Texila International Journal of Academic Research
ISSN: 2520-3088
DOI: 10.21522/TIJAR.2014.12.02.Art008

Business Data Breaches-Impact on Brand Reputation and Employee Integrity: A Case Study of Desjardins in Canada

Kazeem Kolawole Olanrewaju*
Management, University of Central Nicaragua

Abstract

The research explored the effects and the impact of business data breaches on brand reputation and employee integrity, using the 2019 Desjardins Group Canada breach as a case study. The breach in question compromised personally identifiable information of over 9.7 million customers and Desjardins members, revealing vulnerability in data security, governance, and organizational culture. In addition to financial losses, the incident eroded client trust and loyalty, created an internal crisis and uncertainty within the organization. The research examines the effects of the breach on stakeholder confidence, business resilience, and employee morale using a mixed research approach which includes interviews, surveys, and secondary data analysis. The research reveals a significant decline in public trust, financial impacts, and brand damage. Employees faced increased stress levels, low morale, and declining confidence in leadership, which highlighted the human toll of cybersecurity failures. The research explores how perceived risks and threats, protective measures, and trust dynamics can influence stakeholder responses. It emphasizes the necessity of a clear crisis management process, transparency, and robust cybersecurity frameworks to mitigate the adverse effects of data breaches. Organizations that acted swiftly and communicated transparently could restore stakeholder trust and confidence. To enhance information security, businesses should invest in governance, employee training, and cultivate a security-focused culture. Additionally, policymakers should advocate for stringent data protection laws and regulations, mandatory breach disclosures, and cross-sector collaboration to strengthen cybersecurity resilience. This research offers valuable insights for businesses, regulators, and scholars confronting cybersecurity risks and threats in an increasingly digital landscape.

Keywords: *Business Data Breach, Customer Loyalty, Customer Trust, Cybersecurity, Employee Integrity, Organization Reputation.*

Introduction

In today's digital economy, data is an essential and fundamental asset that helps drive decision-making, organizational strategic planning, and operational efficiency and optimization in businesses across all sectors [8]. As business organizations continuously rely on IT and digital infrastructures and peripherals to manage sensitive business information, the risks associated with data breaches have increased exponentially, and businesses, especially in the financial industry, are vulnerable and prime targets [10]. Data breaches can be defined as unauthorized access to, or disclosure of, confidential information, resulting in devastating financial losses, legal consequences, loss of customer trust, and long-term reputational damage [17]. These breaches can profoundly affect organizations, damaging their reputation and the integrity of their staff members. This study investigates the impact of the Desjardins data breach on brand reputation and employee integrity; it will shed light on the implications of the breach and offer insights on

Received: 01.03.2025 ***Accepted: 09.03.2025*** ***Published on: 30.04.2025***
****Corresponding Author: kazeem.k.olanrewaju@gmail.com***

how the organizations can effectively manage the aftermath of such incidents. Brand reputation is significant for any business, influencing customer satisfaction, loyalty, and perceptions [2].

The 2019 Desjardins Group data breach was one of the most significant incidents in Canadian financial history, impacting over 9.7 million Canadians. This breach, caused by an insider threat, exposed the vulnerabilities inherent in even the most robust cybersecurity frameworks and highlighted the multilayered impacts of such breaches on organizational reputation and employee integrity [18]. This study seeks to investigate these dimensions, examining how data breaches influence public opinion, customer loyalty, perception of the brand, stakeholder confidence, and internal organizational culture.

Data breaches have become a recurring phenomenon in the digital age. In this modern age, businesses across the globe heavily rely on technology to analyze data for strategic business decisions, storage, and to maintain their online presence. Many are increasingly falling victim to cyber-attacks from internal or external actors. There are many dire business consequences of a data breach, and the primary concern has shifted to the impact of data breaches on an organization's reputation and employee integrity, the impact on its customer base and loyalty, and continued patronage. With the increasing prevalence of data breaches and the ever-growing integration and interconnectivity of the online world, exploring their impact on business brands is of paramount concern.

Since it is almost impossible to maintain an impenetrable cyber defense in the modern landscape, it is essential to understand how organizations can respond and what steps should be taken in the aftermath to avoid reputation damage and maintain customer trust and loyalty [2]. When a data breach occurs, the process should be written in the organization's policy and procedure, disaster response plan (DRP), and business continuity plan (BCP). An in-depth analysis of Desjardins' data breach, its response, and its impact on business reputation and employee integrity will be conducted. The Desjardin information security practices, pre- and post-data breach incidents, will be reviewed, analyzed, and compared with other data breach incidents that have happened to identify the gap.

