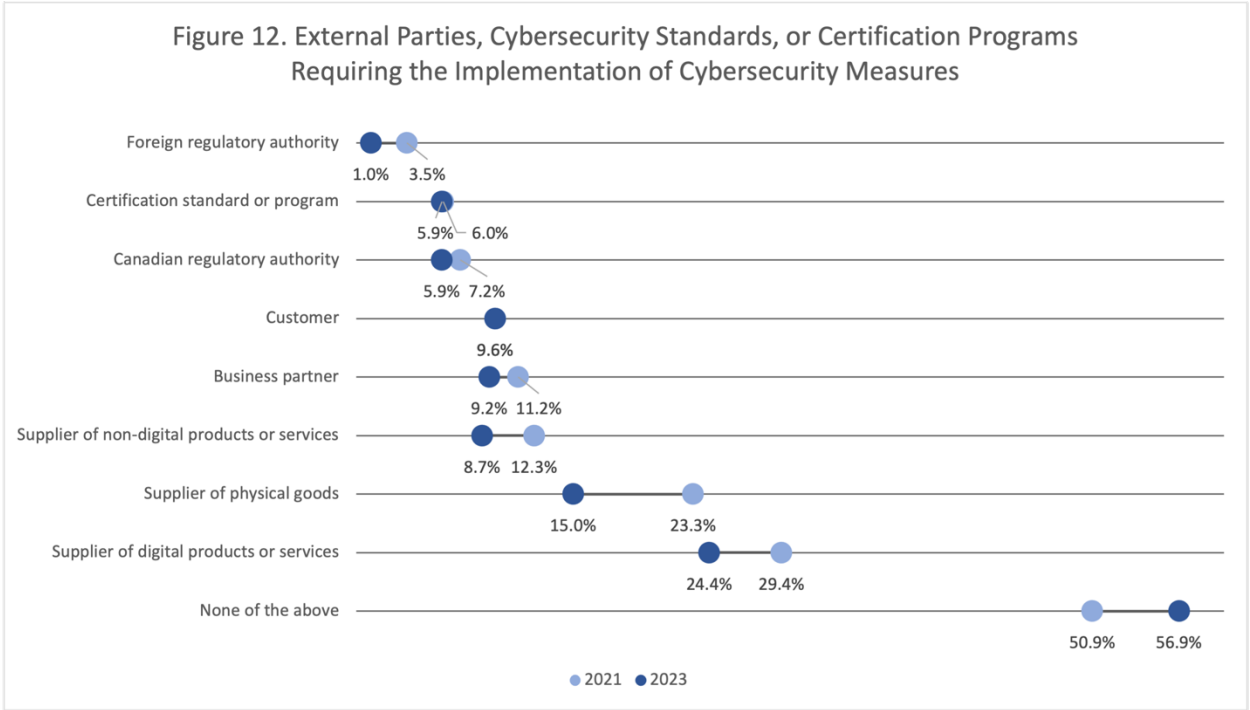


The effects of Law 25 are not limited to the accountability structure surrounding cybersecurity. They also influence the motivations underlying cybersecurity investment decisions. While the legislation prompted businesses to increase reporting to senior management, it also reinforced the protection of personal information as the primary reason organizations devote time and financial resources to cybersecurity, well ahead of fraud and theft prevention (Figure 11).



The changes documented thus far—particularly the strengthening of reporting to senior management and the evolution of the stated motivations for cybersecurity spending—primarily reflect internal dynamics driven by the regulatory pressure created by Law 25. However, an organization's cybersecurity posture is not shaped solely from within. Suppliers, customers, certification bodies, and regulatory authorities all represent sources of external pressure that may require or encourage the implementation of cybersecurity

measures and risk management practices that organizations might not otherwise have adopted on their own initiative. This is illustrated in Figure 12, which shows no difference between 2021 and 2023 with respect to cybersecurity requirements imposed by customers (9.6% in both survey waves) and no significant difference in requirements imposed by Canadian regulatory authorities (6.0% in 2021 versus 5.9% in 2023). Only statistically negligible differences were observed for measures required under certification standards or programs (7.2% in 2021 versus 5.9% in 2023) and by business partners (11.2% in 2021 versus 9.2% in 2023). For the remaining categories of external stakeholders, requests for the implementation of cybersecurity measures declined slightly or modestly among Quebec businesses.



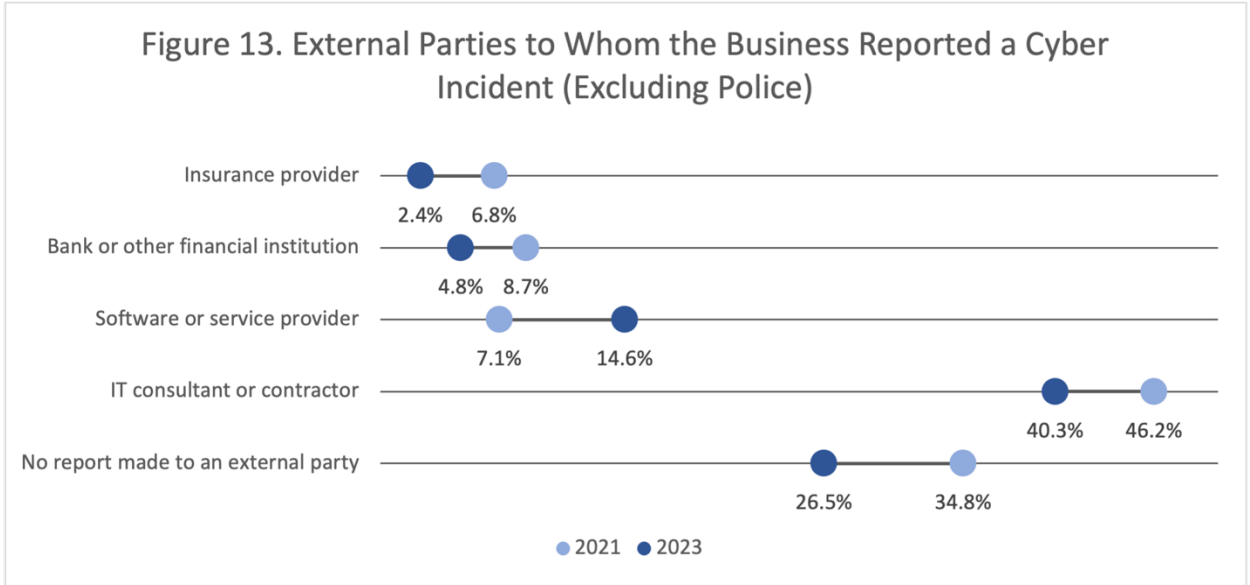
This modest decline in external stakeholder requirements can be interpreted in two ways: either Quebec businesses have improved their cybersecurity posture sufficiently for such requests to have become largely redundant, or the minimum level of compliance expected is now embedded across organizations—particularly following the strengthening of the regulatory framework—and therefore no longer needs to be explicitly requested. Unfortunately, the data analyzed here do not make it possible to distinguish between these two explanations.

Relationships with External Partners and Responses to Cyberattacks

The previous sections documented substantial improvements in the internal cybersecurity posture of Quebec businesses between 2021 and 2023, including stronger governance and a greater emphasis on the protection of personal information as a driver of cybersecurity investment. Cyber resilience, however, cannot be achieved solely through internal organizational efforts. It also depends on an organization's ability to mobilize external resources—such as law enforcement agencies, insurers, regulatory authorities, and cyber threat intelligence-sharing communities—and to contribute to the collective response to cyber

threats by reporting incidents. This is precisely the area where Law 25 was expected to have its most significant structural impact. By requiring Quebec organizations to formally notify the Commission d'accès à l'information (CAI) and affected individuals of privacy breaches, the legislation sought to reduce the temptation to resolve incidents quietly and to institutionalize a culture of transparency. The findings presented in this section invite an assessment of the gap between that legislative ambition and the behaviours actually observed in 2023. They examine, in turn, the consultation practices adopted by Quebec businesses following cyberattacks, their reporting practices to external stakeholders, and the reasons cited for choosing not to report incidents. These findings warrant a critical interpretation. Whereas the previous sections revealed increasing organizational maturity, the analysis of relationships with external partners points to the opposite trend—a measured but consistent shift toward the internal and discreet management of cyber incidents, with implications for cyber resilience that deserve serious consideration.

First, among businesses responding to a cyberattack, Figure 13 shows a clear decline in the reporting of incidents to external third parties (excluding police). Reporting to cyber insurance providers declined significantly, despite the growing adoption of cyber insurance policies over the same period. This divergence suggests that businesses are compartmentalizing their relationship with insurers by purchasing coverage without necessarily initiating claims or notification procedures. Such behaviour may reflect growing disillusionment with cyber insurance as a risk management tool or a more selective use of its benefits. Reporting to Canadian government departments and regulatory authorities also remained at very low levels. While this finding appears inconsistent with the notification obligations introduced by Law 25, it may be explained by the wording of the survey question, which refers to authorities at the national level.



