The Impact of Technology Expenditure on the Commercial Banks' Profitability in Canada

Zijun Lin[1](✉) and Yunan Wang[2]

[1] Tandon School of Engineering, New York University, New York, USA
zl3555@nyu.edu
[2] Minzu University, Beijing, China

Abstract. The growing cyber threat has created an uncontrollable financial mess for the global banking industry. This paper presents a case study that reviews Canada's largest financial data breach and investigates the spillover effects of cyber attack. To test the cyber investment efficiency of banks in Canada, we collect technology-related expenditures and profitability ratios from six Canadian central banks' annual reports. Moreover, we use a multiple linear regression model to examine the impact of technology spending on the financial performance of Canadian banks. The results show that technology expenditure has a significant negative impact on the financial performance of banks. However, we may find different results in future studies that can include more banks in the sample and obtain more comprehensive data sources.

Keywords: Cyber security · Data breach · Bank performance · Profitability · Technology expenses · Multiple linear regression

1 Introduction

Commercial banks have long relied on innovative digital channels to deliver exceptional customer experiences. The global pandemic has accelerated the adoption of digital banking in Canada because of the imposition of self-quarantine to stop the spread of the virus. According to the 2021 Canada's Internet Factbook by the Canadian Internet Registration Authority, 68% of Canadians chose financial institutions as the type of organization they interacted with most during the pandemic [1]. In recent decades, with the rapid growth of Internet usage, network security and data privacy leakage has been the focus of the industry. The financial sector has long been targeted by cyberattacks as it possesses fuller profiles of clients' confidential data, including but not limited to personal information, credit score, account balance, employment history, and education background. Cyber threats have intensified significantly during the COVID-19 pandemic. As demand for digital platforms with work-from-home policies increases, malicious activities are creating more danger by sending epidemic-related phishing emails and developing applications embedded with malware.

F. Balli et al. (Eds.): ESFCT 2022, AEBMR 226, pp. 220–227, 2022.
https://doi.org/10.2991/978-94-6463-052-7_26

The cost associated with a data breach is enormous. According to the 2021 IBM Cost of Data Breach Report, the average total cost of a data breach in Canada is $5.4 million [2]. The average total cost of a data breach in the financial sector is $5.72 million, second only to the healthcare industry [2]. In recent years, banks have increased spending on technology from $5.27 billion in 2017 to $6.67 billion in 2020 to protect against future costs due to data breaches [3]. However, existing studies have not systematically explained how technology expenditure will affect the profitability of commercial banks [4]. This study begins with a case study to understand the background and spillover effects of data breaches at Canada's most significant financial institutions. Finally, we discuss the relationship between technology expenditure and profitability of commercial banks through statistical analysis.

2 Case Review

2.1 Incident Background

Canadian Imperial Bank of Commerce (CIBC) and Bank of Montreal (BMO) are the two major financial institutions in Canada. The former has served more than 11 million customers in its 150-year history, while the latter has had more than 12 million customers worldwide since it was founded in Montreal 200 years ago [5, 6]. On May 27, 2018, CIBC's Simplii Financial and BMO received emails from an individual claiming possession of over 90,000 personal information from two banks and extorting one million Canadian dollars equivalent cryptocurrency from each bank [7]. The investigation found that BMO discovered that the attacks initially took place between June and December 2017, half a year before the group received the threats. The main reason is the loophole of technical safeguard measures [8]. The breach exposed more than 114,000 accounts, negatively impacting the organization's reputation, customer loyalty and financial performance.

2.2 Spillover Effects on Financial Performance

Islam (2020) found that shareholders' loss of confidence in the performance of an organization leads to an immediate change in share price, leading to irregularities, corporate fines and possible litigation [9]. The aftermath of the cybersecurity breach reflected adversely in the commercial banks' financial performance with no surprise. Both CIBC and BMO experienced the stock price plummeting on the trading market right after the breach announcement in the short term. As shown in Fig. 1, The closing price of BMO shares on the Toronto Stock Exchange fell by 1.90% the day after the violation announcement, from C$101.60 to C$99.67, which was more than the usual range of price movements for the company in a month. CIBC was in a similar situation. Figure 2 reveals the stock closing price went down 1.59% from C$24.6 to C$24.21 on May 29, 2018.