Scope and Limitations

This research focuses on the Desjardins Group data breach incident as a case study to provide in-depth analysis and insights into the organizational impacts of data breaches and cybersecurity incidents. The scope includes an analysis of the breach's effects on brand reputation, employee integrity, and the effectiveness of crisis management strategies. While the case study approach allows for detailed exploration, the findings may not be universally generalizable. Additionally, the study relies on primary data (interviews and surveys) and secondary data (Office of the Privacy Commissioner of Canada, financial industry report, Desjardin report, Google Scholar, Research Gate, websites, and media analysis), which may present inherent biases.

Significance of Study

This study holds significant importance and value for both academic and practical purposes. It contributes to the growing body of literature on business data protection, cybersecurity governance, risk management, and organizational behavior for academic purposes. In practical terms, the findings offer critical insights for business organizations, business leaders, information technology professionals, regulators, government, and policymakers aiming to enhance and improve business data protection strategies and crisis response mechanisms. By understanding the correlation between data breaches, brand reputation, and impact on employee integrity, organizations

can better prepare for, respond to, and recover from any data breach incident.

Literature Review

The financial industry's services, products, and roles are crucial to Canada's economy. They facilitate financial transactions like insurance products, investment products, and wealth management for individuals and businesses, enabling them to access their customers' private and personally identifiable information (PII) [18]. However, the increasing dependence and reliance on technologies and digital platforms, coupled with the sensitive nature of data they store in their financial and personal databases, has made financial institutions focal and prime targets for cyber threats, including data breaches. In an industry built on trust and security like this financial institution, any breach can impact customer confidence, negatively impact clients' loyalty, impact employees' morale, affect shareholder value, and result in significant regulatory penalties [24]. As a custodian of people's money and life savings, it cannot afford any data and cyber security incident that shows organizations have weak cybersecurity practices or an inability to protect people's information; this could have a huge impact on reputation, which can erode trust. These breaches can result from external cyberattacks, insider threats, or system vulnerabilities [17]. The increasing frequency and sophistication of data breaches highlight the growing cybersecurity challenges faced by organizations around the globe.

Knowing the impact a business data breach will have on the organization's reputation and employee integrity is important. Brand reputation is a critical intangible asset, goodwill, influencing customer trust, loyalty, and overall business success. Data breaches can severely damage a brand's reputation, leading to loss of customer confidence, adverse media reporting and coverage, and long-term financial consequences [12]. Some existing studies have shown that companies experiencing data breaches more often suffer declines in stock prices, market share and dominance, and customer retention rates [19]. Notably, the breach of consumer data is not the only factor influencing consumer perceptions of brand trust [2]. The response and actions taken by the company in the aftermath of the crisis can have significant consequences on consumer perception and behavior [10]. A delayed response to a breach, evasion of responsibility, or unclear communication, such as legal proceedings or investigations, can all impact consumer perceptions and form opinions of brand reputation [7]. Failing to prevent a data breach is one aspect; however, inadequately managing the aftermath can foster even greater distrust, which can, in turn, negatively affect consumer behavior and attitude toward the brand [2].

Data breaches also have philosophical effects on employee integrity and organizational trust. Employees may feel demoralized, anxious, and distrustful of their organization's ability to protect sensitive information [10]. Data breaches can also result in a decline in trust between employers and employees, especially when it is established that an insider, such as Desjardin Group, caused the breach. Whitener et al. (1998) emphasized that trust is a fundamental component of organizational culture, and breaches can erode this trust, leading to decreased job satisfaction, productivity, and employee retention. An operational and effective security policy and procedure that details cybersecurity governance, risk management, and compliance frameworks is essential for mitigating data breach risks. IT governance strategies provide a structured approach to managing IT risks, ensuring regulatory compliance, and promoting a security-conscious organizational culture (Von Solms & Von Solms, 2004). In designing policies and procedures to secure data, organizations borrow a leaf from different standards and frameworks such as the NIST

Cybersecurity Framework (2018) and ISO/IEC 27001, COBIT, etc., which are widely adopted models that guide organizations in identifying, protecting, and detecting, responding to, and recovering from cybersecurity incidents.