The decline in reporting incidents to external partners is primarily driven by businesses' reluctance to devote additional time or financial resources to incidents that are already placing considerable strain on their operations. This reason for not reporting increased from 6.6% in 2021 to 37.9% in 2023 (Table 3). At

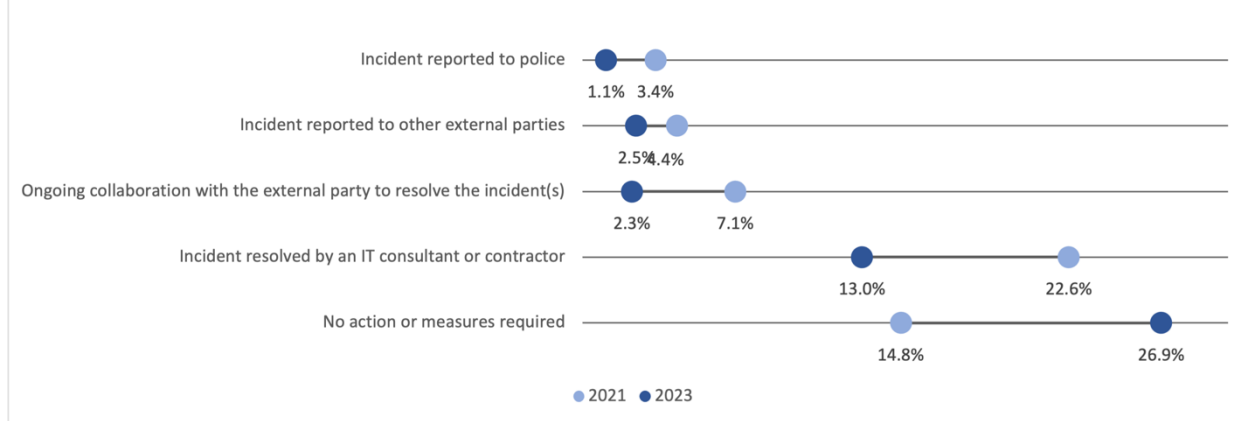
the same time, the proportion of businesses indicating that there was "no benefit or obligation to report" increased from 14.3% to 22.4% (+8.1 percentage points). Together, these two indicators point to the same conclusion: Quebec businesses are increasingly favouring the internal resolution of cyber incidents and are becoming less likely to view external reporting as either useful or necessary. This finding is particularly concerning because it appears to run counter to the objectives of Law 25, which was specifically intended to formalize incident reporting obligations—particularly to the Commission d'accès à l'information (CAI)—and to reduce the tendency to resolve incidents without external disclosure. The 2023 data suggest that, midway through the phased implementation of the legislation, this intended normative effect has not yet translated into reported organizational behaviour. Businesses are absorbing the growing costs of cyber incidents without increasing their participation in information-sharing initiatives or in the exchange of lessons learned.

Table 3. Reasons for Not Reporting Some or All Cyber Incidents to an External Third Party	
Increase	Decrease
• No willingness to devote additional time or money (+31.3 percentage points) • No benefit or obligation to report (+8.1 percentage points) • Incident reported only to a police service (+2.2 percentage points) • Had not considered reporting (+1.7 percentage points)	• Incident was minor with minimal impact (-34.5 percentage points) • To protect the organization's reputation (-1.8 percentage points) • Lack of evidence (-0.9 percentage points)

The growing reluctance to report their own cyber incidents is accompanied by a similar response to incidents reported by external partners. The proportion of businesses taking no action in response to an incident reported by a supplier or business partner increased from 14.8% to 26.9% between 2021 and 2023 (Figure 14). Conversely, collaborative response efforts involving external partners and the use of external consultants both declined modestly. This inward shift is consistent with the increase in non-reporting observed earlier. Quebec businesses therefore appear to be adopting a more internalized and discreet approach to incident management, whether dealing with their own cyber incidents or with those reported by third parties. In doing so, they weaken the cooperation and information-sharing mechanisms that form the foundation of collective cyber resilience.⁶

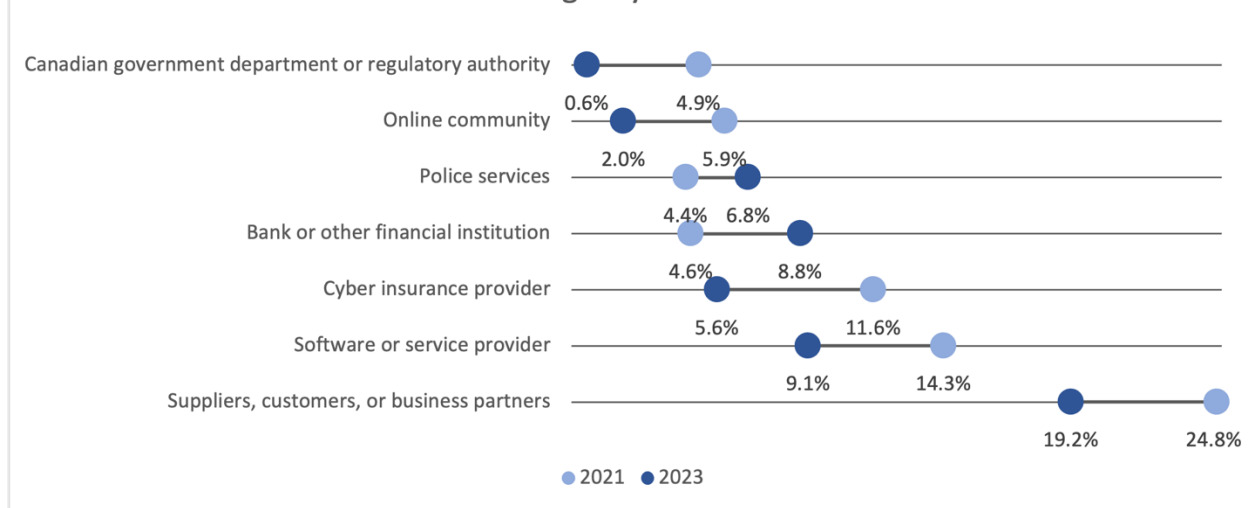
⁶ Benoît Dupont, Clifford Shearing, Maxime Bernier, & Rutger Leukfeldt (2023). "The Tensions of Cyber-Resilience: From Sensemaking to Practice." *Computers & Security*, 132, 1–17.

Figure 14. Business Responses to Incident(s) Reported by External Partners



Once an incident has been detected and is being managed, consultation patterns with external stakeholders closely mirror the shift in the threat landscape documented in the first section (Figure 15). The increased consultation of law enforcement agencies and financial institutions—the two categories of external partners whose assistance businesses sought more frequently in 2023 than in 2021—directly reflects the growing prevalence of financially motivated cyberattacks. Incidents involving the theft of funds or ransomware naturally require specialized expertise in financial crime and criminal investigations. Conversely, reliance on insurers declined markedly, falling from 11.6% to 5.6%. The most striking finding, however, is the collapse in consultations with Canadian government departments and regulatory authorities following a cyber incident, declining from 4.9% in 2021 to 0.6% in 2023—a relative decrease of 88%. In a context where Law 25 was specifically intended to increase the transparency of Quebec organizations toward data protection authorities, this decline represents a troubling paradox.

Figure 15. External Parties Consulted for Information or Advice Following a Cyber Incident



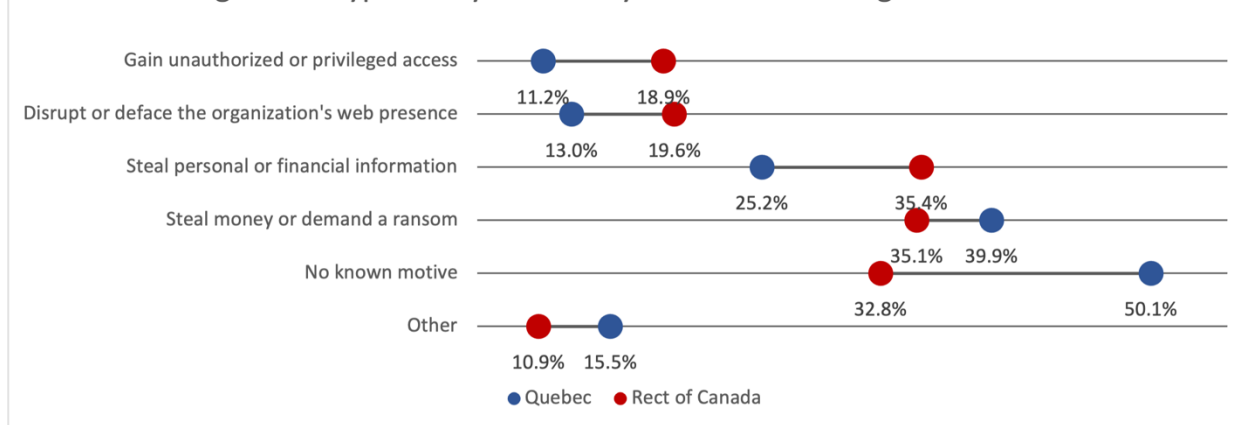
CHAPTER 2. THE CYBERSECURITY POSTURE OF QUEBEC BUSINESSES IN THE CANADIAN CONTEXT

Comparing the practices and experiences of Quebec businesses with those of businesses in the rest of Canada using the 2023 wave of the survey reveals a nuanced picture: overall victimization rates and recovery costs are broadly comparable across the country, while incident profiles, governance models, and reporting behaviours differ in measurable ways. These differences reflect distinct organizational, cultural, and regulatory environments, foremost among them the implementation of Law 25, whose effects are evident across several dimensions of Quebec's cybersecurity posture—sometimes in expected ways, and sometimes in ways that are more counterintuitive.

Comparative Victimization

The difference in exposure to cyberattacks between Quebec businesses and businesses in the rest of Canada is negligible. In 2023, 15.5% of Quebec businesses experienced a cyber incident, compared with 16.3% of businesses elsewhere in Canada. The distribution of incident types nevertheless reveals distinct victimization profiles between Quebec and the rest of Canada (Figure 16). The most striking finding concerns incidents reported as having "no known motive," which were reported by 50.1% of victimized Quebec businesses, compared with 32.8% in the rest of Canada. This 17-percentage-point difference represents the strongest association observed in this comparative chapter with respect to incident types. Two complementary explanations may account for this higher proportion in Quebec. The first relates to a deficit in internal analytical capabilities: Quebec businesses may have fewer tools or less in-house expertise to attribute and classify the cyber incidents they experience. The second, more structural explanation, is that Quebec businesses may be disproportionately affected by opportunistic or relatively unsophisticated attacks, which are inherently more difficult to classify within a specific incident category. Both hypotheses warrant further investigation. Conversely, businesses in the rest of Canada are more frequently targeted by incidents involving the theft of personal or financial information (35.4%, compared with 25.2% in Quebec) and by unauthorized or privileged access intrusions (18.9%, compared with 11.2% in Quebec). These types of attacks generally require a higher degree of sophistication and prior knowledge of the architecture of the targeted information systems. Finally, the proportion of incidents involving attempts to steal money or demand a ransom is comparable between the two subgroups and remains one of the most common forms of cyber incident.

