The Paradox of Cybercrime Risk and Internet Use in Canada: A Socio-Criminological Perspective

A Dissertation Submitted to the

College of Graduate and Postdoctoral Studies

In Partial Fulfillment of the Requirements

For the Degree of Doctor of Philosophy

In the Department of Sociology

University of Saskatchewan

Saskatoon

By

Mohammed Awal Abdulai

PERMISSION TO USE

In presenting this thesis/dissertation in partial fulfillment of the requirements for a Postgraduate degree from the University of Saskatchewan, I agree that the Libraries of this University may make it freely available for inspection. I further agree that permission for copying of this thesis/dissertation in any manner, in whole or in part, for scholarly purposes may be granted by the professor or professors who supervised my thesis/dissertation work or, in their absence, by the Head of the Department or the Dean of the College in which my thesis work was done. It is understood that any copying or publication or use of this thesis/dissertation or parts thereof for financial gain shall not be allowed without my written permission. It is also understood that due recognition shall be given to me and to the University of Saskatchewan in any scholarly use which may be made of any material in my thesis/dissertation.

DISCLAIMER

Reference in this thesis to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by the University of Saskatchewan. The views and opinions of the author expressed herein do not state or reflect those of the University of Saskatchewan, and shall not be used for advertising or product endorsement purposes.

Requests for permission to copy or to make other uses of materials in this thesis/dissertation in whole or part should be addressed to:

Head of the Sociology Department

1019-9 Campus Drive

University of Saskatchewan

Saskatoon, Saskatchewan S7N 5A5 Canada

OR

Dean

College of Graduate and Postdoctoral Studies

University of Saskatchewan

116 Thorvaldson Building, 110 Science Place

Saskatoon, Saskatchewan, S7N 5C9 Canada

Abstract

Increased internet use has created opportunities for criminality. Internet penetration is soaring against the backdrop of the increased risk of cybercrime victimization. A mixed method approach is employed in this study to examine why Canadians continue to use the internet, notwithstanding the fear and persistent or inherent risk of victimization in cyberspace, through the lens of the structure and agency discourse. In other words, has the perception of cybercrime victimization changed internet use? Questions explored include: internet users' knowledge and perceptions of risk, their attitude to internet security, fear of cybercrime and victimization experiences and its impact on behavior, attitude towards reporting, frequency of internet use and effect on behavior, and motivation for internet use. The study utilizes an integrated theoretical framework comprising risk, structuration, and rational choice. Canada-wide data was collected using an online survey. Logistic regression is used to construct models for each outcome variable, while internet use motivation is analyzed using thematic qualitative analysis.

The findings indicate that socio-demographic characteristics such as gender, level of education, and marriage are associated with the risk of cybercrime. While victimization experience is significantly negatively associated with cybercrime fear, it is not significantly associated with cybercrime risk perception. The effect of victimization on internet behavior constraints in terms of avoidance and defensive internet use is inconclusive; similarly, there is an inconclusive relationship between fear of cybercrime and cybercrime incident reporting. It is unclear whether internet use frequency constrains the behavior of internet users, even though the univariable results suggest that frequent internet users have increased odds of adopting avoidance and defensive internet use actions. Thematic analysis revealed motivations for internet use to include education and knowledge acquisition, entertainment and fun, communication and social media access, commercial purposes, work and personal related reasons, news and information access, and others. The thematic results demonstrate that an intricate interaction between structure and agency underpins Canadians' motivations for using the internet.

Based on the findings, the study argues for greater theoretical flexibility to understand the apparent paradox between internet use and cybercrime risk. The results have implications for theory, policy and practice, including for cyberspace offending, victimization, and crime control.

Acknowledgement

I am eternally grateful to the Almighty God for His protection and blessings of good health, strength, and the conviction to see through this research.

Next, I am exceedingly grateful to my supervisor, Dr. Hongming Cheng, for his unflinching support and guidance and for his confidence in my ability to execute this study. I am also thankful to my advisory committee members: Dr. Carolyn Brooks, Dr. John Hansen, and Dr. Mark Olver, for their encouragement and constructive feedback. Your support has been invaluable in my young academic journey. Thank you also to my external examiner, Dr. Steven Kohm, for agreeing to review my work and for the constructive comments.

I also thank the Canadian Hub for Applied and Social Research (CHASR) at the University of Saskatchewan for deploying my survey instrument and facilitating the data collection. I am also thankful to the Centre for Forensic Behavioral Science and Justice Studies (CFBSJS) for their generous financial support (scholarship) for the data collection. I also want to thank my friend and brother, Ibrahim Watara, for his invaluable insight and support during the data analysis phase. A special thank you to Joanie Crandall for proofreading my work and for the encouragement and support all these years. I appreciate and will not forget it.