Implementing those frameworks and standards into business operations is important; IT General Controls must be properly designed based on the standards or frameworks that the organization has chosen, and control-protective and detective measures must be ensured to work as intended. Access control mechanisms protect sensitive data and personnel from unauthorized access. Many techniques, such as multi-factor authentication (MFA), role-based access control (RBAC), and encryption mechanisms, are commonly used to safeguard information from unauthorized access [20]. Security controls, including firewalls, intrusion detection systems, and regular security and logs audits, play an essential role in preventing, detecting, and mitigating data breaches [22]. Incident response plans are critical for effectively managing data breaches. As Chatterjee and Sokol said, the response and actions taken by the company in the aftermath of the crisis can have significant consequences on consumer perception and behavior [2]. The ISMS policy should include a business continuity plan (BCP) outlining procedures for detecting, responding to, and recovering from security incidents [1]. Mitropoulos et al. (2006) highlight the importance of communication during a crisis in maintaining stakeholder trust during and after a breach. Organizations with well-developed incident response plans can effectively and significantly reduce the impact of breaches on their operations and reputation.

Research Methodology

This study adopts a mix of quantitative and qualitative research methods, utilizing a case study approach to provide an in-depth analysis and exploration of the Desjardins Group data breach. The qualitative approach allows for a complete and comprehensive understanding of the subjective experiences and perceptions of many stakeholders affected by the data breach [25]. The case study method is suitable for examining complex issues within real-life contexts.

The case study approach enables an in-depth analysis of the Desjardins Group data breach, focused on its impacts on brand reputation and employee integrity. This approach allows for examining the organization's responses, crisis management strategies, and the broader implications of the breach on stakeholders and the business. The case study is both descriptive and exploratory, aiming to discover and uncover patterns and generate insights that can inform best practices in business data protection and cybersecurity governance.

The study uses both primary and secondary data to investigate, analyze, and substantiate the research findings and to have robust information to enhance the credibility of the findings.

Primary Data

The data was collected through semi-structured interviews and surveys. Interviews were conducted with various stakeholders, including Desjardins employees, management, cybersecurity experts, and affected customers. Surveys are distributed to a broader audience to capture quantitative data on perceptions of brand reputation and employee Integrity and trust.

Secondary Data

This includes organizational reports, regulatory documents, the Canadian Office of Privacy Commission's public website, media articles, academic journals, Google Scholar, and industry publications. It provides context and supports the analysis of primary data.

The study uses purposeful sampling techniques to select participants with direct and indirect experience in the financial industry or relevant knowledge of the Desjardins data breach. It also employs customers of other

financial institutions. The sample participants include:

1. Employees of the financial industry, like banks and Insurance companies.
2. Senior executive officers involved in breach response and crisis management.
3. Staff and employees from various departments to understand internal perceptions.
4. Customers affected by the breach to assess its impact on trust, reputation, and loyalty.
5. Cybersecurity experts and industry professionals for expert insights.

Research Objectives

The primary objectives of this research are to:

1. Evaluate and assess the impact of data breaches on brand reputation using Desjardins Group as a case study in the Canadian financial industry.
2. Examine the effects of data breaches on employee integrity, trust, and organizational culture.
3. Identify and analyze the crisis management strategies employed by Desjardins Group post-breach.
4. Provide actionable recommendations for business organizations to strengthen and improve their cybersecurity posture and resilience against reputational damage after the incident.

Research Questions

This study seeks to answer the following key research questions:

1. What are the immediate and long-term impacts of data breaches on the brand reputation of financial institutions, particularly in the case of Desjardins Group Canada?
2. How does a data breach affect employee integrity, organizational trust, and workplace morale?
3. What crisis management and recovery strategies can organizations adopt to restore stakeholder confidence following a data breach?

Research Hypothesis

Based on the key research questions, two research hypotheses were developed to investigate further the impact of the business data breach on business reputation and trust and how it impacts employee integrity and confidence in the organization using the primary data.

Hypotheses One

Null Hypothesis (H_0): Data breaches at Desjardins Group and financial institutions in Canada have no significant impact on brand reputation.

Alternative Hypothesis (H_1): Data breaches at Desjardins Group and financial Institutions in Canada significantly impact brand reputation.

Hypotheses Two

Null Hypothesis (H_0): Data breaches do not significantly impact employee integrity and confidence in the organization.

Alternative Hypothesis (H_1): Data breaches significantly impact employee integrity and confidence in the organization.