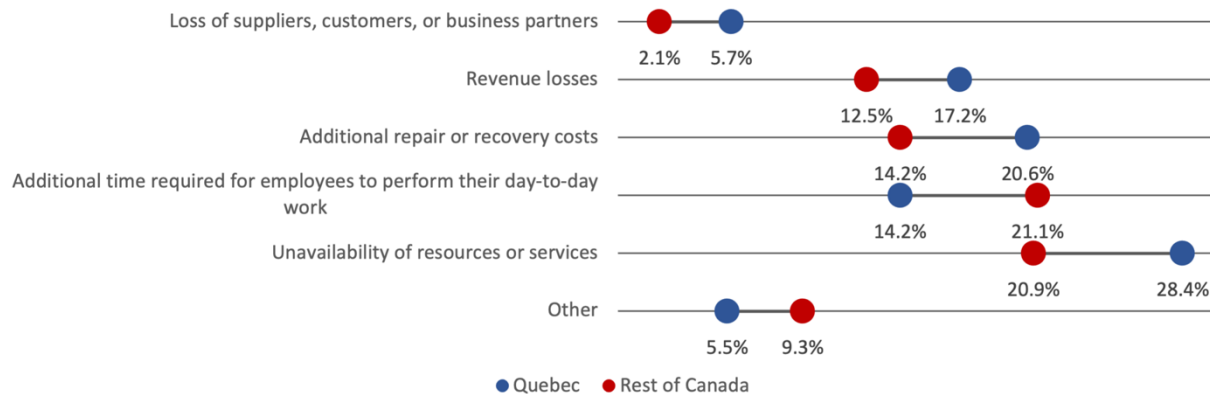
Figure 16. Types of Cybersecurity Incidents Affecting the Business



With respect to recovery costs, the comparison between Quebec and the rest of Canada yields a noteworthy finding. Despite differences in incident reporting behaviour—businesses in the rest of Canada being proportionally more likely not to contact any external third party, while Quebec businesses, when choosing not to report an incident, are far more likely to cite a desire to handle the incident internally (8.4% versus 1.8%)—the total costs incurred to recover from cybersecurity incidents do not differ significantly between the two groups. A slightly higher proportion of Quebec businesses reported incurring recovery costs, but the average level of those costs is comparable across both jurisdictions. This finding indicates that these different incident management strategies generate neither measurable savings nor additional costs. Economic considerations alone therefore cannot justify a shift toward more systematic incident reporting. Instead, the rationale for encouraging greater reporting should rest on its collective value in supporting cyber threat intelligence sharing and strengthening the broader cybersecurity ecosystem. With the exception of the statistically weak differences presented in Figure 17, the remaining consequences are either not statistically significant or statistically negligible.⁷

⁷ Not statistically significant: Damage to the organization's reputation; data tampering or data theft. Statistically negligible: Employees being unable to perform their day-to-day duties; minor incidents having minimal impact on the organization; theft of or compromise to software or hardware integrity; and the obligation to notify external parties of a security breach.

Figure 17. Consequences of Cybersecurity Incidents for the Business

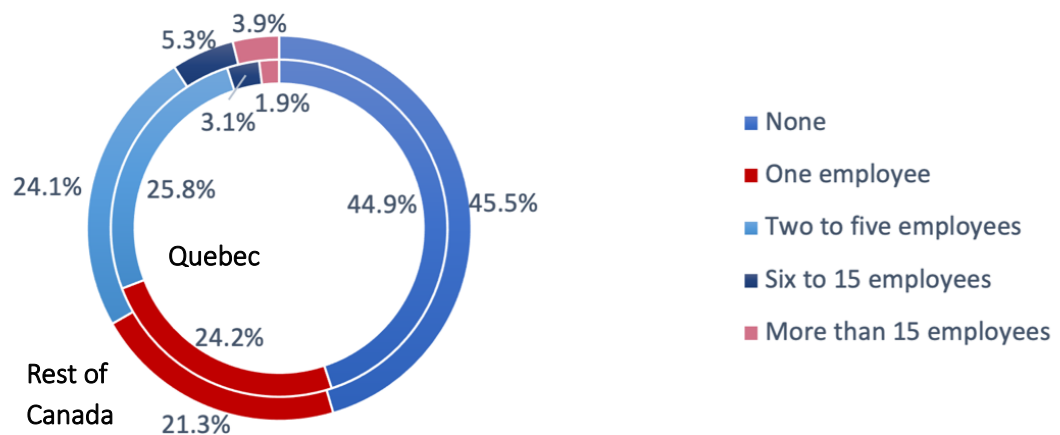


Cybersecurity Measures and Practices

Cybersecurity Specialists and Recruitment

The differences relating to the number of employees dedicated to cybersecurity are all negligible. As shown in Figure 18, nearly half of businesses in the rest of Canada reported having no employees dedicated to cybersecurity-related responsibilities, extending the pattern previously observed among Quebec businesses in the preceding section.

Figure 18. Number of Employees Dedicated to Cybersecurity



The reasons provided to explain this situation are likewise similar across Canada (Figure 19). All observed differences are statistically negligible, with the exception of the use of public sector consultants or contractors, which nevertheless remains a relatively uncommon practice.



Challenges related to specialized cybersecurity talent represent one of the most pronounced distinctions between Quebec and the rest of Canada, although the strength of the association remains modest. While nearly half of businesses elsewhere in Canada report experiencing no difficulty recruiting or retaining qualified cybersecurity personnel, this proportion falls to 29.5% in Quebec (Figure 20). This gap of approximately 20 percentage points reflects a more constrained labour market within the province. The shortage of qualified cybersecurity professionals is consistent with the greater reliance observed among Quebec businesses on external cybersecurity consultants and contractors for cyber risk management. Faced with difficulties recruiting and retaining in-house expertise, Quebec organizations increasingly turn to outsourcing. Law 25 has likely reinforced this trend by introducing governance requirements that many organizations cannot satisfy without access to specialized external expertise.

Figure 20. Difficulties Finding or Retaining Specialized Cybersecurity Personnel

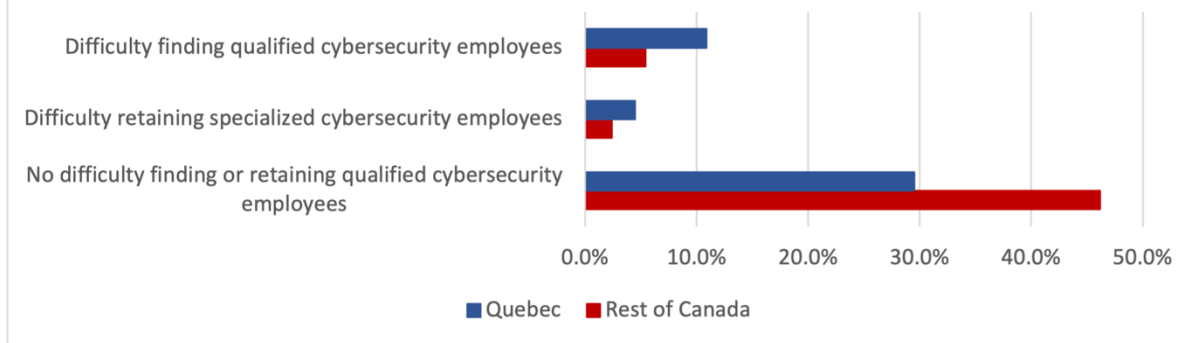
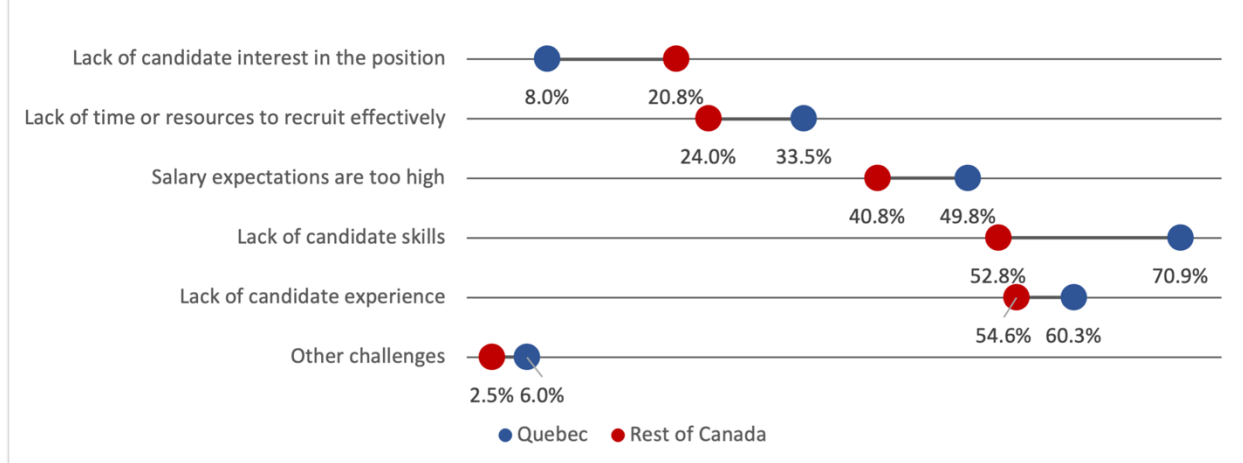


Figure 21 further suggests that Quebec's challenge is not simply quantitative but qualitatively different from that of the rest of Canada. By far the most frequently cited obstacle among Quebec businesses is the lack of qualified candidates, identified by 70.9% of respondents, compared with 52.8% elsewhere in Canada. This 18-percentage-point difference represents the largest gap observed for this question. Employers in Quebec are also more likely to report that salary expectations are too high (49.8% versus 40.8%) and that they lack the time or resources to recruit effectively (33.5% versus 24.0%), further illustrating the pressures affecting the provincial labour market. Conversely, a lack of candidate interest is cited far less frequently in Quebec than in the rest of Canada (8.0% versus 20.8%), suggesting that qualified applicants are not absent from the Quebec labour market, but rather that they often do not possess the skills employers are seeking.