A special thank you also to Dr. Oral Robinson for the mentorship and guidance every step of the way. A heartfelt thank you to my brother from another mother, Dr. Puneet Kapur. You have been an intrinsic part of everything, and this journey would have remained a mirage but for you.

Finally, I want to thank all my family, friends, and everyone who has supported my work and enriched my experience. It has been a whirlwind of a journey, and I am forever grateful.

DEDICATION

I dedicate this work to the memory of my sweetest late mother;

my first and ultimate love.

Table of Contents

List of Tables

List of Figures

Chapter One: Introduction

1.0 Introduction

This chapter provides a general outline of the research. First, I present an outline of the research background and an overview of the issue. I follow this with a definition of the research problem and an examination of the research problem statement. Next, I present the research questions and follow up with the study's rationale and justification. I follow with a quick justification of the research site and conclude with the organization of the dissertation.

1.1 Overview/The Issue

Technological developments have spurred massive transformations in society. Such changes mean the interface of human interactions – social, economic, educational, political, healthcare, etc. – is increasingly changing, from the physical sphere to the cybersphere (cyberspace). For example, cyberspace now provides a convenient outlet for entertainment and interaction through social media while students and faculty complete academic work using online search databases. Also, consumers perform daily shopping and banking needs using online shopping and online banking while doctors maintain prescriptions and sensitive client information online, etc. In other words, internet use has become so commonplace that one can begin to see it as an act of compulsive behavior that people indulge in without conscious volition. However, such a position could equate internet use to addiction (Baumeister & Nadal, 2017), even though this may not be too far from the truth for many users.

Amid these transformations, technological developments have also created opportunities for criminality, as criminals utilize technology and its tools to perpetuate forms of deviance (criminality) in cyberspace (Jaishankar, 2008). Deviants use technological tools, including

computers (desktop and laptop), tablets, mobile phones, and internet connections to victimize and endanger online users. Consequently, users of the internet and diverse types of computer-mediated communication (CMC) have experienced and continue to suffer from varying forms of online victimization.

Users suffer from victimizations such as violent and aggressive sexual solicitation, online consumer fraud, and identity theft, among others (Adler & Adler, 2006; Anderson, 2007; Internet Crime Control Centre, 2006; Mitchell et al., 2003; RCMP [Royal Canadian Mounted Police], 2014; Sanger et al., 2004). Increasing reports of self-reported victimization are occurring against the backdrop of growing consumers' internet use for their daily activities (Arango et al., 2012; Fletcher, 2007). The increased self-reported victimization vis-à-vis growing internet use raises a serious paradox and warrants attention; hence, my research asks: Has the fear and perception of victimization changed how people use computer-mediated communications (internet)?

Findings from this study are expected to significantly contribute to sociological and criminological research, especially in the cybercrime research field. The study is unique in terms of theory, method, and data. Theoretically, the study is among the first to examine the seeming paradox in internet use and its consequences on behavior within the socio-criminological historical tensions between structure and agency. Methodologically, the study straddles positivism and interpretivism, providing enriched data about Canadians' internet use and behavioral patterns. Latently, the research site is also unique and contributes context-specific inputs into policy and practice. By projecting the paradox within the light of the structure and agency discourse, the study aims to make an empirical contribution and add to the literature. As alluded to in the extant literature, current criminological research has a disproportionate emphasis on conventional or physical place-based crime (Jaishankar, 2008; Kshetri, 2010).

However, the increasing trend of cybercriminal victimization means cybercrimes must be given sufficient attention. More importantly, a sociological perspective and contribution to this contemporary problem is urgently needed. Disciplines such as computer science, engineering, psychology, law, and marketing, among others, have made significant leaps forward in studying various aspects of cybercrime (Saban et al., 2002; Van de Weijer & Leukfeldt, 2017; Yazdanifard et al., 2011). A sociological perspective will highlight the problem's different intersectional aspects regarding the multiple and competing stakeholders, the consumer and demand side, and, crucially, the often taken-for-granted social dimensions. This will be made possible from the vantage point of the sociological imagination.

1.2 Defining the Issue

The internet is fast impacting the contemporary world and, likewise, criminality. Cybercrime encompasses several forms of online and computer crime and is gradually becoming the focus of criminology, victimology, and security research. However, before delving into the issue, it is imperative to indicate that cybercrime broadly involves two main actors: victims and perpetrators. Each actor can be either an individual or corporate entity or both. For this research, the issue under investigation relates to individual victims (and potential victims) of cybercrime. This clarification at the outset is crucial as it helps delineate the boundaries of the current research.