Research Questionnaire Design

Impact on Brand Reputation survey design:

Section 1: Demographics

1. What is your age group?
    a) 18-25
    b) 26-35
    c) 36-45
    d) 46-55
    e) 56+
2. What is your gender?
    a) Male
    b) Female
    c) Other

Section 2: Professional Background

3. What is your role at Desjardins/ or your current employer if not with Desjardins?
    a) Customer-facing employee
    b) Back-office employee
    c) Management
    d) Other (please specify)
4. How long have you been employed at Desjardins?
    a) Less than 1 year
    b) 1-3 years
    c) 4-6 years
    d) 7+ years
    e) Not Applicable

Section 3: Perception of Data Breaches

5. Have you been directly or indirectly impacted by a data breach at Desjardins?
    a) Yes
    b) No
6. On a scale of 1-5, how do you perceive the company's response to data breaches?
    a) 1: Very Poor
    b) 2: Poor
    c) 5: Excellent

Section 4: Impact on the Brand Reputation

7. To what extent do you think data breaches affect Desjardins' reputation among their customers?
    a) Not at all
    b) Slightly
    c) Moderately
    d) Strongly
8. Do you think customers' trust in Desjardins has been affected?
    a) Yes
    b) No

Section 5: Impact on Employee Integrity

9. Have data breaches diminished your trust in management or made you feel less confident about Desjardins' systems or the company you work for if you are not with Desjardins?
    a) Yes
    b) No
10. On a scale of 1-5, how likely are you to consider leaving Desjardins due to trust issues related to data breaches?
    a) 1: Not at all likely
    b) 5: Extremely likely

Data Collection Method and Approach

Primary data was gathered through semi-structured interviews with different Financial Institutions, Desjardins employees, management, cybersecurity experts, and affected customers, as stated below. Surveys were distributed anonymously (This means that the identity and information of respondents were unknown) to a broader audience to capture quantitative perceptions of the business data's impact on the organization. Secondary data included the Office of Canada Privacy Commissioner, organizational reports, regulatory documents, media articles, and academic literature. Thematic analysis was also employed to identify recurring themes from the qualitative data [6].

1. Interview Guide: It was designed to facilitate semi-structured interviews about the impact of breaches on business reputation, employee Integrity and confidence, security breach awareness, crisis response, organizational trust, and employee morale.
2. Survey Questionnaire: The questionnaire includes closed- and open-ended questions to capture quantitative and qualitative data on stakeholders' opinions and perceptions of the breach's impact.

The data collected was analyzed using the Chi-Square Test for independence, regression analysis, and thematic analysis for trend and pattern. The thematic analysis includes identifying, analyzing, and reporting patterns (themes) within the data [6]. The process includes:

1. Data familiarization means reading and re-reading transcripts to become immersed in the data to help with analysis.
2. Reviewing Themes, meaning refining themes and patterns to ensure they accurately represent the data.
3. Interpreting Data means connecting findings to research questions and existing literature.

Validity and Reliability

To ensure the validity and reliability of this study, the concept of triangulation was used, and multiple data sources and methods were used to corroborate our findings, in addition to the empirical result of primary data analysis. We ensure the Audit Trail maintains detailed records of data collection and analysis processes for accuracy, reference, and to substantiate the findings.

Ethical Considerations

Ethical considerations are essential, given the sensitivity of data breach incidents. The study adheres to ethical research principles, including:

1. Informed consent was obtained to ensure all participants were informed about the study's purpose, procedures, and rights before consent.
2. Confidentiality to ensure the anonymity and privacy of participants' identities and responses.
3. Data Security, implementing measures to protect the security and integrity of data collected to date.

Limitations of Methodology

While a mixed method using the case study approach provides rich, detailed insights, it has limitations [6]. Findings may not apply to all organizations, especially those in the nonfinancial industry, due to the focus on a single case. The bulk of data used in this research was primarily secondary, and primary data was limited due to concerns about employees and employers. In addition, there might be potential biases in participant responses and researcher interpretations. Limited access to the most recent data from the Desjardin Group may affect the comprehensiveness of the analysis; many members were reluctant to participate, and those who participated did so in anonymity.

Survey Data Analysis

The total number of respondents is 200 (A random sampling of customers, employees, and non-employees of Desjardin who are working in the financial industry and across various departments)

Summary of Survey Response

- **Question 5:** 60% answered directly impacted, and 40% not impacted.
- **Question 6:** Average score: 2.8/5.
- **Question 7:** 70% believed reputation is strongly affected.
- **Question 8:** 80% think customer trust is affected.
- **Question 9:** 65% feel less confident in systems and feel less trusted by the employer.
- **Question 10:** Average score: 3.2/5.

The **Chi-Square (χ^2) formula** is applied as follows:

$$\chi 2 = \sum (Oi - Ei) 2Ei \chi^2 = \sum \frac{(O_i - E_i)^2}{E_i} \chi 2 = \sum Ei(Oi - Ei) 2$$

Where:

- Oi = Observed frequency of each category
- Ei = Expected frequency of each category
- ∑= Summation across all categories

Hypotheses One Testing

Null Hypothesis (H_0): Data breaches at Desjardins Group and financial institutions in Canada have no significant impact on brand reputation.

