Profile of Canadian Businesses who Report Cybercrime to Police

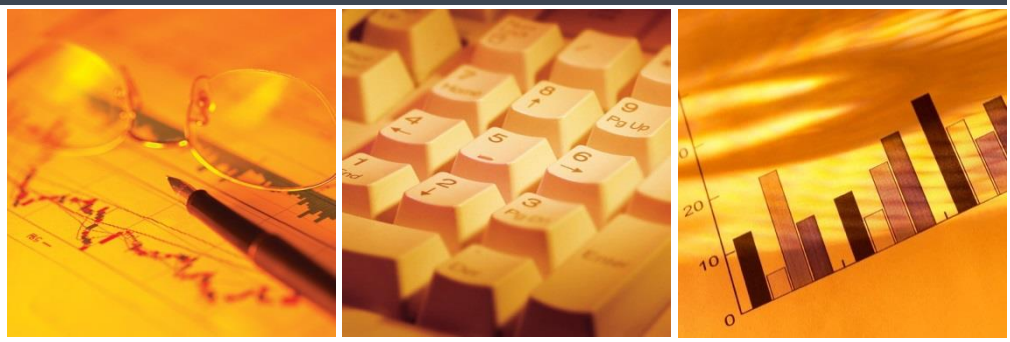
The 2017 Canadian Survey of Cyber Security and Cybercrime

by Kayla A. Wanamaker

RESEARCH REPORT: 2019–R006

RESEARCH DIVISION

www.publicsafety.gc.ca



BUILDING A **SAFE** AND **RESILIENT CANADA**

Public Safety Canada | Sécurité publique Canada

Canada

Abstract

Cybercrime – crimes where the Internet and information technology (IT) are used, such as hacking, virus dissemination, and organized crime – is a growing concern for governments, organizations, individuals and businesses worldwide. Research conducted in the United States, United Kingdom and Canada has concluded that cybercrime and cyber security incidents are underreported to law enforcement. The reasons why this is the case, however, are not well known, especially within a Canadian context. As such, the goal of the current study was to examine the phenomenon of underreporting of cyber security incidents to police services using data from the 2017 Canadian Survey of Cyber Security and Cybercrime that was administered to Canadian businesses. Results indicated that while just over 20% of businesses experienced cyber-related incidents, only about 10% are reporting these incidents to the police. Businesses did not report incidents because they were resolved internally or through an IT consultant, or were thought to be too minor to report to police. Risk management, formal training, and sharing best practices were found to be related to businesses' likelihood of reporting incidents to police. Larger businesses were more likely to report cybercrime to police when they implemented less security measures, whereas scores on security measures were not related to police reporting for small businesses. Results suggest a need to increase awareness of the frequency of cybercrime, as well as the availability of formal training options on cyber-related issues. They also underscore the importance of having enhanced cyber security protocols in place.

Author's Note

The views expressed are those of the author and do not necessarily reflect those of Public Safety Canada. Correspondence concerning this report should be addressed to:

Research Division
Public Safety Canada
340 Laurier Avenue West
Ottawa, Ontario
K1A 0P8
Email: PS.CSCCBResearch-RechercheSSCRC.SP@canada.ca

Acknowledgements

The author wishes to thank the Investment, Science and Technology Division at Statistics Canada for conducting the Canadian Survey of Cyber Security and Cybercrime and providing their support. The author would also like to thank the National Cyber Security Directorate at Public Safety Canada for their ongoing support and advice related to cyber security and cybercrime.

Product Information:

Cat. No.: PS18-51/2019E-PDF
ISBN Number: 978-0-660-33576-6

Table of Contents

Introduction

Cybercrime, including hacking, virus dissemination, and organized crime using the computer is a growing concern for governments, organizations, individuals, and businesses worldwide (Kshetri 2010). It poses a range of economic and social impacts on businesses (Kaplan, Sharma and Weinberg 2011). Due to the widespread use of technology and the digitization of economic activities, businesses are increasingly becoming concerned about their systems and network security (Kaplan et al. 2011; Kshetri 2010). A cyber security risk report conducted by AON (2019) indicates that increased connectivity leads to new and amplified security vulnerabilities. As such, businesses are now more concerned about being victims of cybercrime than physical crime (Keizer 2006).

Research conducted by McAfee (2018)[1] demonstrates the large financial impact that cybercrime has had, with cybercrime costing the world almost $600 Billion dollars (US). This may be due to the fact that cybercrime is becoming such a common experience, with nearly two-thirds of people who use online services having experienced it in some form. Also, those who commit cybercrime are often not prosecuted or even caught (McAfee 2018).