Figure 21. Challenges Encountered When Hiring Specialized Cybersecurity Personnel



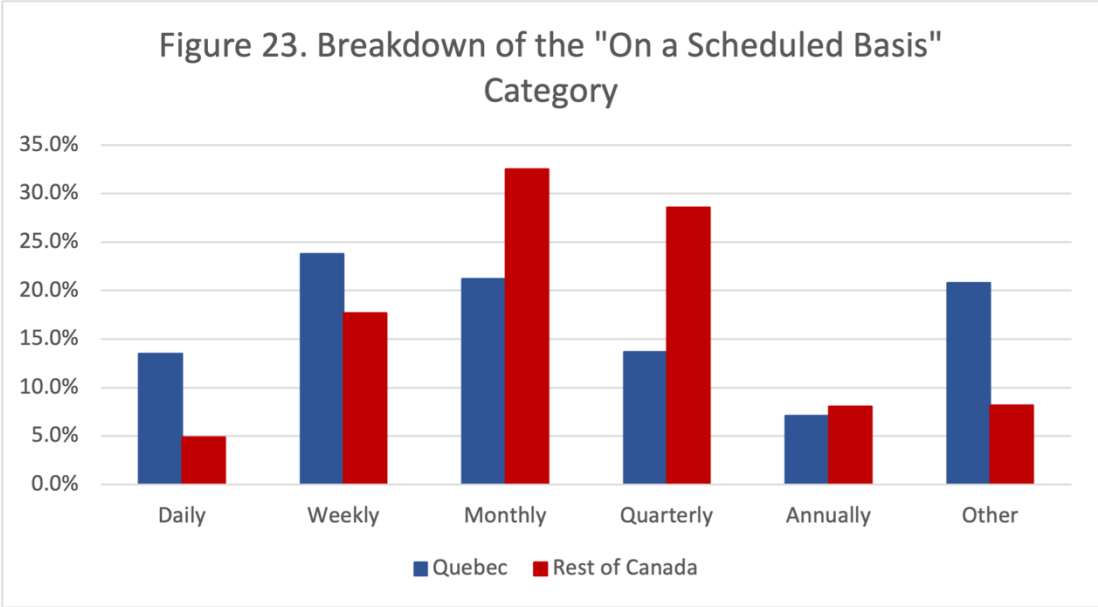
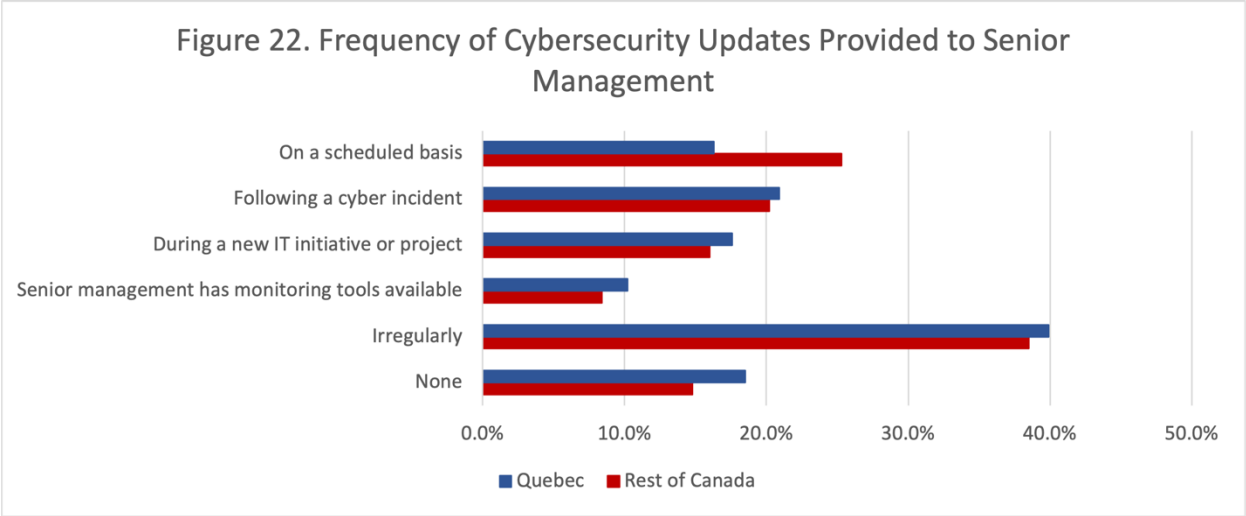
Organization-Wide Cybersecurity Awareness: Quebec Lags Behind

One of the most significant differences between Quebec and the rest of Canada concerns neither victimization nor the technical security measures implemented, but rather the internal dissemination of cybersecurity awareness. In 2023, 58.4% of businesses elsewhere in Canada reported communicating cybersecurity best practices or general cyber risk information to all employees, compared with only 46.9% of businesses in Quebec. This statistically significant difference of 11.5 percentage points indicates that more than half of Quebec businesses have yet to provide organization-wide cybersecurity awareness to their entire workforce.

This finding is significant for several reasons. First, it suggests that Quebec businesses may be concentrating their efforts more heavily on technical teams and senior leadership—a pattern consistent with the substantial increase in cybersecurity reporting to senior management documented in the 2023 survey wave—at the expense of fostering a broader organizational culture of vigilance. Second, it contrasts with the relatively high level of preparedness reported by Quebec businesses. Feeling better prepared than one's counterparts while providing less systematic cybersecurity awareness training to employees points to a gap between perception and practice that warrants further examination. Finally, in the context of Law 25, whose training and awareness requirements were specifically intended to broaden the dissemination of sound privacy and cybersecurity practices throughout organizations, this disparity suggests that compliance efforts remain unevenly distributed across Quebec's business community.

Frequency and Regularity of Reporting to Senior Management: Two Distinct Governance Profiles

The comparison of reporting frequencies to senior management reveals two fundamentally different governance approaches, whose interpretation requires going beyond a simple assessment of whether reporting is more or less frequent (Figures 22 and 23). Businesses in the rest of Canada favour institutionalized reporting routines: 32.5% provide monthly cybersecurity updates (compared with 21.2% in Quebec), while 28.6% report quarterly (compared with 13.7% in Quebec). These scheduled reporting cycles are embedded within established organizational governance processes. Quebec businesses exhibit the opposite profile, with a greater reliance on daily reporting (13.5% versus 4.9%) and ad hoc or "other" reporting schedules (20.8% versus 8.2%). These findings suggest a more reactive governance model: senior leaders in Quebec are consulted more frequently, but according to less formalized reporting cycles. Law 25 is likely one factor contributing to this increased level of executive engagement. By assigning responsibility for the protection of personal information to the individual with the highest authority within the organization, the legislation creates an institutional demand for more sustained executive oversight. However, it does not, by itself, explain the irregular nature of these reporting practices. Further research into the factors underlying these differences would be valuable.



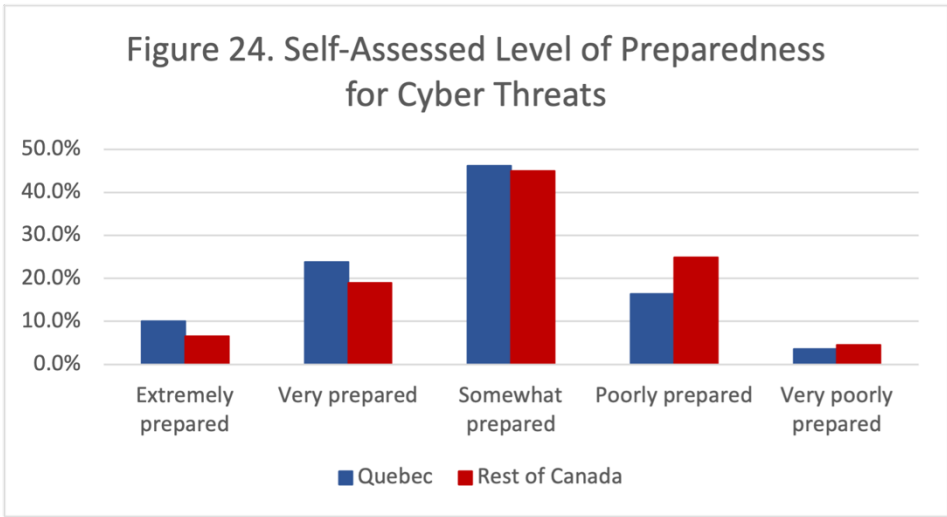
Self-Assessment of Preparedness and the Risk of Overconfidence

Figure 24 invites a comparison between Quebec businesses' perceptions of their own preparedness and the objective indicators of cybersecurity practices documented throughout this report. Quebec businesses consistently report feeling better prepared to respond to cyber threats than their counterparts elsewhere in Canada.

However, none of the practice-based indicators examined in this section supports this confidence. Quebec businesses communicate cybersecurity best practices less broadly across their workforce, experience greater difficulty recruiting specialized cybersecurity personnel, and deploy technical security measures and risk management practices that are broadly comparable to those observed elsewhere in Canada, without any measurable advantage. Although senior management involvement is considerably greater in

Quebec, it is unlikely, in the broader context examined here, that this factor alone materially improves operational capabilities for detecting and responding to cyber incidents.

This disconnect between perceived preparedness and observed practices is a well-documented phenomenon in the organizational security culture literature and is not without consequences. Organizations that overestimate their preparedness are generally less likely to invest in the areas where they are genuinely vulnerable and are less responsive to the warning signs that often precede cybersecurity incidents. In this respect, the Quebec paradox of perceived preparedness constitutes one of the most concerning findings to emerge from this comparative analysis.



Risk Management and Internal Measures

Across the remaining dimensions examined in this section—including the technical security measures deployed at the systems and network levels (Figure 25), cybersecurity risk identification activities, and risk management practices (Figures 26 and 27)—Quebec businesses and those in the rest of Canada exhibit broadly similar profiles. A few isolated differences remain, particularly with respect to the motivations cited for cybersecurity investments, where the protection of personal information and the prevention of fraud are more frequently identified by Quebec businesses (Figure 28), likely reflecting the influence of Law 25. Quebec businesses also lag slightly behind the rest of Canada on certain technical security measures. These differences, however, are of weak magnitude and do not reflect structural divergences comparable to those documented in the preceding subsections. This convergence is itself informative. It indicates that the Quebec-specific characteristics identified in this report—such as lower levels of organization-wide cybersecurity awareness, a more reactive governance model, and greater recruitment challenges—do not reflect a generalized gap across all cybersecurity practices. Rather, they represent targeted areas of weakness within a cybersecurity posture that, across most measurable dimensions, remains broadly aligned with that of businesses elsewhere in Canada.