Alternative Hypothesis (H_1): Data breaches at Desjardins Group and financial

Institutions in Canada significantly impact brand reputation.

The results of the surveys are organized in the Table 1. Reputation Survey Response below:

Table 1. Reputation Survey Response

Response Category	Observed Frequency (O)	Expected Frequency (E)
Not at all	20	50
Slightly	30	50
Moderately	30	50
Strongly	120	50

Total sample size: 200 respondents

Then compute the Chi-Square Statistic based on the formula stated and Table 1 above.

$$\chi^2 = \frac{(20-50)^2}{50} + \frac{(30-50)^2}{50} + \frac{(30-50)^2}{50} + \frac{(120-50)^2}{50}$$

$$\chi^2 = \frac{(-30)^2}{50} + \frac{(-20)^2}{50} + \frac{(-20)^2}{50} + \frac{(70)^2}{50}$$

$$\chi^2 = \frac{900}{50} + \frac{400}{50} + \frac{400}{50} + \frac{4900}{50}$$

$$\chi^2 = 18 + 8 + 8 + 98$$

$$\chi^2 = 132.0$$

Determine the p-value

The **p-value** is calculated using a chi-square distribution table or statistical software.

1. Degrees of Freedom (df) Formula is equal to: Df= Number of categories − 1

Since we have four response categories, the degrees of freedom: Df= 4−1= 3

2. The computed **p-value** = **2.00×10^{-28}**, which is **extremely small**.

Decision Rule

Compare the **p-value** to the standard significance level ($\alpha = 0.05$):

1. **If p-value < 0.05** → Reject the null hypothesis (**H_0**).
2. **If p-value > 0.05** → Fail to reject the null hypothesis (**H_0**).

Since **p-value = 2.00×10^{-28} which** is far less than 0.05, we **reject H_0**.

Interpretation of Result

1. The higher value of χ^2 (132.0) and very low p-value indicate that the observed distribution of trust and reputation perception responses significantly differs from what we expect under a uniform assumption.
2. That means data breaches strongly impacted the organization's reputation and customer trust, as most respondents reported a "Strongly" adverse impact.

Conclusion on Hypothesis One

Reject the Null Hypothesis (H_0) and accept Alternative Hypothesis (H_1) based on the test of hypothesis, which means Data breaches at Desjardins Group and Financial Institutions in Canada significantly impact brand reputation.

Hypothesis Two Testing

1. **Null Hypothesis (H_0):** Data breaches do not significantly impact employee Integrity and confidence in the organization.
2. **Alternative Hypothesis (H_1):** Data breaches significantly impact employee integrity and confidence in the organization.

To analyze and test hypothesis two, the survey response data related to confidence and integrity were tabulated Table 2 below.

Table 2. Confidence and Integrity

Response Category	Observed Frequency (O)	Expected Frequency (E)
Feel Less Confident	130	100
Feel Unaffected	70	100

The responses were categorized as follows:
Total sample size: 200 respondents

Using the Chi-Square Statistic

$$\chi^2 = \frac{100(130-100)^2}{100} + \frac{100(70-100)^2}{100}$$

We break it down as follows:

$$\chi^2 = \frac{100(30)^2}{100} + \frac{100(-30)^2}{100}$$

$$\chi^2 = \frac{100 \times 900}{100} + \frac{100 \times 900}{100}$$

$$\chi^2 = 9 + 9$$

$$\chi^2 = 18.0$$

Then we determine the **p-value**

1. Degrees of Freedom (df):

Df will be Number of categories minus 1, which will be 2−1=1

2. The computed p-value = 2.21×10^{-5} (0.0000221)

Compare the **p-value** to the standard significance level ($\alpha = 0.05$), then:

1. **If p-value < 0.05** → Reject the null hypothesis (**H_0**).
2. **If p-value > 0.05** → Fail to reject the null hypothesis (**H_0**).

Since our **p-value = 0.0000221** is much smaller than **0.05**, we **reject H_0**.

Interpretation of Hypothesis Two

1. The higher value of χ^2 (18) and very small p-value means that observed differences in employee Integrity and confidence are statistically significant.
2. This result means the data breaches harmed employee integrity and confidence in the company's internal systems.

Conclusion on Hypothesis Two

Reject the Null Hypothesis (H_0) and accept Alternative Hypothesis (H_1) that says Data breaches at Desjardins Group significantly impact employee Integrity and confidence in the organization.

Result and Discussion

The analysis of primary and secondary data and the interpretation of the key research results and findings, connecting them to existing literature and theoretical frameworks as discussed earlier, gave us a reliable conclusion of our investigation. The discussion explores the implications of the Desjardins Group data breach on brand reputation and employee integrity. Moreover, analyzed the organizational resilience. In addition, it highlights the practical, theoretical, and policy-related insights derived from the study.