Socio-criminological studies have investigated cybercrime from a conceptual lens, including the dual or binary cybercrime conceptual framework (Gordon & Ford, 2006; McGuire & Dowling, 2013) and the tripartite cybercrime conceptual framework (Ibrahim, 2016; see cybercrime also by Yazdanifard et al., 2011). Also, some studies have examined the fear of

distinct types of cybercriminal victimization (Henson et al., 2013; Van Wilsem, 2011). Other studies have looked at the predictors of victimization from such crimes (Abdulai, 2020; Henson et al., 2013; van de Weijer & Leukfeldt, 2017; Virtanen, 2017). Furthermore, cybercrime has been studied from the standpoint of global security by examining the impact of diplomacy in fostering international cyber security (van der Meer, 2015). Researchers have examined cybercrime victimization from several theoretical standpoints, including the Routine Activity Theory (Holt & Bossler, 2008; Pratt et al., 2010). For example, Pratt et al. (2010) examined how actors' personal characteristics (the socio-demographic to which they belong) and online routines create opportunities for and increase their exposure to motivated offenders. Pratt et al. found that "sociodemographic characteristics shape routine online activity" and that "indicators of routine online activity fully mediate the effect of sociodemographic characteristics on the likelihood of being targeted for fraud online" (2010, p. 268). A recent exploratory study also investigated the application of Beck's Risk Society thesis to fear of being a victim of credit/debit card fraud (Abdulai, 2020). The study suggests that self-reported prior victimization predicts current self-reported worry of future credit/debit card fraud (2020).

In all of these criminological and victimological research programs in cybercrime, a thorough examination of the relationship between perceptions and experiences of cyber victimization and internet use, motivations for use, and risk of victimization within a Canadian context are conspicuously missing. Some limited studies in this area include those by Böhme and Moore (2012), Riek et al., (2015), and Saban et al. (2002). For example, Riek et al. (2015) examined cybercrime perception's effects on online service avoidance, finding that the potential risk regarding cybercrime negatively affects the utilization of three types of internet services – online banking, online shopping, and social networking. However, their study utilized secondary

information from a cross-sectional, pan-European population study that did not account for unique country differences in respondent experiences. Conversely, Saban et al. (2002) explored the consequences of cybercrime on consumer behavior. They found that cybercrime, including even its weakest form – spam e-mails – has a definite effect on consumer internet behavior and affects the "attractiveness of the internet as a viable marketing tool" (p. 29). However, they used a sample of only students in marketing courses over three campuses based in the United States. Furthermore, Saban et al.'s study had a marketing orientation and lacked a sociological focus and input. Böhme and Moore (2012) conducted secondary analyses of the spring 2012 Eurobarometer special survey data to examine how EU citizens' exposure to cybercrime affects their internet use. They found that prior (direct) cybercrime experience, latent cybercrime concern, and media exposure reduce the likelihood of using online services. Though an excellent exploratory work, Böhme and Moore's use of a cross-sectional population survey means country-specific effects moderate their findings. For instance, in the regression, whereas knowing cybercrime's effect is no robust predictor of online participation with country-fixed effects, it becomes significant without those effects (Böhme & Moore, 2012, p. 8).

Notwithstanding the limitations revealed in the above works, these exploratory studies provide helpful templates and insights for further work on the topic, which the current study aims to pursue. Hence, the current research examines Canadian internet users' perception of cybercrime risks, their fear of cybercrime victimization in general, and the consequences of each (risk perception and fear) on their internet usage routines in terms of avoidance and defensive online behaviors. The research also explores the motivations and rationale for Canadians' continuous internet use, notwithstanding the apparent risk of cyber victimization within a Canadian context.

1.3 Statement of Research Problem

The trend of increased incidents of self-reported online victimization in juxtaposition to the equally continuous and increasing use of the internet raises a paradox. More than 35 million Canadians are internet users, with a digital audience projected to reach 38 million (about 99% of the population) by 2023 (Clement, February 2019). With 43.5 hours per month for each Canadian, Canadians use the internet the most of any nation around the world, per capita (Public Safety Canada, 2018, p. II). A surge in the popularity of online interaction is occurring; however, consumers entertain a fear of becoming victims of cybercrime rather than physical crime (Pratt et al., 2010). A special Eurobarometer survey revealed that an overwhelming majority (85 %) of internet users across the European Union (EU) agreed that their risk of cybercrime victimization is increasing, an increase of nine percentage points from the previous year's survey (TNS Opinion & Social, 2015, pp. 45-46). Internet consumers worry over their online transactions in addition to their concerns regarding cyber security and their risk of victimization. For instance, two main concerns are prevalent among EU internet consumers: 43 % have reservations regarding "misuse of personal data," and 42 % are concerned about "security of online payments" (TNS Opinion & Social, 2015, p. 23). Moreover, the concern about internet transactions has increased among EU citizens; increases of 6 and 7 % are observed in the concern for the abuse of personal information and online payments security, respectively (TNS Opinion & Social, 2015, pp. 23-26; also see Bhatnagar et al., 2000 and Horrigan, 2008 for higher perceived risk of credit card use against low perceived benefits). The European situation points to yet another paradox regarding people's perception of the safety of cyberspace (internet) and their continued use of the internet.