Figure 25. Cybersecurity Measures Currently Implemented by the Business

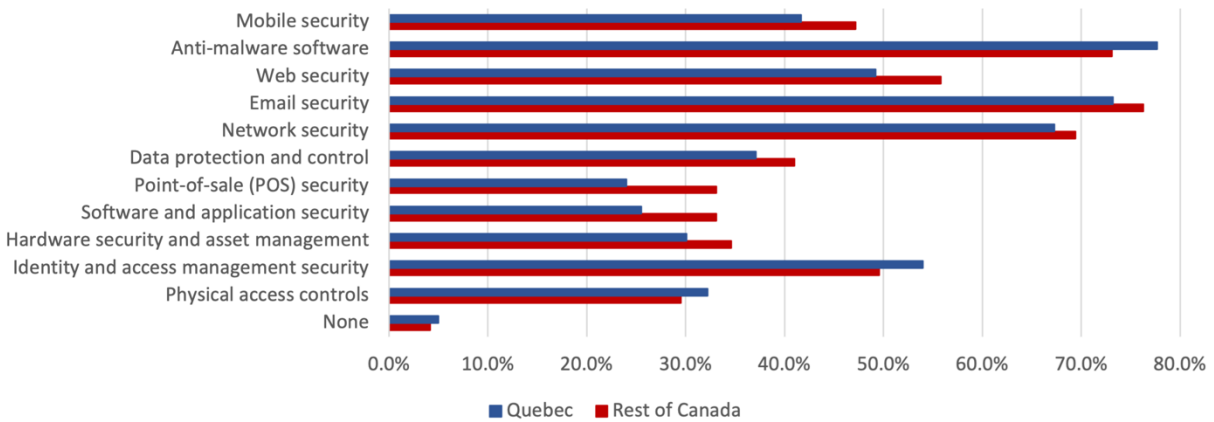


Figure 26. Activities Conducted by the Business to Identify Cybersecurity Risks

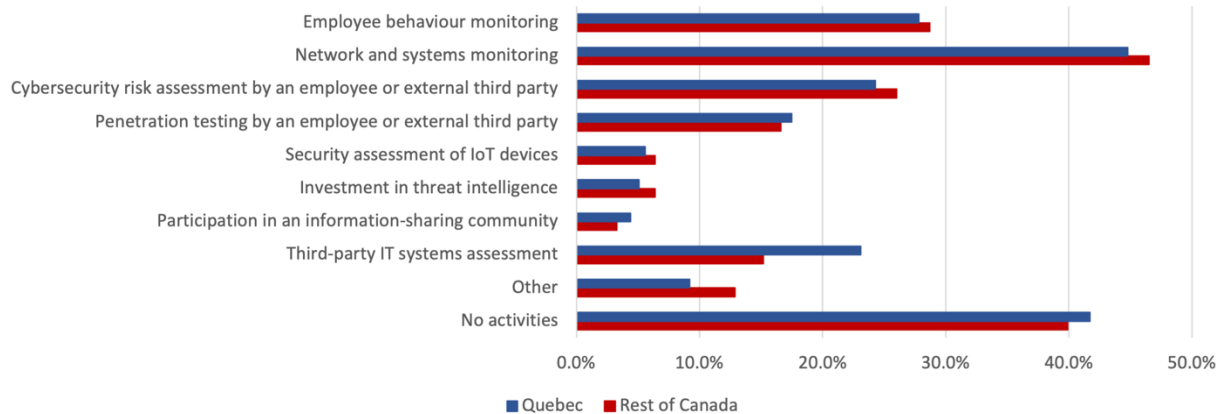
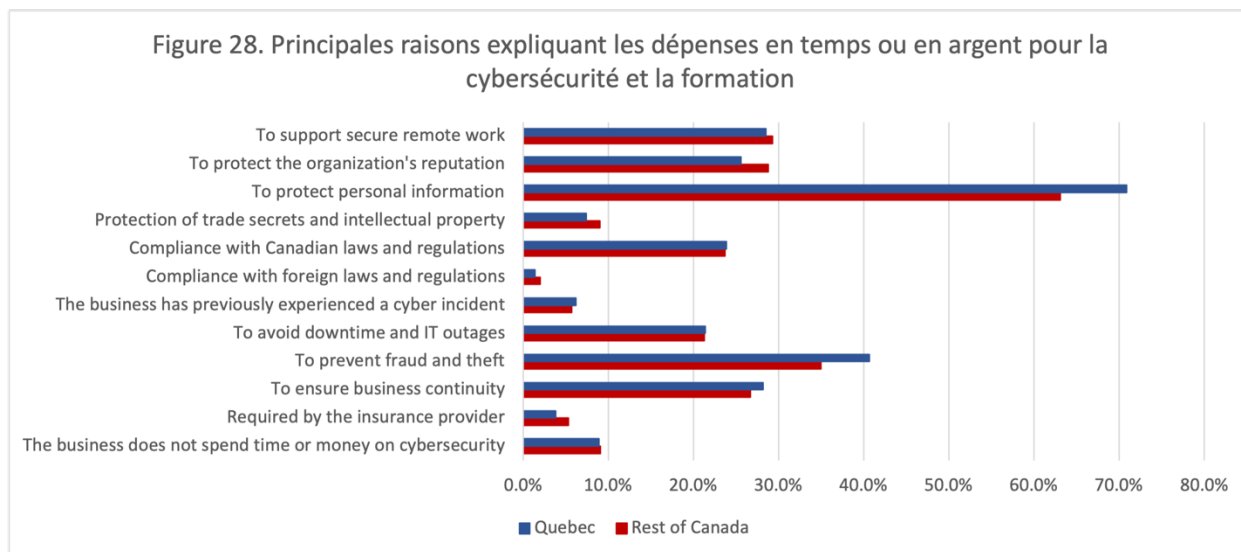


Figure 27. Cybersecurity Risk Management Measures Currently in Place

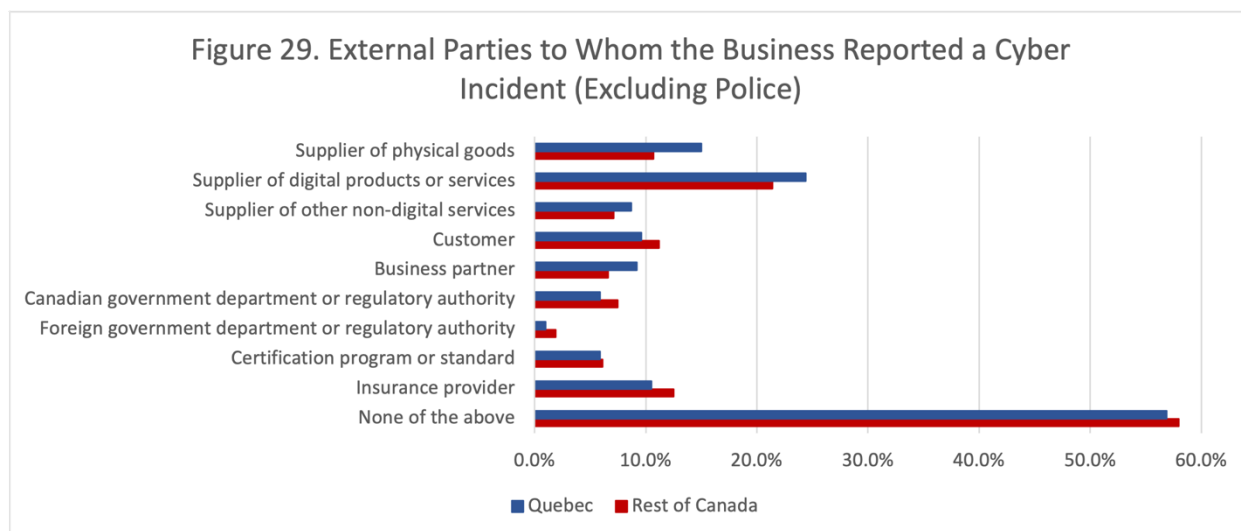




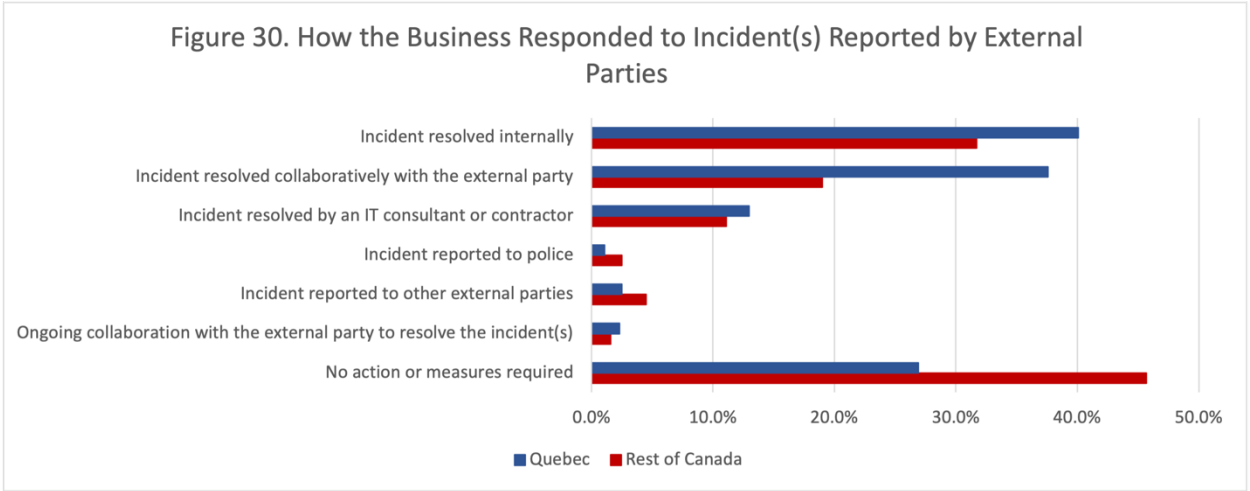
Collaboration and Partnership Practices

The comparison of collaborative practices used to manage the consequences of cyberattacks reveals a distinctive pattern in Quebec relative to the rest of Canada.