The primary data analysis shows that the Desjardins data breach significantly impacted Brand Reputation and diminished customer trust in the organization, resulting in brand reputational damage and financial repercussions. The result aligns with prior research indicating that data breaches negatively affect brand image, public perception, and consumer loyalty [19]. Comparative analysis done from the secondary data, which compared the Desjardin incident with the industry as shown in Figure 1 shows that Desjardin's impact was higher in the industry. Moreso, compare the incident of Desjardins' business data breach with high-profile data breaches that have occurred in Canada, like Equifax, Target, etc., shows a familiar pattern:

1. Insider Threats: Similar to the Desjardins incident, insider threats were common and significant in many business data breaches [32].
2. Delayed Detection: Not being proactive and prolonged detection times worsened the impact of breaches and was familiar to those known incidents.
3. Reputational Recovery: Organizations that communicated honestly and transparently and implemented robust post-incident security reforms recovered their reputations more effectively [33].

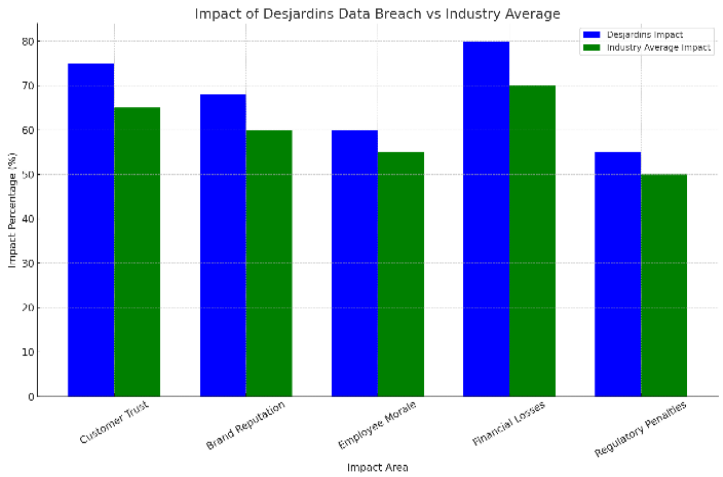

Figure 1. Impact: Desjardins Vs Industry Average

The media coverage increased public awareness of the breach and further damaged Desjardins' credibility. Though honest and transparent communication can help to reduce the impact on the brand, it was not sufficient to fully mitigate reputational damage, emphasizing the long-term nature of brand recovery post-breach according to the secondary data [7].

The Impact on Employee Integrity and Confidence in Desjardins was significantly impacted according to the result of the primary analysis, which was analyzed and tested in hypothesis two. In secondary data analysis, the breach weakened employee morale, created a culture of suspicion, and increased stress levels in the organization. This finding aligns with Herath and Rao (2009), who maintain that data breaches can diminish and erode organizational trust, confidence, and psychological safety. Because the breach was attributed to an insider, the employees were subjected to increased scrutiny and supervision, leading to feelings of demotivation and distrust in leadership and vice versa. The breach exposed weaknesses and vulnerabilities in the organization's internal control and internal data protection and security practices, stressing the urgency for continuous training, cybersecurity awareness, and robust policy standards and ethical frameworks to reinforce employee integrity.

Desjardins incident and crisis management were effective. The management responded immediately by public disclosure, notifying the Office of the Privacy Commissioner of Canada and affected customers [32]. The enhancement and improvement in cybersecurity infrastructure and IT general controls after the incident demonstrated seriousness and commendable commitment to managing in the future if a similar incident occurs effectively. The breach exposed weaknesses and vulnerabilities in the organization's readiness, incident response, and business continuity planning [34]. This finding further emphasized the importance of proactive risk management strategies, as stated in the NIST Cybersecurity Framework (2018).

Practical Implications

The findings offer several practical implications for business organizations and policymakers, especially those in the financial industry:

1. Improving and Strengthening Cybersecurity Readiness: Businesses should prioritize and establish robust information and cybersecurity governance, risk management, and compliance frameworks to prevent, detect, and promptly respond to data breaches.
2. Employee Engagement: Creating and encouraging a security-conscious environment and culture through

continuous training and responsible, ethical leadership is essential to maintain employee confidence and integrity.