Cybercrime is increasing in Canada (RCMP, 2014; Statistics Canada, 2019). Almost 4,000 cybercrime incidents were reported in 2012, an increase of more than 800 incidents from the previous year (RCMP, 2014, p. 7). The Canadian Anti-Fraud Centre (CAFC) recorded more than "16,000 complaints of cyber-related fraud (e-mail and website scams), accounting for more than $29 million in reported losses" in the year 2013 (2014, p. 7). Statistics Canada (2019) reported 15,184 total police-reported cybercrime incidents in Canada in 2014 (47.7 per 100,000 population). Fast forward to 2018, where Statistics Canada reported that the total police-reported cybercrime incidents more than doubled, increasing to 32,968 reported incidents (89.4 per 100,000 population). The Canadian situation also reveals a significant paradox regarding people's experiences of cybercrime victimization amid their continued internet use. These paradoxes (perception of safety and internet use and cybercrime victimization experience and internet use) warrant attention as they raise critical questions about the nature of the internet and other forms of CMCs. The paradoxes also appear to bring into focus the notions of rationality among internet users. Do universal and objective conceptions of rationality exist, or does rationality manifest in subjective and context-specific ways?

The above preamble serves as the basis of my research problem. What is the general perceived prevalence of cybercrime among Canadian internet-using adults, and not just in terms of a specific type of cybercrime, e.g., credit card fraud? Given the fear of victimization, why has internet use surged? Has the specter of risk and fear of victimization constrained the behaviors of internet users? What about the internet causes consumers to ignore or look beyond – consciously or unconsciously – the inherent risks of using it? What are the pull forces at play?

1.4 Research Questions

The primary inquiry in this study is, thus: Why, notwithstanding the fear and persistent or inherent risk of victimization in cyberspace, do internet users continue to use various forms of computer-mediated communication? To explore this question more fully, I also ask: has the perception of victimization changed how people use the internet?

The secondary research questions are:

1. What association do socio-demographic characteristics have with the risk of cybercrime victimization?
2. What is the relationship between prior cybercrime victimization experience and the fear of future cybercrime victimization?
3. What is the association between cybercrime victimization experience and the perceived risk of cybercrime?
4. In what ways do victimization experiences constrain internet use behavior?
5. In what ways does cybercrime incident reporting affect fear of cybercrimes?
6. How does internet use frequency constrain internet use behavior?
7. What are the motivations for internet use among Canadian adults?

This study is an extension of my previous Master of Arts work, which examined the determinants of cybercrime victimization among university students; however, notwithstanding such carryover, the questions of the current study are not only valid but timely. Replicating some of the earlier questions will provide a framework to compare findings and determine any potential source(s) of variances. Also, the questions are valid because the focus and target of the previous study were different, i.e., a student sample, compared to the national focus of this

current study. Finally, the present study's focus on general cybercrime, rather than credit/debit card fraud, means it is substantially different from the previous work. In this sense, the previous work was exploratory and served as the foundation for the present research.

1.5 Rationale/Justification of Study

Due to technological advancement, using a computer and the internet has become an integral part of most people's everyday lives. Internet usage continues to increase over time as the pace of technological transformation progresses. However, internet use has also created an opportunity for crime (Jahankhani & Al-Nemrat, 2011; Kshetri, 2010; Li, 2017) and has brought in its wake cyber criminality. The opportunity for crime is enhanced by the cloak of invisibility that cyberspace fosters (Sukhai, 2004) and spurs on users with negative or criminal ends. Such opportunity for crime in cyberspace has exposed internet users to various forms of online victimization. Therefore, this situation has engendered several research programs in cybercriminal victimization. While the type of online behaviors that expose consumers to victimization and the circumstances under which those actions manifest have been investigated, minimal research has explored the behavioral response to risk, fear of victimization, and users' motivations for internet access. Also, studies into fear of criminal victimization in cyberspace are in their infancy, with some studies considering specific types of cybercrimes. As a result, the current study's justification primarily lies in making a scholarly contribution to an emerging or contemporary but less studied social problem and domain of criminology.

1.6 Research Site Justification – Canada

Canada makes for a compelling case as a site for this research. Canada's position as an advanced Western country and a member of the Group of 8 (G-8) industrialized nations is

significant. Also, Canada is a member of the Five Eyes intelligence alliance of nations, including the United States, United Kingdom, Australia, and New Zealand (Pfluke, 2019). Beyond this, several other factors are considered.

First, internet penetration is very high in Canada relative to the global penetration rate (DataReportal, 2022a, 2022b). As Table 1.1 shows, internet penetration in Canada at the beginning of 2022 was 96.5 % of the national population representing a growth of +0.9 % over the previous year. The internet penetration rate means an overwhelming majority of Canadians are using the internet. Table 1.1 also reveals that 87.1 % of Canadians are active social media users, showing a growth of +3.4 % over the previous year.