In the long run, banks have to settle lawsuits and spend considerable sums to compensate victims. The Bank of Montreal paid about C$6.85 million to reimburse fraudulent electronic transfers and another C$5.45 million to provide victims with free credit monitoring and identity protection. CIBC proposed a similar plan as BMO did, compensating

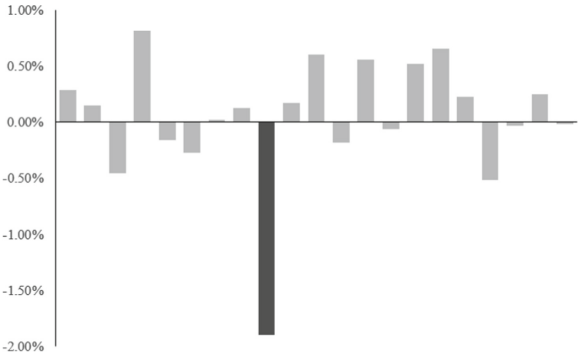

Fig. 1. The Bank of Montreal's Percentage Change in Stock Price from May 15, 2018 to June 14, 2018 in Toronto Stock Exchange

Fig. 2. The Canadian Imperial Bank of Commerce's Percentage Change in Stock Price from May 15, 2018 to June 14, 2018 in Toronto Stock Exchange

affected customers for C$1.78 million in stolen funds, offering free credit tracking and offering gift cards as a thank you and customer retention [10]. The direct cost associated with the breach could reach at least C$28 million for BMO and C$3 million for CIBC. This amount does not include indirect costs such as time spent by incident response related to litigation and investigation of violations [10].

2.3 Hypothesis Development

In fact, investment in information technology will shield commercial banks from compensation related to large-scale cyber attacks, and a company's effective spending on technology may reduce the likelihood of data breaches [11]. However, if companies invest inefficiently in cyber security, they will end up taking greater risks, which will ultimately have a negative impact on company performance [12]. This paper uses data analysis to understand the connection between the technology-related spending in Canadian central banks and profitability in terms of return on asset (ROA), return on equity (ROE), and net interest margin (NIM).

3 Empirical Analysis of the Impact of Technology Expenditure on Profitability

3.1 Data Source and Selection

The research sample includes financial performance statements and technology-related operating expenses for six major banks from 2012 to 2022, yielding 60 observations. The banks include Bank of Montreal (BMO), Canadian Imperial Bank of Commerce (CIBC), Royal Bank of Canada (RBC), Toronto-Dominion Bank (TD), Scotiabank, and National Bank of Canada. We manually extract the secondary data from the commercial banks' financial statements published on the companies' websites and the Canadian Bankers Association database. We collect profitability indicators (ROA, ROE and NIM) as dependent variables, and technology-related operating expenses as independent variables. As the Canadian securities laws currently do not require the banks in Canada to disclose detailed CyberTech-related expenses separately in the income statement, the model includes technology and equipment expenses as the first independent variable. We also take non-interest corporate support costs as the second independent variable which provide financial institutions with information technology support, including data analysis and network security monitoring services. In addition, the data also includes bank size as a control variable. This study adopts the following model to conduct multiple linear regression analysis to test the impact of technology-related expenditures on the profitability of commercial banks.

$$ROA_{i,t} = \alpha + \beta_1 TE_{i,t} + \beta_2 CS_{i,t} + \beta_3 SIZE_{i,t} + \varepsilon \quad (1)$$

$$ROE_{i,t} = \alpha + \beta_1 TE_{i,t} + \beta_2 CS_{i,t} + \beta_3 SIZE_{i,t} + \varepsilon \quad (2)$$

$$\mathrm{NIM_{i,t}} = \alpha + \beta_1 TE_{i,t} + \beta_2 CS_{i,t} + \beta_3 SIZE_{i,t} + \varepsilon \quad (3)$$

$\mathrm{ROA_{i,t}}$: bank i return on average assets at time t (%, net income / average assets).

$\mathrm{ROE_{i,t}}$: bank i return on total shareholders' equity at time t (%, net income / total equity).

$\mathrm{NIM_{i,t}}$: bank i return on net internet income at time t (%, net interest income / average earning assets).

$\mathrm{TE_{i,t}}$: bank i technology/equipment expenses at time t (in billion).

$\mathrm{CS_{i,t}}$: bank i corporate support expenses at time t (in billion).

$\mathrm{SIZE_{i,t}}$: bank i log-normal total asset at time t.

3.2 Data Analysis

Table 1 presents the descriptive statistics result of the dataset. The average ROE is 14.34%, which is significantly higher than the ROA, and the result depends on the business nature of the financial institution and the existence of liabilities. The net interest income margin indicates that the Canadian banks generate 1.87% net interest income from the average earning assets on the benchmark. The data also shows the average

technology-related spending of the sample banks. Of this, spending on technology and equipment are C$1.14 billion, and business support services spending is C$790 million. The sample detects no outliers.