3. Crisis Communication: Prompt, honest, transparent, timely, and empathetic communication during business data breaches can help manage stakeholder expectations and lessen reputational harm.
4. Regulatory Compliance: Regulators must hold businesses accountable and improve their oversight function, especially on those companies that comply with standards like GDPR, PIPEDA, FINTRAC, SOCS, and SOXS, which are compulsory to adhere to data protection to ensure privacy and accountability.
5. Cross-Sector and Industry Collaboration: Information sharing between the public and private sectors should be encouraged, which can improve cybersecurity resilience at the provincial and national levels.

Conclusion and Recommendations

The case of the Desjardins Group data breach serves as a critical case study on the comprehensive impacts of business data breaches beyond financial losses. The incident highlights the importance of detailed and comprehensive cybersecurity governance, proactive risk management, continuous monitoring, and detective mechanisms, as well as the need for organizations to foster a culture of security awareness. The lessons learned from Desjardins' experience provide valuable insights for other organizations seeking to mitigate the risks and consequences of data breaches. Businesses must prioritize technological defenses and cybersecurity's human and cultural aspects to build strong, secure, resilient, and trustworthy institutions.

Insider threats, among other cybersecurity threats, remain the most challenging ones to mitigate because of their complexity and the potential for access and privilege abuse. It is also difficult to distinguish between legitimate access and malicious intent because of its intrinsic difficulty. Comparing this to external threats, which can be more often prevented and mitigated through perimeter defenses and threat intelligence and analytics, insider risks more often exploit the inherent trust within business organizations, which makes detection and prevention mostly challenging.

The Desjardins Group data breach underlines the profound and complicated impacts of business data breaches on organizations, from reputation damage to loss of trust and confidence, and employee integrity. Data breaches corrode brand reputation, compromise employee integrity, and challenge organizational resilience. A holistic approach that consolidates robust and enormous cybersecurity measures, proper and ethical leadership, and a proactive approach to risk management would be required to overcome these challenges. Businesses must understand and recognize that cybersecurity is not just a technical issue but a strategic importance and integral part of the overall business goal that affects all aspects of business operations. Therefore, by learning from past data breaches and incidents, such as the Desjardins case, organizations can better prepare for future threats and cyber-attacks and build a resilient, secure, and trustworthy digital environment and platform.

For Future Research

For future research endeavors, it will be of value to investigate data breaches across various industries to identify sector-specific risks and vulnerability and mitigation strategies, which will expand its applicability. It will also be good to conduct long-term studies to assess the enduring effects of data breaches on brand reputation and employee integrity. It is also good to use quantitative methods to quantify the financial and operational impacts of business data breaches more precisely. That is, finding the correlation between business data breaches and profitability.

Acknowledgments

I sincerely thank Professor Samuel Bodunrin, my guide, for his insightful critique, mentoring, encouragement, and promptness. Professor Sam's wealth of experience in research and teaching has been instrumental and helpful during this research process.

Conflict of Interest

To the best of my knowledge, there is no conflict of interest in conducting this research.

References

[1]. Alazab, M., Broadhurst, R., Bou-Harb, E., & Hutchings, A., 2015, Cybercrime: Risks and Responses. *International Journal of Cyber Criminology*, 9(2), 143-159.

[2]. Arcuri, A., 2015, The Impact of Data Breaches on Customer Trust: A Comparative Analysis. *Journal of Business Ethics*, 127(3), 491-504.

[3]. Barney, J., 1991, Firm Resources and Sustained Competitive Advantage. *Journal of Management*, 17(1), 99-120.

[4]. N. Kshetri, Recent US cybersecurity policy initiatives: challenges and implications, Computer, 48 2015

[5]. D. Massa, R., Valverde, A fraud detection system based on anomaly intrusion detection for E-commerce applications, *Comput Inf Sci*, 7 2024.

[6]. Braun, V., & Clarke, V., 2006, Using Thematic Analysis in Psychology. *Qualitative Research in Psychology*, 3(2), 77-101.

[7]. Cavusoglu, H., Mishra, B., & Raghunathan, S., 2004, The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers. *International Journal of Electronic Commerce*, 9(1), 69-104.

[8]. Gatzlaff, K. M., & McCullough, K. A., 2010, The Effect of Data Breaches on Shareholder Wealth. *Risk Management and Insurance Review*, 13(1), 61-83.

[9]. Gordon, L. A., Loeb, M. P., & Zhou, L., 2010, The Impact of Information Security Breaches: Has There Been a Downward Shift in Costs? *Journal of Computer Security*, 19(1), 33-56.

[10]. Herath, T., & Rao, H. R., 2009, Encouraging Information Security Behaviors in Organizations: Role of Penalties, Pressures, and Perceived Effectiveness. *Decision Support Systems*, 47(2), 154-165.

[11]. ISO/IEC. 2013. ISO/IEC 27001: Information Security Management. *International Organization for Standardization*.