Most research looking at the impact of cybercrime has thus far been conducted in the United States (e.g., Norton 2018). The exact level of cybercrime in Canada is not known, primarily because organizations are not required to report data breaches (Soloman 2018), although research is emerging (e.g., Statistics Canada, 2018a).

An abundance of research has concluded that cyber offences are underreported (Department for Digital, Culture, Media and Sport, 2018, Kethineni and Cao 2019; Rantala 2008; Statistics Canada 2018a; Sukhai 2004). Research has indicated that companies refrain from reporting crimes due to several reasons including: a belief that the incident is not severe enough; a fear of bad publicity, which would affect public trust (Soloman 2016; Sukhai 2004) and business credibility (Kshetri 2010); disruptions due to a potential investigation (Sukhai 2004); and because compensation is not guaranteed (Khalid 2004).

Although there may be several reasons why cybercrime goes unreported generally, it is essential to understand the specific reasons behind why certain Canadian businesses do not report cyber-related crimes, the factors that may increase the likelihood of reporting a cyber incident, and the profiles of businesses who report cyber incidents. By obtaining a better understanding of who reports and their incentives for reporting, cybercrime and national security policy makers and law enforcement agencies can be better equipped to address the issues around underreporting. As such, the current study uses data from the 2017 Canadian Survey of Cyber Security and Cybercrime (CSoCC), the first survey of its kind in Canada. It was administered to Canadian businesses in 2018 to identify the number and percentage of businesses who report cybercrime to authorities, the reasons behind why cybercrimes are not reported, and the characteristics of businesses who report cybercrimes in comparison to those that do not in order to be able to make predictions.

[1] In partnership with the Center for Strategic and International Studies.

Method

Canadian Survey of Cyber Security and Cybercrime

The 2017 CSoCC was conducted on behalf of Public Safety Canada (PS) in partnership with Statistics Canada. Data were collected from January to April 2018. The goal of the survey was to collect Canadian business data on cyber security prevention measures, experiences of cybercrime, and activities to mitigate the effects of cybercrime across small, medium, and large businesses. The survey included 35 questions assessing several main areas including business characteristics, the cyber security environment (e.g., security measures currently in place), cyber security readiness (e.g., the risk management arrangements that are currently in place), business resilience (e.g., cyber security risks and/or threats that are considered most detrimental to a business), cost to prevent or detect cyber security incident(s), information about cyber security incident(s) (e.g., how businesses were impacted by cyber security incidents), reporting cyber security incident(s), and the cost of recovering from cyber security incident(s). For more information on the results of this survey, see Statistics Canada (2018a). Notably, this type of data had not previously been collected in Canada, and as such, this data will act as a benchmark for future surveys and data collection strategies.

Questionnaire Development and Testing

The CSoCC was designed by Statistics Canada through consultation with various government agencies including PS, as well as police agencies, subject matter experts, academics, private businesses, and business associations. After creating an initial survey, two rounds of questionnaire testing were conducted whereby 48 randomly selected businesses from Montreal, Ottawa, Toronto, and Vancouver were asked to identify any issues with the questionnaire in terms of content and flow. Additionally, meetings were held with Information Technology (IT) managers to assess the information being captured and the language being used in the questionnaire. Overall, the questionnaire was refined to the 35 questions used for this study (Statistics Canada, 2018b). The survey was designed to be completed in 30 minutes and referred to incidents/security questions that occurred the prior year (January to December 2017).

Survey Sample

An electronic version of the survey was administered and data were collected from businesses with Canadian operations and with 10 or more employees, across all sectors except for government and public administration. Businesses that had under $100,000 revenue (or $250,000 in some cases, depending on the sector), were excluded. The survey was sent to either IT management or a senior staff member with the most knowledge of the cyber security practices of the business. A total of 12,597 businesses were sampled, drawn from a population of 194,569 businesses across Canada; the response rate was 86% resulting in a final sample size of 10,794 businesses. Approximately 44.9% of the respondents were small businesses, 35.5% medium businesses, and 19.6% large businesses.[2] Notably, responses were weighted based on how many businesses of a particular size (by employee counts) exist in the population. As such, because

[2] Businesses were considered small if they consisted of 10 to 49 employees, medium if they consisted of 50 to 249 employees, and large if they consisted of 250 or more employees.

there are more small businesses in the economy, the majority of the weight was held by small businesses.