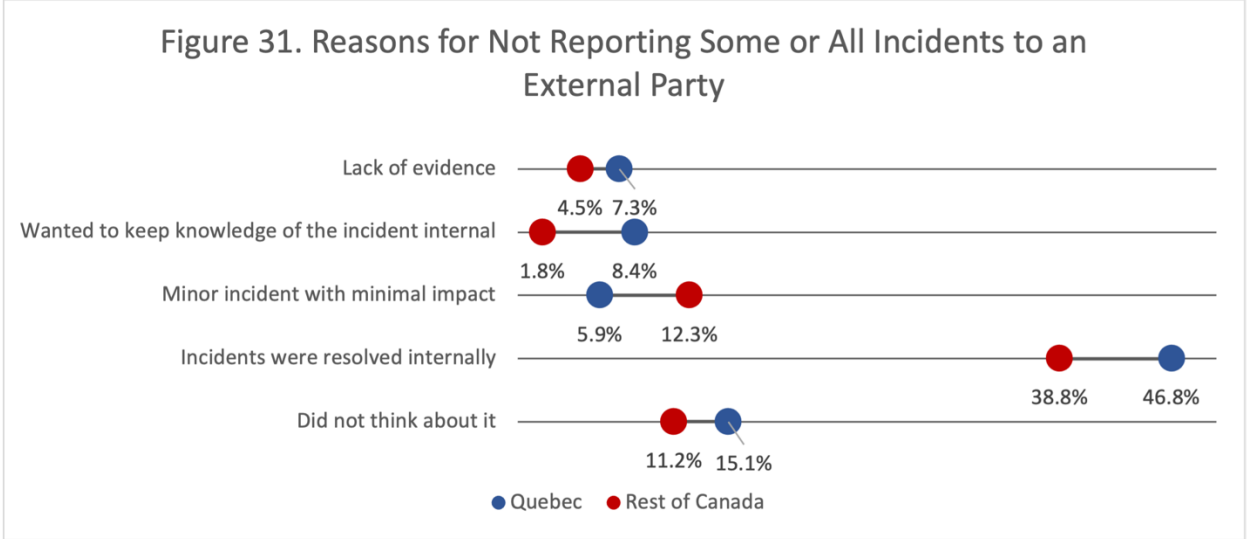
When Quebec businesses experience a cyberattack, they are proportionally more likely than businesses elsewhere in Canada to report the incident to at least one external partner other than law enforcement (26.5% report the incident to no one, compared with 38.9% in the rest of Canada) (Figure 29). The nature of this reporting also differs. Quebec businesses primarily seek assistance from IT consultants or contractors (40.3% versus 33.0%) and from specialized cybersecurity employees working for other organizations (11.0% versus 5.9%), whereas businesses elsewhere in Canada rely more heavily on software or service providers (10.6% versus 4.8%) and cyber insurance providers (6.2% versus 2.4%).



With respect to how businesses respond to incidents reported by external partners, Quebec businesses likewise demonstrate a much greater willingness to engage in a collaborative resolution process with the reporting partner (Figure 30): 37.6%, compared with 19.0% among businesses elsewhere in Canada. In addition, businesses outside Quebec are almost twice as likely to take no action in response to such notifications (45.7% versus 26.9%). Quebec therefore stands out for its greater willingness to collaborate during cyber incidents, although this collaboration appears to occur primarily within bilateral, private relationships rather than through institutional channels.



This pattern is further reflected in the reasons cited for not reporting cyber incidents to external third parties. Quebec businesses are nearly five times more likely than their counterparts elsewhere in Canada to explicitly state that they prefer to keep knowledge of the incident internal (8.4% versus 1.8%) (Figure 31). Although this difference is of modest magnitude, it is consistent with the behaviour observed above: Quebec businesses tend to favour the discreet, bilateral management of cyber incidents with trusted partners, a practice that may undermine the institutional transparency that Law 25 was specifically intended to promote.



Most of the remaining findings relating to peer consultation and incident reporting practices do not reveal significant differences between the two groups and are therefore not discussed further.

Overall, this comparative analysis suggests that Quebec's cybersecurity posture is characterized less by a generalized lag than by a distinctive configuration marked by a notable disconnect between institutional engagement, operational capabilities, and perceived preparedness. Quebec businesses are no more exposed to cyberattacks than businesses elsewhere in Canada, and the recovery costs they incur remain broadly comparable. They do, however, stand out for a higher proportion of incidents with no known motive, greater difficulty recruiting specialized cybersecurity professionals, less systematic cybersecurity awareness across their workforce, and a cybersecurity governance model that is more intensive but less institutionalized. Law 25 appears to have strengthened organizational attention to the protection of personal information and increased the direct involvement of senior management, but these changes have not yet translated into measurable improvements in technical performance, organizational security culture, or collective incident response capabilities. The primary challenge, therefore, is not merely to increase compliance with a new legislative framework, but to transform that compliance into a driver of sustainable organizational learning and a foundation for stronger cyber resilience.

CHAPTER 3. CYBERSECURITY PRACTICES AND CYBER RESILIENCE: A MULTIVARIATE ANALYSIS

The previous sections provided a descriptive and comparative overview of the evolution of the cybersecurity posture of Quebec businesses between 2021 and 2023, followed by an examination of how it compares with that of businesses elsewhere in Canada. They highlighted several notable developments, including stronger senior management involvement in cybersecurity governance, a greater emphasis on the protection of personal information as a driver of cybersecurity investment, and persistent weaknesses such as the low rate of monthly vulnerability patching and the absence of formal cyber risk identification activities in nearly four out of ten businesses. These findings raise a question that descriptive analyses alone cannot answer: to what extent do the risk management practices adopted by Quebec businesses have a measurable effect on their exposure to cyberattacks and on their ability to absorb their consequences and recover efficiently?

This section addresses that question by drawing on the five regression models described in the methodology: three binary logistic regression models for dichotomous outcomes (cyber victimization, occurrence of recovery costs, and occurrence of service disruptions), and two generalized linear models (GLMs) with a Gamma distribution for continuous outcomes (amount of recovery costs and duration of service disruptions). The descriptive statistics presented at the beginning of this section use the weighted CSCSC data to provide a representative profile of the target population of Quebec businesses. The regression models that follow are based on the unweighted confidential microdata, in accordance with Statistics Canada's confidentiality requirements governing access to detailed survey microdata. This distinction does not affect the internal validity of the estimated coefficients, since weighting is not required for estimating associations between variables. It does, however, mean that the regression results should be interpreted as associations observed within the study sample rather than as estimates that can be generalized to the entire population of Quebec businesses. These models make it possible to distinguish the factors that genuinely enhance organizational cyber resilience from those that merely create the appearance of preparedness.

Sample Profile and Distribution of Variables

Before presenting the regression results, it is useful to describe the characteristics of the sample on which the models are based (Table 4). The distribution by business size is representative of the Quebec economy: small businesses (10 to 49 employees) account for 81.2% of the weighted sample ($n = 44,724$), medium-sized businesses for 16.9% ($n = 9,333$), and large businesses for 1.9% ($n = 1,019$), for a total of 55,075 businesses. This distribution accurately reflects Quebec's business landscape, which is dominated by small and medium-sized enterprises (SMEs), and provides the structural context within which the following results should be interpreted.

With respect to dedicated cybersecurity personnel—a key variable in the multivariate analyses—the table confirms the findings reported in the previous chapters: 44.9% of businesses have no employees assigned to cybersecurity-related responsibilities, 24.2% employ one dedicated cybersecurity employee, and 25.8%

employ between two and five. Larger cybersecurity teams remain the exception, representing only 5% of businesses.

The adoption of cybersecurity risk management measures varies considerably across practices. Employee behaviour monitoring (27.8%), senior management involvement (27.2%), and formal cybersecurity risk assessments (24.3%) are the most commonly implemented measures. By contrast, participation in cyber threat information-sharing communities (4.4%), mandatory cybersecurity training (9.2%), and business continuity planning (8.9%) remain relatively uncommon. These descriptive statistics reinforce the conclusion that the adoption of cybersecurity practices is far from uniform across Quebec businesses. The purpose of the regression analyses that follow is therefore to determine which of these practices have a measurable impact on cybersecurity outcomes.

The continuous dependent variables exhibit highly skewed distributions, justifying the use of Gamma GLMs. Among businesses that experienced a cyber incident and reported recovery costs ($n = 4,399$), the median recovery cost was \$6,500, while the mean reached \$34,000 ($SD = \$91,700$), with a maximum value of \$712,000. This classic pattern—in which most businesses incur relatively modest losses while a small proportion experience extremely high costs—is consistent with the aggregate findings presented in Chapter 1, where total recovery costs more than doubled despite the relative stability of the victimization rate. Service disruption duration follows a similarly skewed distribution, with a median of 12 hours, a mean of 23.98 hours ($SD = 28.41$), and a maximum duration of 170 hours.

Table 4. Descriptive Statistics, Quebec 2023 (weighted data)				
	n	%		
Business Size				
Small (10–49 employees)	44,724	81.2		
Medium-sized (50–249 employees)	9,333	16.9		
Large (250 employees or more)	1,019	1.9		
Total	55,075	100.0		
Employees Dedicated to Cybersecurity				
None	23,311	44.9		
One employee	12,536	24.2		
Two to five employees	13,379	25.8		
Six to 15 employees	1,629	3.1		
More than 15 employees	1,005	1.9		
Total	51,861	100.0		
Cybersecurity Risk Management Measures				
Written risk management policy	11,941	21.7		

Cyber insurance	10,583	19.2		
Employee notification procedures	9,242	16.8		
Business continuity plan	4,893	8.9		
Senior management involvement	14,985	27.2		
Mandatory cybersecurity training	5,075	9.2		
Insider threat monitoring	15,320	27.8		
Formal risk assessment	13,400	24.3		
Penetration testing	9,627	17.5		
Participation in an information-sharing community	2,430	4.4		
Third-party IT systems assessment	12,732	23.1		
Dependent Variables				
Victim of a cyber incident	8,520	15.5		
Recovery costs (among victims)	4,410	51.8		
Service disruption (among victims)	3,379	39.7		
Continuous Variables (Among Affected Businesses)				
	n	Median (\$)	Mean (\$)	SD
Recovery costs	4,399	6,500	34,000	91,700
Service disruption duration (hours)	3,373	12.00	23.98	28.41

Note: Recovery costs are rounded to the nearest thousand dollars to comply with Statistics Canada's microdata confidentiality requirements.

Determinants of Cyber Victimization: What Actually Protects Organizations

The results of the first logistic regression model (Table 5) provide an analytical perspective that could not be obtained from the descriptive data alone. By controlling for all other variables, the model isolates the independent effect of individual cybersecurity risk management practices on the likelihood of experiencing a cyber incident. The findings are both reassuring in some respects and concerning in others.