Table 1.1

Internet Penetration Overview – Global and Canada

Comparison	World			Canada		
	Penetration (billion)	Rate (%)	% Change from 2021	Penetration (million)	Rate (%)	% Change from 2021
Internet use	4.95	62.5	+4.0	36.89	96.5	+0.9
Social media use	4.62	58.4	Over +10	33.30	87.1	+3.4

Source: Extracted from DataReportal (2022a, 2022b). *Global and Canada Digital Overview*

Additionally, internet connection speed in Canada is very high and relatively stable (DataReportal, 2022b). Whereas the median mobile internet connection speed via cellular networks as of February 2022 was 72.87 Mbps (an increase over the prior year of +11.1 %), the median fixed internet connection speed was 97.51 Mbps (an increase of +27.6 % from the prior

year) (2022b). The high internet connection speed means Canadian internet users are motivated to continue using the internet for various purposes.

Second, internet use frequency in Canada was another factor motivating the research location. Table 1.2 illustrates Canadian internet usage based on usage frequency, age grouping, and gender identification for personal non-business purposes. Table 1.2 shows that a minimum of two-thirds (67.5 %) of Canadian internet users of both sexes from any age group used the internet every day at least once in 2010, increasing to a minimum of 80 % for those under 45 years. However, in 2012, it grew to two-thirds (70.2 %) for persons of both sexes from any age group and 84 % for those under 45 years.

Table 1.2

Canadian Internet Usage by Usage Frequency, Age Grouping, and Sex identification

Geography	Canada (map)	
Frequency of use	Using the Internet at least once a day	
Sex	Both sexes	
Age group	2010	2012
	Percent	
Total, Internet users aged 16 years and over	75.5	80.0
Internet users aged 16 to 24 years	83.9	88.8
Internet users aged 25 to 44 years	80.7	84.7
Internet users aged 45 to 64 years	67.5	73.4
Internet users aged 65 years and over	67.5	70.2

Source: Statistics Canada (May 2017a). Table 27-10-0018-01 Internet use by frequency of use, age group and sex

Table 1.3 shows personal internet use in Canada based on location and usage frequency. Table 1.3 reveals that only a small percentage (10.1 %) of internet users in Canada

who are 16 years or older accessed the internet from a public library for personal non-business purposes in 2010, whereas the majority (77.2 %) accessed it from home. A similar usage frequency based on location was observed in 2012: less than one-in-ten (9 %) and eight-in-ten (80 %) of all internet-using Canadians accessed the internet from a public library and home, respectively.

Table 1.3

Canadian Internet Usage based on Location and Usage Frequency

Geography	Canada (map)	
Frequency of use	Total, frequency of use	
Location of use	2010	2012
	Percent	
Internet use from home	77.2	80.8
Internet use from work	30.7	33.2
Internet use as a student from school	14.3	14.5
Internet use from a public library	10.1	9.7
Internet use with a wireless handheld device	26.2	48.6
Internet use from any other location (for example a friend's or relative's home or hotel)	35.2	40.5

Statistics Canada (May 2017b). Table 22-10-0026-01 Internet use, by location and frequency of use

Moreover, Canadian attitudes and behaviors towards the internet, are important factors in selecting the research location, particularly with the start of the COVID-19 pandemic. According to a Statistics Canada (2020) report, the start of the pandemic affected Canadian attitudes and behaviors towards the internet while increasing their vulnerability. According to the Statistics Canada (2020) report, with the start of the pandemic:

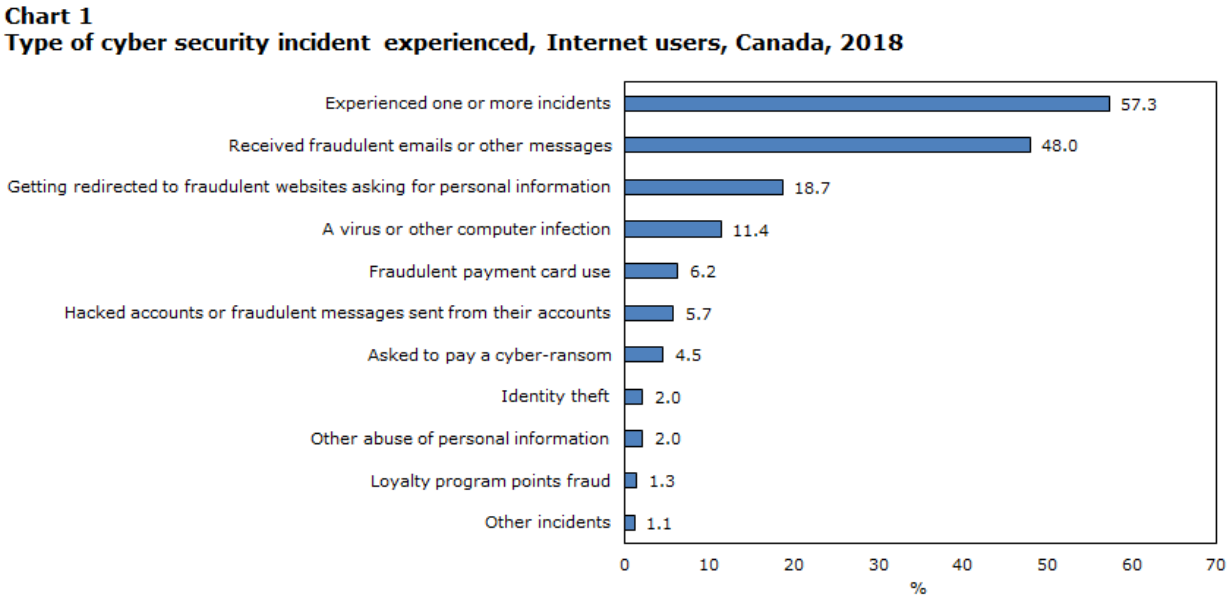
- Canadians expended more on digital technologies, with about half (44 %) indicating they "spent more online on technology" (p. 1).