Table 2 reflects the correlation between variables. Technology-related expenditure has a weak negative correlation with bank profitability index. There is no multicollinearity between independent variables and control variables, and the variance inflation factor (VIF) is less than 5.

Table 3 provides the regression results of the sample. Technology and equipment costs are significantly negatively correlated with profitability without considering control variables. At the same time, the enterprise support cost also showed a negative impact, but not significant. We re-run the regression model by adding the control variable bank size. In terms of ROA, the additional control variable improves the effectiveness of corporate support to become significantly correlated with the model within a significance level of 0.1, while it also results in a further significant relationship between ROA and technology expenses. Both independent variables. Technology expenses become more significant within the level of 0.01, while. The same result is found in the NIM model, where enterprise service costs are significantly correlated with NIM at a significance level of 0.1. However, the ROE model shows no considerable significance improvement, as the adjusted R-square of the model decreased by approximately 1% when adding a control variable.

3.3 Result and Limitation

Overall, technology and equipment costs have a significant negative impact on all three profitability measures, regardless of whether control variables are present. The results show that although investment in technology and equipment may be beneficial to the operation of Canadian enterprises, the reduced income of banks due to technology expenditure exceeds the marginal income of investment, which leads to a contradiction [13].

In the absence of control variables, the coefficient of enterprise support expenditure is negative but not significant. The inefficiency can be explained by the insufficient sample size and the broad range the banking corporate support-related expenses. Since these six banks dominate the Canadian banking sector, accounting for more than 90% of the market share of the Canadian banking system, we are only able to collect 60 sample sizes over a 10-year period. Meanwhile, as banks are not required to disclose a detailed breakdown of technology-related service expenses in the income statement, we can only observe the total non-interest costs in the corporate support department. In addition to the spending on cyber security maintenance, the total includes spending not related to network development, such as spending on human resources, internal audit or corporate finance functions. Among the control variables, the bank size is closely correlated with technology cost and enterprise service cost, as shown in Table 2. By including such a control variable, the significance levels for both independent variables improve. However, due to the small sample size of this analysis, the overfitting problem will also lead to the improvement of significance level.

Adding a control variable shows a higher adjusted R-square in ROA and NIM models, but a lower score in the ROE model, because bank size has no significant effect on

Table 1. Descriptive Statistics

	Mean	Median	SD	Min	Max
ROA	0.8254	0.8393	0.1107	0.5200	0.9935
ROE	14.3436	14.0047	2.2915	9.4800	20.0100
NIM	1.8652	1.9106	0.3932	0.8900	2.4200
TE	1.1385	1.1165	0.5274	0.3000	2.3350
CS	0.7934	0.5415	0.8476	-0.2450	2.9470
SIZE	5.8478	5.9128	0.2611	5.2502	6.2377

Table 2. Correlation Matrix

	ROA	ROE	NIM	TE	CS	SIZE	VIF
ROA	1						
ROE	0.6704	1					
NIM	0.1524	-0.4065	1				
TE	-0.3265	-0.2827	-0.3653	1			1.5514
CS	-0.1232	-0.0893	-0.2299	0.0895	1		1.1199
SIZE	0.1105	-0.1088	-0.1410	0.5884	0.3072	1	1.6993
VIF				1.5514	1.1199	1.6993	

Table 3. Multiple Linear Regression Result

Variables	ROA	ROA*	ROE	ROE*	NIM	NIM*
TE	-0.0667	-0.1326	-1.2032	-1.5118	-0.2591	-0.3483
P-value	0.0137	0.0000	0.0337	0.0323	0.0057	0.0027
CS	-0.0124	-0.0310	-0.1745	-0.2616	-0.0922	-0.1174
P-value	0.4520	0.0503	0.6141	0.4754	0.1058	0.0504
SIZE	-	0.2353	-	1.1024	-	0.3188
P-value		0.0004		0.4521		0.1800
Adj. R-sq	0.0845	0.2593	0.0519	0.0448	0.1436	0.1561
Significance F	0.0302	0.0002	0.0819	0.1366	0.0045	0.0058

ROE. Comparing the results from different models, ROA is the most dependent on the technology investment, followed by NIM. Internet investment has the weakest impact on return on equity. Compared with the other two models, bank size and technology have the most significant impact on ROE. Canadian banks cannot grow without capital investment in technology spending, which will be reflected in asset expansion and potential customer base growth [14].