Data Analysis

Frequencies were examined across the various business sizes (and overall) on various items on the survey related to reporting incidents to police (see Table 1A in Appendix A). This was followed by an analysis of variance to examine whether there were differences between the business sizes related to reasons for not reporting cyber incidents (see Table 2A in Appendix A). In addition, means, standard deviations and t-tests were examined which compared businesses who reported cyber incidents to police to businesses that did not report incidents to police (see Table 3A in Appendix A).

Finally, to examine whether there are distinct characteristics of businesses who report cyber security incidents to police services, and whether there were certain factors that were related to why businesses did or did not report cybercrime to police, logistic regression analyses were conducted (see Table 4A in Appendix A). This was examined across the different business sizes. Specifically, business size was examined as a moderator (whereby small businesses were compared to medium/large businesses) to determine if certain factors were more predictive of reporting cyber incidents to police for businesses that were smaller versus larger and vice versa. Four predictor variables were included in the regression analyses. These variables were created by adding together yes/no responses from a subset of items from the survey:

- *Risk management protocols.* Scores on the risk management protocols variable range from 0 to 7, with higher scores indicating more risk management protocols put in place by the business. This variable is made up of 7 yes/no items (e.g., does the business have a written policy in place? Does the business have a continuity plan?). The reliability was found to be adequate ($\alpha = .68$).
- *Formal training offered by businesses.* Scores on the formal training variable range from 0 to 3, with higher scores indicating more formal training mechanisms put in place by the business. This variable is made up of 3 yes/no items (e.g., does the business provide training to internal IT? To other employees? To stakeholders?). The reliability was found to be adequate ($\alpha = .69$).
- *Cyber security measures put in place.* Scores on the cyber security measures variable range from 0 to 11, with higher scores indicating more security measures put in place by the business. This variable is made up of 11 yes/no items (e.g., does the business have mobile security? Network security? Does the business have identity management?). The reliability was found to be very good ($\alpha = .87$).
- *Business sharing best practices with employees and IT personnel.* Scores on the sharing best practices variable ranges from 0 to 2, with higher scores indicating that best practices are shared with employees. This variable is made up of 2 yes/no items (e.g., does the business share best practices with employees?). The reliability could not be assessed as it is based solely on two items.

Results

The results are described in two main sections; the first section highlights the frequencies of various questions on the survey that are of particular interest in this report (including frequencies of businesses who reported cyber incidents to police, why businesses did not report the incident(s) to police, and the types of incidents most often reported to police). This section also highlights the differences and similarities between the business sizes in terms of responses on the survey. The second section highlights results from the logistic regression analyses, detailing the variables that may be most predictive of reporting incidents to police.

Descriptive Analyses and Business Size Differences

One-fifth of businesses experienced a cyber incident

Approximately 20.8% of businesses experienced some form of cyber incident, which included 18.8% of small, 28.0% of medium, and 41.0% of large businesses (see Table 1A in Appendix A).

Less than ten percent of businesses report cyber incidents to police

In terms of reporting the incident(s) to police, only 9.6% of businesses engaged in this practice, which consisted of 8.4% of small businesses, 12.5% of medium businesses, and 15.0% of large businesses. Overall, only 6.3% of businesses reported all cyber security incidents to police (small = 6.3%, medium = 6.2%, large = 7.6%) (see Table 1A in Appendix A).

Cyber incident reports to police consisted of stealing personal or financial information

The cyber security incident reports that police most commonly received (based on this survey data) were the same for small, medium and large businesses, consisting predominately of incidents to steal money or demand ransom payments (reported by 26.5% of businesses), incidents to steal personal or financial information (reported by 17.4% of businesses), incidents to access unauthorized areas (reported by 15.6% of businesses), or because of an unknown motive (reported by 9.5% of businesses).

Over half of businesses resolve cyber incidents internally rather than report to police

Importantly, businesses did not report incidents to police because: incidents were resolved internally (52.1%), incidents were resolved through an IT consultant (32.5%), incidents were thought to be too minor to report to police (29.1%), the business did not think to contact the police (23.5%), the business thought the police service would not consider the incident important enough (18.8%), the business did not want to invest additional time/money on the issue (14.2%), and/or the business did not think the perpetrator would be adequately punished/convicted (12.3%) (see Table 2A in Appendix A).