[12]. Lwin, M. O., Wirtz, J., & Williams, J. D., 2017, Consumer Online Privacy Concerns and Responses: A Power-Responsibility Equilibrium Perspective. *Journal of the Academy of Marketing Science*, 35(4), 572-585.

[13]. Mayer, R. C., Davis, J. H., & Schoorman, F. D., 1995, An Integrative Model of Organizational Trust. *Academy of Management Review*, 20(3), 709-734.

[14]. Mitropoulos, S., Patsakis, C., & Douligeris, C., 2006, Incident Response Planning: The Critical Role of Crisis Communication. *Journal of Information Security*, 7(2), 137-147.

[15]. NIST. 2018, Framework for Improving Critical Infrastructure Cybersecurity. *National Institute of Standards and Technology*.

[16]. Ponemon Institute. 2019, Cost of a Data Breach Report 2019. *IBM Security*.

[17]. Ponemon Institute. 2020, 2020 Data Breach Investigations Report. *Verizon*.

[18]. Rogers, R. W., 1975, A Protection Motivation Theory of Fear Appeals and Attitude Change. *Journal of Psychology*, 91(1), 93-114.

[19]. Romanosky, S., 2016, Examining the Costs and Causes of Cyber Incidents. *Journal of Cybersecurity*, 2(2), 121-135.

[20]. Samarati, P., & De Capitani di Vimercati, S., 2001, Access Control: Policies, Models, and Mechanisms. *Foundations of Security Analysis and Design*, 2171, 137-196.

[21]. M. Loganathan, E. Kirubakaran, A study on Cyber Crimes and protection, *Int J Comput Sci Issue*, 18 2021 7-35.

[22]. Stallings, W., 2013, Network Security Essentials: Applications and Standards. *Pearson Education*.

[23]. Von Solms, B., & Von Solms, R., 2004, The 10 Deadly Sins of Information Security Management. *Computers & Security*, 23(5), 371-376.

[24]. Whitener, E. M., Brodt, S. E., Korsgaard, M. A., & Werner, J. M., 1998, Managers as Initiators of Trust: An Exchange Relationship Framework for Understanding Managerial Trustworthy Behavior. *Academy of Management Review*, 23(3), 513-530.

[25]. Yin, R. K., 2014, Case Study Research: Design and Methods. *Sage Publications*.

[26]. Elhoseny, M., Darwiesh, A., El-Baz, A. H., Rodrigues, J. J., Enhancing cryptocurrency security using AI risk management model. *IEEE Consum Electron Mag.* 2023;13(1):48–53. doi: 10.1109/MCE.2023.3238848.

[27]. Osamy, W., Khedr, A. M., Salim, A., AlAli, A. I., El-Sawy, A. A., Recent studies utilizing artificial intelligence techniques for solving data collection, aggregation and dissemination challenges in wireless sensor networks: A review. *Electronics.* 2022;11(3):313. doi: 10. 3390/electronics11030313.

[28]. Amaldi, E., Capone, A., Cesana, M., Filippini, I., Malucelli, F., Optimization models and methods for planning wireless mesh networks. *Comput Networks.* 2008;52(11):2159–71. doi: 10.1016/j.comnet.2008.02.020.

[29]. Bentotahewa, V., Hewage, C., Williams, J., Solutions to Big Data privacy and security challenges associated with COVID-19 surveillance systems. *Front Big Data.* 2021; 4:645204. doi: 10.3389/fdata.2021.645204

[30]. Nawaf, L., Optimizing IoT security by implementing Artificial Intelligence – Infosecurity Magazine; June 2022, [online]. https://www.

[31]. Bago, P., Cyber security and artificial intelligence. *Economy Finance*. 2023;10(2):189–212. doi: 10.33908/ef.2023.2.5.

[32]. Office of the Privacy Commissioner of Canada. 2020, Commissioner's findings: Investigation into Desjardins' handling of a data breach. Office of the Privacy Commissioner of Canada. https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2020/pipeda-2020-005/

[33]. Office of the Privacy Commissioner of Canada. 2020, December 14. Statement from the Privacy Commissioner of Canada on the government's response to the Desjardins investigation. Office of the Privacy Commissioner of Canada. https://www.priv.gc.ca/en/opc-news/speeches-and-statements/2020/s-d_20201214/

[34]. Office of the Privacy Commissioner of Canada. 2020, December 14. The government response to Desjardin's investigation is a step forward, but stronger privacy laws are still needed. Office of the Privacy Commissioner of Canada. https://www.priv.gc.ca/en/opc-news/news-and-announcements/2020/nr-c_20121