In all, the financial institutions in Canada appear to be raising the awareness of cybersecurity investment to improve their business operation. However, because of the lag effect of cyber technology spending on banks' financial performance, the marginal return brought by technology expenditures still not cover the diminished impact of revenue for banks in Canada. Future research can consider including small Canadian banks as the research object, expand the sample size, and use the future bank performance scale to replace the current year's profitability to eliminate the lagging effect. In addition, it is necessary to collect non-interest itemized expense details from the bank for non-disclosure corporate support departments to eliminate noise in the sample.

4 Conclusion

Ensuring cybersecurity is well-function enough to protect clients against cyber-attacks is a long journey. Due to the data source limitations in detailed disclosures and size in number, we can only observe that technology and equipment expenditure has a significant negative impact on bank performance in terms of profitability in Canada. The lag effect of technology spending and inefficient network investment strategy will reduce the actual impact on income. Future studies can increase the sample size by including small banks and improve data quality by obtaining detailed expense descriptions of banks.

References

1. Canadian Internet Registration Authority, "Canada's Internet factbook 2021," Accessed: Apr. 30, 2022. [Online]. Available: https://www.cira.ca/resources/factbook/canadas-internet-factbook-2021
2. IBM, "Cost of a data breach report 2021," Accessed: May. 6, 2022. [Online]. Available: https://www.ibm.com/downloads/cas/OJDVQGRY
3. M. Tattersall, "How Canadian banks will adapt tech spending for the coronavirus economy," Accessed: May. 24, 2022. [Online]. Available: https://www.businessinsider.com/how-canadian-banks-will-adapt-tech-spending-amid-pandemic-2020-11
4. S. Walton, P. R. Wheeler, Y. Zhang, and X. Zhao, "An integrative review and analysis of cybersecurity research: current state and future directions," J. Inf. Syst., vol. 35, no. 1, pp. 155–186, May. 2020, Art. no. 100170, doi: https://doi.org/10.2308/ISYS-19-033.
5. "CIBC quick facts." The Canadian Imperial Bank of Commerce. https://www.cibc.com/en/about-cibc/corporate-profile/quick-facts.html (accessed May. 7, 2022)
6. "About BMO." The Bank of Montreal. https://www.bmo.com/main/about-bmo/ (accessed May. 7, 2022)
7. J. Bradshaw, "Federal privacy commissioner says BMO security breach in 2017 affected 113,000 client accounts." The Globe and Mail. https://www.theglobeandmail.com/business/article-federal-privacy-commissioner-says-bmo-security-breach-in-2017-affected/ (accessed May. 8, 2022).
8. Office of the Privacy Commissioner of Canada, "Security deficiencies at BMO lead to large-scale breach," Accessed: May. 8, 2022. [Online]. Available: https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2021/pipeda-2021-003/#toc5

9. R. Islam, "The impact of data breaches on stock performance," Glucksman Inst. for Res. in Securities Markets, Leonard N. Stern School of Bus., New York Univ. New York, USA, 2020 [Online]. Available: https://www.stern.nyu.edu/sites/default/files/assets/documents/Islam_Glucksman%20Paper_final_200520.pdf
10. H. Solomon, "Two Canadian banks could pay up to $23 million to settle lawsuits in 2018 hacks." IT World Canada. https://www.itworldcanada.com/article/two-canadian-banks-could-pay-up-to-23-million-to-settle-lawsuits-in-2018-hacks/446673 (accessed May. 10, 2022).
11. C. M. Angst, E. S. Block, J. D'Arcy, and K. Kelley, "Why do IT security investments matter? Accounting for the influence of institutional factors in the context of healthcare data breaches," MIS Q., vol. 32, no. 2, pp. 314–341, Aug. 2015, doi: https://doi.org/10.1080/07421222.2015.1063315.
12. R. Sen and S. Borle, "Estimating the contextual risk of data breach: an empirical approach," J. Manag, Inf. Syst., vol. 41, no. 3, pp. 893–916, 2017, doi: https://doi.org/10.25300/MISQ/2017/41.3.10.
13. Z. He, S. Jiang, D. Xu, and X. Yin, "Investment in lending technology: IT spending in banking," working paper, Becker Friedman Inst., Univ. of Chicago. Chicago, IL, USA, 2021 [Online]. Available: https://bfi.uchicago.edu/working-paper/investing-in-lending-technology-it-spending-in-banking/
14. Canadian Bankers Association, "Focus: bank revenues and profits," Accessed: May. 11, 2022. [Online]. Available: https://cba.ca/bank-revenues-and-earnings-profits