The most robust finding in the entire analysis relates to dedicated cybersecurity personnel. In the control model, a business employing one dedicated cybersecurity professional is 3.85 times less likely to experience cyber victimization than a business with no dedicated cybersecurity employee (OR = 0.26; $p < 0.001$). This protective effect remains both statistically significant and substantively meaningful in the explanatory model (OR = 0.38; $p < 0.001$). This strong and consistent relationship reinforces a central conclusion: cybersecurity is, before anything else, a matter of human expertise, rather than simply technology or policy. This finding directly echoes the comparative analysis presented earlier in the report,

which showed that Quebec businesses experience greater difficulty than their counterparts elsewhere in Canada in recruiting qualified cybersecurity professionals. That shortage of specialized talent may, in turn, help explain the higher proportion of incidents classified as having "no known motive" in Quebec.

The relationship between business size and cyber victimization is more nuanced. While medium-sized businesses are significantly less likely than small businesses to experience cyber incidents (OR = 0.59; p = 0.004 in the explanatory model), this protective effect does not extend to large businesses, whose coefficient is not statistically significant. This finding suggests that medium-sized organizations may have reached a critical threshold in terms of resources and organizational maturity that strengthens their cybersecurity posture, whereas large organizations, facing more sophisticated threats and substantially larger attack surfaces, do not enjoy the same relative advantage.

Among the explanatory variables themselves, two counterintuitive findings deserve particular attention. Businesses that monitor employee behaviour to detect insider threats are 1.39 times more likely to experience a cyber incident than businesses that do not implement such monitoring (OR = 1.39; p = 0.011). Similarly, businesses conducting formal cybersecurity risk assessments also exhibit a higher probability of cyber victimization (OR = 1.34; p = 0.037). These positive associations should not be interpreted as evidence that these practices increase cyber risk. Rather, they reflect a well-known phenomenon of reverse selection bias. Organizations facing greater cyber risk—whether because they operate in higher-risk environments or have recently experienced cyber incidents—are precisely those that are more likely to invest in advanced monitoring and detection capabilities. The direction of causality is therefore reversed: heightened exposure to cyber risk drives the adoption of these practices, rather than these practices increasing the risk of victimization. All remaining explanatory variables—including written policies, cyber insurance, business continuity plans, mandatory training, and similar measures—are not statistically significant, indicating that, when considered individually, they do not measurably reduce the likelihood of being targeted by a cyberattack.

This finding has an important practical implication. From the perspective of Law 25, which has primarily encouraged the implementation of formal governance mechanisms—such as written policies, greater senior management involvement, and incident reporting procedures—the data suggest that these measures, while essential for regulatory compliance, do not, by themselves, provide greater protection against cyber victimization. The single factor that matters most—specialized cybersecurity human capital—is precisely the area in which Quebec businesses continue to face their greatest challenges.

Table 5. Logistic Regression—Determinants of the Probability of Experiencing a Cyber Incident, Quebec, 2023						
	Control Model			Explanatory Model		
	OR	95% CI	Sig.	OR	95% CI	Sig.
Control Variables						
Business Size						
Small (ref.)	—	—	—	—	—	—
Medium-sized	0.48	0.34–0.66	***	0.59	0.41–0.84	**

Large	0.75	0.54–1.05		0.82	0.59–1.16	
Cybersecurity Employees						
None (ref.)	—	—	—	—	—	—
One employee	0.26	0.16–0.44	***	0.38	0.22–0.67	***
Two to five employees	0.40	0.24–0.67	***	0.53	0.31–0.93	*
Six to 15 employees	0.58	0.36–0.95	*	0.71	0.42–1.19	
More than 15 employees	0.45	0.23–0.86	*	0.47	0.24–0.92	*
Explanatory Variables						
Written risk management policy				0.86	0.65–1.14	
Cyber insurance				0.93	0.72–1.21	
Employee notification procedures				1.24	0.93–1.65	
Business continuity plan				1.02	0.73–1.41	
Senior management involvement				1.11	0.85–1.44	
Mandatory cybersecurity training				0.81	0.59–1.13	
Insider threat monitoring				1.39	1.08–1.80	*
Formal risk assessment				1.34	1.02–1.76	*
Penetration testing				1.16	0.87–1.55	
Information sharing				1.28	0.89–1.85	
Third-party IT systems assessment				1.02	0.79–1.31	
χ^2	97.040 ***			128.591 ***		
Nagelkerke R ²	0.072			0.094		
Hosmer-Lemeshow Test	4.415 (p = 0.621)			12.711 (p = 0.079)		

Note: OR = Odds Ratio. Significance levels: * p < 0.05; ** p < 0.01; *** p < 0.001. N = 2,055. Unweighted data.

Determinants of Recovery Costs: Governance as a Protective Factor

While the results presented in Table 5 focused on the probability of experiencing a cyber incident, the next two models examine the financial consequences of those incidents for businesses that become victims. This analytical distinction is fundamental because it separates the factors that reduce exposure to cyber risk from those that influence an organization's ability to recover once an incident occurs. As the data demonstrate, these two dimensions of cyber resilience follow partially different dynamics.

The first finding is itself substantively important: the variables included in the logistic regression models do not predict whether a cyber incident will generate recovery costs for the affected business (Table 6—the models are not statistically significant, $\chi^2 = 5.772$ and 19.160). This lack of predictive power likely reflects the inherently random and unpredictable nature of post-incident costs, which are strongly influenced by factors that could not be measured through the survey questionnaire, such as the specific type of attack, the organization's ability and strategy for negotiating with attackers, the support provided by insurers, the speed with which the incident was detected, and other incident-specific circumstances. This represents an important methodological limitation that should be acknowledged. The CSCSC data

make it possible to document the magnitude of the phenomenon but not to predict it reliably at the level of an individual business.

One notable exception should nevertheless be highlighted. In the explanatory model, businesses whose senior management is actively involved in cybersecurity decision-making are significantly less likely to incur recovery costs following a cyber incident (OR = 0.56; $p = 0.016$). This finding constitutes one of the few empirical results in the entire analysis demonstrating a direct relationship between an organizational governance practice and a reduction in the financial consequences of cyber incidents. It provides quantitative support for the interpretation advanced earlier in the report: the substantial increase in cybersecurity reporting to senior management observed between 2021 and 2023, partly driven by the implementation of Law 25, is not merely a symbolic indicator of regulatory compliance. Rather, it appears to be associated with a greater organizational capacity to absorb the financial impact of cyber incidents when they occur.

Table 6. Logistic Regression—Determinants of the Probability of Incurring Recovery Costs Following a Cyber Incident, Quebec, 2023						
	Modèle contrôle			Modèle explicatif		
	RC	IC (95 %)	Sig.	RC	IC (95 %)	Sig.
Control Variables						
Business Size						
Small (ref.)	—	—	—	—	—	—
Medium-sized	1.51	0.86–2.68		1.43	0.77–2.65	
Large	1.30	0.75–2.25		1.14	0.65–2.03	
Cybersecurity Employees						
None (ref.)	—	—	—	—	—	—
One employee	0.50	0.22–1.15		0.37	0.14–0.98	*
Two to five employees	0.55	0.25–1.26		0.43	0.17–1.10	
Six to 15 employees	0.60	0.28–1.26		0.52	0.23–1.20	
More than 15 employees	0.35	0.11–1.08		0.33	0.11–1.05	
Explanatory Variables						
Written risk management policy				0.62	0.38–1.01	
Cyber insurance				0.87	0.55–1.37	

Employee notification procedures				1.05	0.65–1.69	
Business continuity plan				1.19	0.70–2.03	
Senior management involvement				0.56	0.35–0.90	*
Mandatory cybersecurity training				0.86	0.50–1.50	
Insider threat monitoring				0.94	0.61–1.44	
Formal risk assessment				1.26	0.77–2.06	
Penetration testing				1.04	0.63–1.72	
Information sharing				1.28	0.69–2.35	
Third-party IT systems assessment				1.34	0.87–2.08	
χ^2	5.772 (n.s.)			19.160 (n.s.)		
Nagelkerke R ²	0.018			0.058		
Hosmer-Lemeshow Test	1.862 (p = 0.762)			5.205 (p = 0.636)		

Note: OR = Odds Ratio. Significance levels: * p < 0.05; ** p < 0.01; *** p < 0.001. n.s. = not statistically significant. N = 432. Unweighted data.

The Gamma GLM examining the amount of recovery costs (Table 7) presents a more nuanced picture. The overall model is statistically significant ($\chi^2 = 75.804$; p < 0.001), confirming that certain predictors have a measurable effect on the magnitude of recovery expenditures—even though a substantial proportion of the variance remains unexplained, as reflected by the relatively high deviance/degrees of freedom ratio (3.05) and Pearson χ^2 /degrees of freedom ratio (2.67).

Business size is the strongest predictor. Medium-sized businesses incur, on average, 97% higher recovery costs than small businesses (mean ratio = 1.97; p < 0.001), while large businesses incur costs five times higher (mean ratio = 5.04; p < 0.001). This size-cost gradient is readily explained by the broader exposure of larger organizations, both in terms of the volume of compromised data and systems and the complexity of recovery operations. Combined with the earlier finding that large businesses are not less likely to experience cyber victimization (Table 5), this result depicts a coherent risk profile: the largest organizations are also those that incur the greatest financial losses when incidents occur.

The presence of dedicated cybersecurity employees also significantly reduces recovery costs. Compared with businesses that have no cybersecurity specialists, organizations employing one dedicated cybersecurity professional experience 56% lower recovery costs (mean ratio = 0.44; p = 0.020), while those employing two to five specialists experience 67% lower costs (mean ratio = 0.33; p < 0.001). This complementary finding reinforces the conclusions drawn from Table 5: specialized cybersecurity human

capital plays a dual protective role. It reduces both the likelihood of experiencing a cyber incident and, when an incident does occur, substantially mitigates its financial impact.

One final result deserves attention, although it should be interpreted with the same caution as the counterintuitive associations reported in Table 5. Businesses that conducted a formal cybersecurity risk assessment incurred, on average, recovery costs twice as high as those that did not (mean ratio = 2.02; $p = 0.013$). As with the positive association previously observed between insider threat monitoring and cyber victimization, organizations conducting formal risk assessments are precisely those operating in environments where cyber risks are objectively greater and where incidents, when they occur, tend to be more costly. It is therefore not the risk assessment itself that increases recovery costs; rather, it is heightened exposure to cyber risk that motivates organizations to undertake formal risk assessments.