- Many welcomed spending more time on screens, with four-in-ten (41 %) indicating they "[spent] more time on social media and messaging services since the onset of the pandemic, while 3 % spent less time" (p. 2).
- Canadians experienced increased vulnerability, with close to half (42 %) experiencing "at least one type of cyber security incident" … "including phishing attacks, malware, fraud and hacked accounts" (p. 3).
- They increased their online behavioral precautions, especially among younger age groups, "with three-quarters (75 %) of those aged 15 to 34 increasing or maintaining their usage of multi-factor authentication, compared with less than half of those aged 65 and older (39 %)" (p. 3).

These attitudinal and behavioral changes add to the relevance of Canada as a site for a study of the current nature.

It is imperative that additional research on the rising trend of cybercrime prevalence in Canada is conducted. The 2018 Canadian internet use survey indicated that more than half (57 %) of Canadian internet users reported a cyber security incident in 2018 (Statistics Canada, December 2019). Additionally, the 2018 Uniform Crime Reporting Survey revealed that Canadian police services reported over 30,000 cyber-related violations (cybercrimes), an increase of 12 % from the previous year (Statistics Canada, December 2019). The overall prevalence rate and disaggregated prevalence information are shown in Figure 1.1.

Figure 1.1. Cyber Security Incidence Prevalence in Canada, 2018



Source: Statistics Canada (December 2019). *Just the Facts: Cybercrime in Canada*

Canadian enterprises, according to the 2017 Canadian Survey on Cybersecurity and Cybercrime, spent almost $15 billion to prevent, detect, and recover from cybercrime (Statistics Canada, December 2019). A significant majority (94 %) of Canadian businesses expended some funds on cybercrime prevention or detection and spent $78,000 on average to implement such measures. The above expenditure profile presents only a snapshot picture, as it does not include expenditure by the government and individuals.

Finally, the police in Canada, as in other places, face a challenge in policing cybercrime, with the foremost reason being the lack of reporting (Bidgoli, 2015; Bidgoli & Grossklags, 2016; Burgard & Schlembach, 2013; Statistics Canada, December 2019; van de Weijer et al., 2019). Reporting crime is essential to successfully prosecute and subsequently prevent its recurrence. But, for various reasons, individuals and organizations do not always disclose incidents of

cybercrime to the authorities. For instance, of the two-in-ten (21 %) Canadian businesses that were affected by cybercrime in 2017, only one-tenth (10 %) disclosed their experiences to the police (Statistics Canada, December 2019). Some of the reasons for the reluctance (by individuals and organizations) to notify the authorities about cybercrime – in Canada and other places – include internal resolution, underestimating impact or offense seriousness, distrust in the police, unclear or complicated reporting process, and victim self-blaming, among others (Bilodeau et al., 2019; Goucher, 2010; Wall, 2008; Yar, 2013).

The factors discussed in the preceding paragraphs, including the increasing trend of cybercrime in Canada as reported by individuals, businesses, and the police, mean that cybercrime and cybersecurity need to be given particular attention by all stakeholders. They also emphasize the decision to conduct the current research in Canada.

1.7 Dissertation Organization

The remaining chapters of the dissertation are divided into seven sections. Chapter 2 presents the literature review. Some theoretical approaches to cybercrime research, including the theoretical framework adopted for this doctoral study, are highlighted in Chapter 3. Chapter 4 describes the research's methodology, along with the variables, related hypotheses, and research design, with further details about the conceptual and analytical frameworks. In Chapter 5, the results and statistical analysis are presented. Chapter 6 highlights the qualitative analysis dimension because the study uses mixed methods. A discussion of the results and their theoretical and practical implications is presented in Chapter 7. Chapter 8 finishes the study, provides a summary, and makes suggestions for additional research.