Larger businesses refrain from reporting cyber incidents for different reasons than medium and small businesses

There are some similarities and differences across business sizes in terms of reasons for not reporting cyber incidents to police (see Table 2A in Appendix A). For instance, large businesses (70.3%) were more likely to indicate that incidents were resolved internally in comparison to

medium (55.3%) or small businesses (50.0%). Similarly, incidents were resolved through an IT consultant more for small (33.5%) and medium businesses (32.4%), rather than for larger businesses (18.0%). Large businesses (42.2%) were more likely to indicate that their cyber incident was too minor to report to police than small (25.4%) and medium businesses (38.7%). More small businesses (24.6%) indicated that they did not think to call the police about the cyber incident in comparison to medium (21.6%) or large (15.0%) businesses. In addition, almost a quarter of large businesses (23.0%) did not think that police services would consider their incident important, compared to 20.8% of medium and 18.0% of small businesses.

Predicting Incident Reporting to Police Services

Businesses that report cyber incidents have more protective mechanisms in place

Businesses that reported cyber incidents to police tended to have more risk management protocols put in place, more formal training mechanisms, had more cyber security measures put in place, and engaged in sharing a number of best practices with employees and IT, in comparison to businesses who did not report cyber incidents to police (see Table 3A in Appendix A).

The logistic regression confirmed the importance of risk management protocols, formal training, cyber security measures, best practices, and business size when predicting business likelihood of reporting cyber incidents to police (see Table 4A in Appendix A).

Business size influences when and why incidents are reported to police

The size of a business also influenced the likelihood of reporting a cybercrime to police with large and medium businesses more likely to report than smaller businesses (see Table 4A in Appendix A). Larger businesses were more likely to report cybercrime to police when they implemented less security measures, whereas scores on security measures were not related to police reporting for small businesses. Small businesses were less likely to report cybercrime to police when they implemented best practices. Both larger and smaller businesses were more likely to report cybercrime to police when there were more formal training measures put in place. Finally, all businesses (regardless of size) were more likely to report cybercrimes to police when they implemented more risk management practices.

Discussion

With the increase in reliance on technology, businesses are also increasingly becoming concerned with their systems and network security (Kaplan et al. 2011; Kshetri 2010). While the exact level of cybercrime in Canada is not known, research has concluded that cyber offences are underreported (Kethineni and Cao 2019; Rantala 2008; Statistics Canada 2018a; Sukhai 2004). While cyber security incidents are going unreported the reasons for this are not well known, especially within a Canadian context. As such, the goals of the current study were to examine the number of businesses that report cybercrimes to authorities, the reasons for reporting, and the characteristics of businesses who report cybercrime in comparison to those that do not, using data from the 2017 CSoCC that was administered to Canadian businesses.

Summary of Results

Overall results indicate that just over 20% of businesses are experiencing a cyber incident, with larger businesses indicating experiencing more cyber incidents than smaller businesses; however, very few businesses are reporting the incident(s) to police. The main reasons why businesses are refraining from reporting to police are because: the majority of incidents were resolved internally or through IT consultants, the incident was thought to be too minor to report, or the businesses did not consider reporting to police (i.e., did not think to contact the police).

Generally, risk management, formal training, and sharing best practices were found to be related to reporting incidents to police. More specifically, as businesses increased their risk management protocols and formal training, the likelihood of reporting incidents to police also increased. Interestingly, as sharing best practices increased, the likelihood of reporting to police decreased. However, this may be due to the fact that the best practices variable was only based on two items and may not be comprehensive enough to adequately gauge sharing best practices among businesses.

Policy Implications

The high rates of cyber-related incidents experienced by Canadian businesses suggest the importance of improving awareness around the frequency of cybercrime and the need for businesses to have enhanced cyber security. Although small businesses may not have the resources necessary to provide formal training initiatives for their employees and IT personnel, it is nonetheless important to improve awareness around formal training options and programs that may be broadly available for businesses around cyber safety and cyber security.

One of the main reasons why businesses failed to report cybercrime was because they did not think the police would consider the cyber incident important (approximately 20% of businesses listed this as a reason for not reporting to police). Approximately 20% of businesses also stated that they did not think to contact the police about their cyber incidents. As many businesses did not report incidents to police due to the level of severity (e.g., minor incident), this demonstrates that these businesses may not fully understand the criminal implications of cyber-related incidents, indicating further need to improve awareness. As such, more public awareness is required regarding the importance of reporting to police, regardless of how minor an incident is considered to be. Further, since smaller businesses are least likely to report cyber-related incidents, perhaps education should be targeted towards those smaller businesses and future policy and programs can find a way to incentivize businesses to report to police.