Table 7. Gamma GLM—Determinants of Recovery Costs Following a Cyber Incident, Quebec, 2023			
	Mean Ratio	95% CI	Sig.
Control Variables			
Business Size			
Small (ref.)	—	—	—
Medium-sized	1.97	1.16–3.37	***
Large	5.04	2.41–10.53	***
Cybersecurity Employees			
None (ref.)	—	—	—
One employee	0.44	0.22–0.88	*
Two to five employees	0.33	0.18–0.64	***
Six to 15 employees	0.30	0.07–1.33	
More than 15 employees	0.52	0.16–1.73	
Explanatory Variables			
Written risk management policy	1.46	0.77–2.76	
Cyber insurance	0.70	0.43–1.14	
Employee notification procedures	1.72	0.97–3.05	
Business continuity plan	0.63	0.32–1.22	
Senior management involvement	0.91	0.46–1.69	
Mandatory cybersecurity training	1.19	0.61–2.32	

Insider threat monitoring	1.08	0.67–1.73	
Formal risk assessment	2.02	1.16–3.54	*
Penetration testing	0.98	0.53–1.80	
Information sharing	1.66	0.82–3.37	
Third-party IT systems assessment	1.16	0.72–1.88	
Deviance	551,446		
Pearson χ^2	483,293		
Likelihood Ratio (χ^2)	75,804 ***		
Residual Degrees of Freedom	181		

Note: Mean Ratio = Exp(B). Significance levels: * $p < 0.05$; ** $p < 0.01$; *** $p < 0.001$. N = 199. Unweighted data.

Determinants of Service Disruptions: The Limits of Predictability

The final two models examine the operational consequences of cyber incidents: the occurrence of a service disruption and its duration. The overall picture is less encouraging.

The logistic regression models predicting the probability of a service disruption (Table 8) are not statistically significant ($\chi^2 = 11.440$ and 19.035), with one notable exception. In the control model, businesses employing one dedicated cybersecurity employee are significantly less likely to experience a service disruption (OR = 0.29; $p = 0.004$), an effect that remains significant in the explanatory model (OR = 0.25; $p = 0.006$). Only one explanatory variable reaches statistical significance: the implementation of employee notification procedures is associated with a reduced likelihood of experiencing a service disruption (OR = 0.59; $p = 0.037$). Although this finding stands alone, it is consistent with the logic of organizational preparedness. Ensuring that employees understand the procedures to follow in the event of a cyber incident likely accelerates containment and response efforts, thereby reducing operational disruptions. Across all other dimensions, the variables included in the models do not demonstrate measurable predictive power with respect to the occurrence of a service disruption.

Table 8. Logistic Regression—Determinants of the Probability of a Service Disruption Following a Cyber Incident, Quebec, 2023

	Control Model			Explanatory Model		
	OR	95% CI	Sig.	OR	95% CI	Sig.
Control Variables						
Business Size						

Small (ref.)	—	—	—	—	—	—
Medium-sized	1.04	0.59–1.85		0.96	0.52–1.79	
Large	0.87	0.50–1.50		0.84	0.47–1.50	
Cybersecurity Employees						
None (ref.)	—	—	—	—	—	—
One employee	0.29	0.12–0.67	**	0.25	0.09–0.68	**
Two to five employees	0.59	0.26–1.33		0.55	0.22–1.39	
Six to 15 employees	0.55	0.26–1.16		0.57	0.25–1.29	
More than 15 employees	0.55	0.19–1.64		0.53	0.18–1.59	
Explanatory Variables						
Written risk management policy				0.83	0.50–1.38	
Cyber insurance				0.80	0.51–1.28	
Employee notification procedures				0.59	0.36–0.97	*
Business continuity plan				1.17	0.69–2.00	
Senior management involvement				1.17	0.73–1.89	
Mandatory cybersecurity training				1.11	0.63–1.93	
Insider threat monitoring				1.02	0.66–1.59	
Formal risk assessment				0.96	0.58–1.58	
Penetration testing				1.01	0.60–1.71	
Information sharing				1.23	0.67–2.27	
Third-party IT systems assessment				1.01	0.65–1.58	
χ^2	11.440 (n.s.)			7,595 (n.s.)		
Nagelkerke R ²	0.035			0,058		
Hosmer-Lemeshow Test	8.024			11,578		

Note: OR = Odds Ratio. Significance levels: * p < 0.05; ** p < 0.01; *** p < 0.001. n.s. = not statistically significant. N = 432. Unweighted data.

The Gamma GLM examining the duration of service disruptions (Table 9) is likewise not statistically significant overall ($\chi^2 = 26.338$; n.s.), although one isolated coefficient reaches statistical significance—a finding that should be considered exploratory. Businesses that conducted a comprehensive third-party assessment of their IT systems experienced service disruptions that were, on average, 72% longer than those of businesses that did not (mean ratio = 1.72; $p = 0.005$). Although this result appears counterintuitive at first glance, it follows the same pattern of selection bias observed elsewhere in the analysis. Organizations whose information systems are sufficiently complex or critical to warrant an independent third-party assessment are precisely those whose service disruptions, when they occur, tend to last longer. The general lack of predictive power for service disruption duration further supports the conclusion that this outcome is determined more by the specific nature of the cyberattack and the architecture of the affected information systems than by the generic cybersecurity risk management measures captured in the survey.

Table 9. Gamma GLM—Determinants of Service Disruption Duration Following a Cyber Incident, Quebec, 2023			
	Mean Ratio	95% CI	Sig.
Control Variables			
Business Size			
Small (ref.)	—	—	—
Medium-sized	1.12	0.69–1.82	
Large	1.13	0.67–1.92	
Cybersecurity Employees			
None (ref.)	—	—	—
One employee	0.86	0.50–1.50	
Two to five employees	1.01	0.60–1.70	
Six to 15 employees	0.78	0.33–1.84	
More than 15 employees	0.84	0.38–1.84	
Explanatory Variables			
Written risk management policy	1.15	0.77–1.71	
Cyber insurance	0.98	0.67–1.42	
Employee notification procedures	1.04	0.70–1.55	
Business continuity plan	1.38	0.87–2.18	

Senior management involvement	0.77	0.51–1.18	
Mandatory cybersecurity training	1.35	0.85–2.14	
Insider threat monitoring	0.72	0.51–1.03	
Formal risk assessment	1.11	0.70–1.77	
Penetration testing	0.62	0.38–1.00	
Information sharing	0.73	0.44–1.22	
Third-party IT systems assessment	1.72	1.17–2.52	**
Deviance	199.878		
Pearson χ^2	191.925		
Residual Degrees of Freedom	149		
Likelihood Ratio (χ^2)	26.338 (n.s.)		

Note: Mean Ratio = Exp(B). Significance levels: * $p < 0.05$; ** $p < 0.01$; *** $p < 0.001$. n.s. = not statistically significant. N = 167. Unweighted data.

SUMMARY: CYBERSECURITY AS AN INVESTMENT IN HUMAN CAPITAL

Taken together, the five models presented in this section paint a more nuanced—and, in some respects, less optimistic—picture than that suggested by the descriptive analyses alone. Three overarching conclusions emerge.

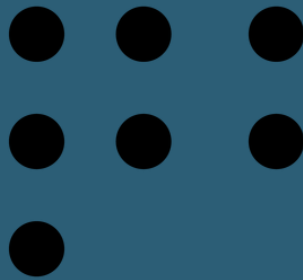
The first is that cybersecurity is fundamentally a matter of human capital. The most robust, consistent, and stable predictor across all five models is the presence of dedicated cybersecurity personnel. This variable reduces the likelihood of cyber victimization, lowers recovery costs, and, to some extent, decreases the probability of service disruptions. No other variable demonstrates such a consistently protective effect. This finding directly echoes one of the most concerning blind spots identified in the preceding chapters: the near-stagnation of specialized cybersecurity hiring in Quebec and the particular challenges of the province's labour market in this field. The shortage of cybersecurity professionals is therefore not merely a governance or regulatory compliance issue. According to these models, it represents the principal structural vulnerability facing Quebec businesses in the evolving cyber threat landscape.

The second conclusion is that formal governance measures have limited and narrowly defined effects on cybersecurity outcomes. Written policies, business continuity plans, cyber insurance, and cybersecurity training programs—whose prevalence generally increased between 2021 and 2023, partly as a result of Law 25—do not exhibit significant predictive power with respect to either cyber victimization or recovery costs in any of the models. The only notable exceptions are senior management involvement and employee notification procedures, both of which are associated with a lower probability of incurring

recovery costs. This finding should be interpreted cautiously. It does not imply that these measures lack value, but rather that their effects are not directly observable in the CSCSC data. This may be because they influence dimensions not captured by the survey, because their implementation remains too recent, or because their adoption varies too widely in quality and maturity across organizations to produce measurable effects at the sample level.

The third and final conclusion underscores the importance of interpreting these findings with appropriate caution. Several counterintuitive associations—such as the positive relationship between insider threat monitoring and cyber victimization, or between formal cybersecurity risk assessments and higher recovery costs—illustrate the challenges posed by reverse causality in observational cybersecurity research. These findings highlight the need for methodological caution. Organizations facing the greatest cyber risks are also those most likely to invest in advanced monitoring, detection, and risk assessment capabilities during a given period. Consequently, correlations observed in cross-sectional data, rather than longitudinal observations, tend to reflect organizations' adaptive responses to increasingly hostile threat environments rather than unintended adverse effects of these cybersecurity practices.

Overall, this multivariate analysis suggests that the cybersecurity posture of Quebec businesses remains unbalanced. Investments in regulatory compliance and formal governance measures continue to grow, even though their direct effects on cybersecurity outcomes remain difficult to demonstrate empirically. At the same time, organizations continue to underinvest in the factor that appears to matter most: specialized cybersecurity expertise. Closing this gap represents both the greatest challenge and the greatest opportunity for strengthening the cyber resilience of Quebec businesses in the years ahead.



Prompt

1200 McGill College Ave suite 1650, Montreal,
Quebec H3B 4G7

promptinnov.com

With the financial support of

 **prompt**

Québec  