Chapter Two: Literature Review

2.0 Introduction

This chapter examines the key elements that emerge from a review of research literature on cybercrime conceptualization and victimization. It focuses on themes relevant to cybercrime victimization and internet use. The rest of the chapter is divided into the following sections. I begin by giving a summary of the chapter. Next, I examine the literature around cybercrime conceptualization, revealing some of the definitional challenges and how they impact cybercrime prevalence estimation. I make clear my stands on the definitional conundrum and specify the operational definition of cybercrime that is utilized in the current study. I follow up with a review of the prevalence of internet and computer use. Next, I discuss cybercrime trends, followed by a review of victimization effects on cyber risk perception. I then follow this with a review of perceptions of victimization and internet use and details about the cost of cybercrime for individuals, businesses, and governments. In the following section, I discuss cybercrime incident reporting. I conclude with insights from the literature and their implications for the current study.

2.1 Overview

Technological advancements have spurred changes to communication systems and have subsequently changed the nature of deviance and criminality. Such transformations have subsequently made it imperative to alter the definitions of deviance and crime. As a result, the normative definition of crime relating to statutory violations of established legal codes with prescribed punishments needs to be expanded to make way for conduct violations in cyberspace. Technological advancements have made it possible for deviants and persons with criminal

motives to seize technological tools to victimize unsuspecting computer users. As a result, various forms of cybercrimes have become commonplace. Some debates and trends are emerging in the socio-criminological literature about the internet and crime. The foremost debate concerns an acceptable definition of cybercrime; various perspectives have been presented as researchers grapple with potential definitions (Gordon & Ford, 2006; Ibrahim, 2016; Kraemer-Mbula et al., 2012; Kshetri, 2010; Royal Canadian Mounted Police [RCMP], 2015). For instance, the RCMP conceives of cybercrime in terms of "technology-as-instrument" and "technology-as-target" crimes (p. 7) while Gordon and Ford (2006) presented the relational conception comprising of "techno-centric or Type I" and "people-centric or Type II" crime categories (p. 15). One of the trends is that internet penetration and frequency of use are increasing globally, especially among the advanced economies, including the European Union (EU) and Canada (Clement, 2019; Eurostat, 2017; Van Wilsem, 2011). People in these societies regularly use the internet for various purposes, notably online shopping and purchases (Eurostat, 2017; Smith & Anderson, 2016; StatsCan, 2009; Van Wilsem, 2011). Another issue is that the steady increase in internet penetration has raised concerns about cyber victimization. The debate around internet use frequency and its associations with increased risk of cybercrime victimization was explored early on by Mitchell et al. (2003) and continued by Internet Crime Control Centre (ICCC) in 2006, which ICCC continued to grapple with in its annual reports from 2007 through 2017. Many researchers have waded into the debate (Arango et al., 2012; Australian Bureau of Statistics, 2008; StatsCan, 2009; Marcum et al., 2010; Office for National Statistics, December 2018).

Some debates have also evolved around the consequences of cyber victimization on risk perception (Abbott & McGrath, 2017; Chadee et al., 2019; Gainey et al., 2011; Hale, 1996;

Logan & Walker, 2017; Riek et al., 2015). Another rising trend concerns the effects of risk perception of cybercrime on internet utilization (Böhme & Moore, 2012; Riek et al., 2015; Saban et al., 2002). Last, but not the least, cybercrime reporting is a notable theme in the criminological literature, which has examined the challenges of reporting and the reasons why people and businesses are reluctant to disclose their encounters to the authorities (Bidgoli & Grossklags, 2016; Goodman & Brenner, 2002; Goucher, 2010; van de Weijer et al., 2019; Wall, 2008; Yar, 2013).

2.2 Defining Cybercrime

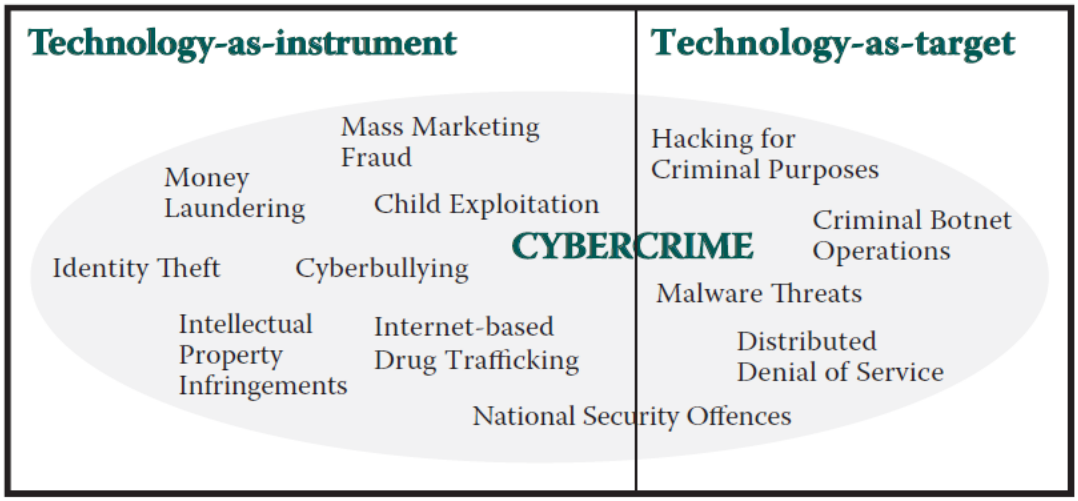
As a product of technological advancement, establishing an overarching definition of cybercrime is challenging. Yet crafting a definition for any social phenomenon is essential to better understand the phenomenon under consideration. Researchers and institutions have contributed to defining the concept of cybercrime from different perspectives.