Limitations and Future Directions

Given that this is the first national survey distributed by Statistics Canada on cybercrime and cyber security, there are some limitations that should be discussed. For instance, results could not be disaggregated by industry type due to the small sample of businesses who reported incidents to police. Future research is needed looking at the differences across industry types in terms of frequency of reporting to police, reasons for reporting to police and variables that may be related to why businesses report to police (e.g., more formal training, etc.). Future iterations of the survey are needed to examine how reporting to police may change over time and across various business sizes and types. This would help identify gaps in services and policies that are put in place, especially with the ever-changing cyber world. More research is also needed on businesses

reporting to third parties in comparison to businesses who report incidents to police in order to obtain a fuller picture on how businesses react to cyber-related incidents. Finally, it would be relevant to distinguish between insider business cybercrime, and cybercrime that is external in origin.

Conclusion

The current study offers some information around why some businesses are more likely to report to police and the types of incidents that are being reported to police. Importantly, only one-tenth of all businesses who experienced an incident are actually reporting incidents to police. By understanding not only the reasons why businesses are not reporting incidents but also understanding factors that may increase the likelihood of reporting to police, we can gain a better sense of businesses that are most at risk of experiencing a cyber-incident and target the appropriate businesses in terms of prevention efforts, providing services, and awareness campaigns. The CSoCC is the first survey of its kind and offers valuable information to Canadian businesses, governments, and the general population. Examining data from future iterations of the survey will help to decipher trends, and guide research and policy efforts.

References

AON. (2019, February). *2019 Cyber Security Risk Report: What's Now and What's Next*. Retrieved from https://www.aon.com/mwginternal/de5fs23hu73ds/progress?id=tHMHtR8q0_OmcVHKqQhUwNWef9bxKiiL99rvl3blz4,&dl

Department for Digital, Culture, Media and Sport. (2018). *Cyber Security Breaches Survey 2018: Statistical Release*. Department for Digital, Culture, Media and Sport. United Kingdom.

Kaplan, J., Sharma, S., & Weinberg, A. (2011, June). *Meeting the Cybersecurity Challenge.* Retrieved from https://www.mckinsey.com/business-functions/digitalmckinsey/our-insights/meeting-the-cybersecurity-challenge

Keizer, G. (2006, January). *Cybercrime feared 3 times more than physical crime*. Information week.

Kethineni, S., & Cao, Y. (2019). The rise in popularity of cryptocurrency and associated criminal activity. *International Criminal Justice Review* (advance online publication), 1-20. doi: 10.1177/1057567719827051

Khalid, A. (2004, March). *Cyber crime: Business and the law on different pages*. The Star. Retrieved from http://www.niser.org.my/news/2004_03_05_01.html

Kshetri, N. (2010). *The Global Cybercrime Industry: Economic, Institutional and Strategic Perspectives*. New York, NY: Springer. doi: 10.1007/978-3-642-11522-6

McAfee. (2018, February). *The Economic Impact of Cybercrime—No Slowing Down.* Santa Clara, CA. Retrieved from https://www.mcafee.com/enterprise/eus/assets/executive-summaries/es-economic-impact-cybercrime.pdf

Norton. (2018). *2017 Norton Cyber Security Insights Report: United States Results.* Symantec, CA: USA. Retrieved from https://www.symantec.com/content/dam/symantec/docs/ about/ 2017-ncsir-united-states-results-en. pdf

Rantala, R. R. (2008, September). *Cybercrime Against Businesses, 2005.* Washington, D.C.: U.S. Department of Justice; Bureau of Justice Statistics. Retrieved from http://www.justiceacademy.org/iShare/Library-BJS/CyberCrimes.pdf

Soloman, H. (2016, June). *Firms too scared to report cyber crime, says police investigator*. IT World Canada: Toronto, Ontario. Retrieved from https://www.itworldcanada.com/article/ firms-too-scared-to-report-cyber-crime-says-police-investigator/383747

Soloman, H. (2018, February). *Cyber crime costs the world almost US$600 billion a year: Report.* IT World Canada: Toronto, Ontario. Retrieved from https://www.itworldcanada.com/article/cyber-crime-costs-the-world-almost-us600-billion-a-year-report/402038

Statistics Canada. (2018a, October). *The Daily: Impact of cybercrime on Canadian businesses, 2017*. Ottawa, Ontario. Retrieved from https://www150.statcan.gc.ca/n1/daily-quotidien/181015/dq181015a-eng.htm

Statistics Canada. (2018b). *Canadian Survey of Cyber Security and Cybercrime* (Survey). Ottawa, Ontario. Retrieved from http://www23.statcan.gc.ca/imdb/p3Instr.pl?Function=assembleInstr&Item_Id=418254

Sukhai, N. B. (2004, October). Hacking and Cybercrime. In *Proceedings from the 1st Annual Conference on Information Security Curriculum Development* in Kennesaw, GA. doi: 10.1145/1059524.1059553

Appendix A – Summary Tables

Table 1A

Frequency of cyber incidents and reporting of incidents to police by business size

Frequency	Total %	Business Size		
		Small %	Medium %	Large %
Experienced a cyber incident	20.8	18.8	28.0	41.0
Reported a cyber incident to police	9.6	8.4	12.5	15.0
Reported all experienced cyber incidents to police	6.3	6.3	6.2	7.6

Note. Businesses were considered small if they consisted of 10 to 49 employees, medium if they consisted of 50 to 249 employees, and large if they consisted of 250 or more employees.

Table 2A

Comparing reasons why businesses did not report cyber incidents to police across small, medium, and large businesses

Reason for not reporting cyber incident to police	Total	Business Size			
		Small	Medium	Large	
	%	%	%	%	*F*
Incident resolved internally	52.1	50.0	55.3	70.3	221.38**
Resolved through IT consultant	32.5	33.5	32.4	18.0	113.64**
Too minor of an incident	29.1	25.4	38.7	42.2	196.78**
Didn't think to contact police	23.5	24.6	21.6	15.0	143.73**
Didn't think police service would consider it important	18.8	18.0	20.8	23.0	170.02**
Didn't want to spend more time/money on the issue	14.2	15.2	11.4	12.2	155.72**
Didn't think perpetrator would be adequately punished	12.3	13.2	9.9	8.5	158.09**
Lack of evidence	9.3	8.2	12.8	10.0	173.34**
Reporting process too complicated	3.8	3.8	3.7	4.4	174.00**
Police response unsatisfactory in the past	2.5	2.3	2.9	3.8	176.33**

Note. Reasons for not reporting are not mutually exclusive; businesses could indicate several reasons for not reporting incidents to police. As such, percentages will not add up to 100%. Businesses were considered small if they consisted of 10 to 49 employees, medium if they consisted of 50 to 249 employees, and large if they consisted of 250 or more employees. $^{**}p < .001$

Table 3A

Comparing scores on various cyber protective mechanisms for businesses that reported an incident versus businesses that did not report an incident

	Reported Incident		**Did not Report Incident**		
Protective mechanisms	***M***	***SD***	***M***	***SD***	***t***
Risk Management Protocols (Range: 0-7)	3.02	1.89	2.30	1.43	-28.41**
Formal Training (Range: 0-3)	1.04	1.01	.50	.83	-37.04**
Cyber Security Measures (Range: 0-11)	7.03	2.90	6.29	2.98	-14.60**
Sharing Best Practices (Range: 0-2)	1.29	.91	1.18	.87	-7.11**

Note. M = mean. *SD* = Standard deviation. *t* = t test results. This refers to police reported incidents; does not include incidents reported to third parties. ***p* < .001

Table 4A

Logistic regression results predicting businesses likelihood of reporting cyber incidents to police

Predictor variables	***b* (*SE*)**	**χ^2**	**OR**	**95% CI**
Risk management protocols	.20 (.02)	121.64***	1.22	[1.18, 1.26]
Formal training offered	.60 (.03)	482.86***	1.83	[1.73, 1.93]
Cyber security measures	-.01 (.01)	.35	1.00	[1.00, 1.01]
Sharing best practices	-.44 (.03)	203.74***	1.55	[1.46, 1.64]
Business size	.30 (.05)	38.28***	1.34	[1.22, 1.48]
Interactions				
Risk management x business size	-.02 (.03)	.59	1.02	[.97, 1.08]
Formal training x business size	-.11 (.05)	6.14*	1.12	[1.02, 1.22]
Security measures x business size	-.08 (.02)	20.87***	1.08	[1.05, 1.12]
Best practices x business size	.55 (.07)	73.10***	1.74	[1.53, 1.97]

Note. b = regression coefficient. SE = Standard error. χ^2 = Wald's chi square. OR = Odds Ratio. CI = Confidence Interval. *$p < .05$, ***$p < .001$