The RCMP define cybercrime as "any crime where cyber – the Internet and information technologies, such as computers, tablets, personal digital assistants or mobile devices – has a substantial role in the commission of a criminal offense" (Royal Canadian Mounted Police, 2015, p. 7). The RCMP classifies cybercrime into two main groups after acknowledging the vast reach of its definition:

A. *technology-as-target – criminal offenses targeting computers and other information technologies, such as those involving the unauthorized use of computers or mischief in relation to data, and;*
B. *technology-as-instrument – criminal offenses where the Internet and information technologies are instrumental in the commission of a crime, such as those*

involving fraud, identity theft, intellectual property infringements, money laundering, drug trafficking, human trafficking, organized crime or terrorist activities, child sexual exploitation or cyber bullying (p. 7; emphasis added).

Figure 2.1. *Cybercrime categories*



Source: Royal Canadian Mounted Police, 2014, p. 6

The RCMP's proposed conceptual definition of cybercrime is broad: it appears as an attempt to account for all categories of cybercrimes. Although a helpful approach for classification, the RCMP's definition of cybercrime is technical and can be confusing to the layperson. References to "technology-as-target" and "technology-as-instrument" do not sound accessible to the everyday user of the internet and other computer-mediated communications.

Conversely, Kraemer-Mbula et al. (2012) described cybercrime simply as "illegal internet-based activities" (p. 541). Initially, this comes across as straightforward. On the one hand, the simplistic rendering of cybercrime appears to be a good one. On the other hand, this way of looking at cybercrime is also overly broad and lacks clarity. The determination of illegal activities, especially in cyberspace, is not a straightforward action. As Kshetri (2010) argued,

countries differ in terms of what is deemed illegal or otherwise, with some decisions likely influenced by socio-cultural worldviews and other context-specific realities of nations. The simplistic and broad conception of cybercrime can be a pragmatic approach, however. A definition of cybercrime that is comprehensive and open allows countries to identify specific illegal activities within their geographical space.

Another definition that has been proposed is that cybercrimes are "unlawful acts wherein the computer is either a tool or target or both" (Chawki et al., 2015, p. 6). Although simplistic, Chawki et al.'s (2015) definition could also be deemed ambiguous. The ambiguity lies in the determination of "unlawful" given that such decisions are not uniform across countries. Also, this type of definition looks to be quite broad and all-encompassing. Criminal activities in the technological era involve the internet or computer-mediated communication at least at some point in the planning or execution. In this way, Chawki (2015) et al.'s definition includes all criminal activities, including place-based criminal activities.

Gordon and Ford (2006) argued for a relational view of cybercrime that represents "a continuum ranging from crime which is almost entirely technological in nature and crime which is really, at its core, entirely people-related" (p. 15). Thus, they suggested that cybercrime refers to "techno-centric or Type I" and "people-centric or Type II" crime categories based on the degree of the cyber or the people component. Cybercrimes of Type I (techno-centric) include phishing, data theft or service manipulation through hacks or virus, identity theft, and more (Gordon & Ford, 2006). The Type II (people-centric) variant include cyberstalking, harassment, cyberbullying, and blackmail (2006). Gordon and Ford (2006) have thus provided a simple and valuable template for distinguishing cybercrimes that at its core is a broad and ambitious attempt

to account for all forms of cybercrimes. In such ambition, however, Gordon and Ford appear to account for all types of crimes, conventional ones included.

Figure 2.2. ***The Continuum of Cybercrime***

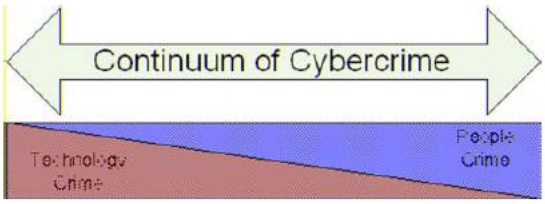
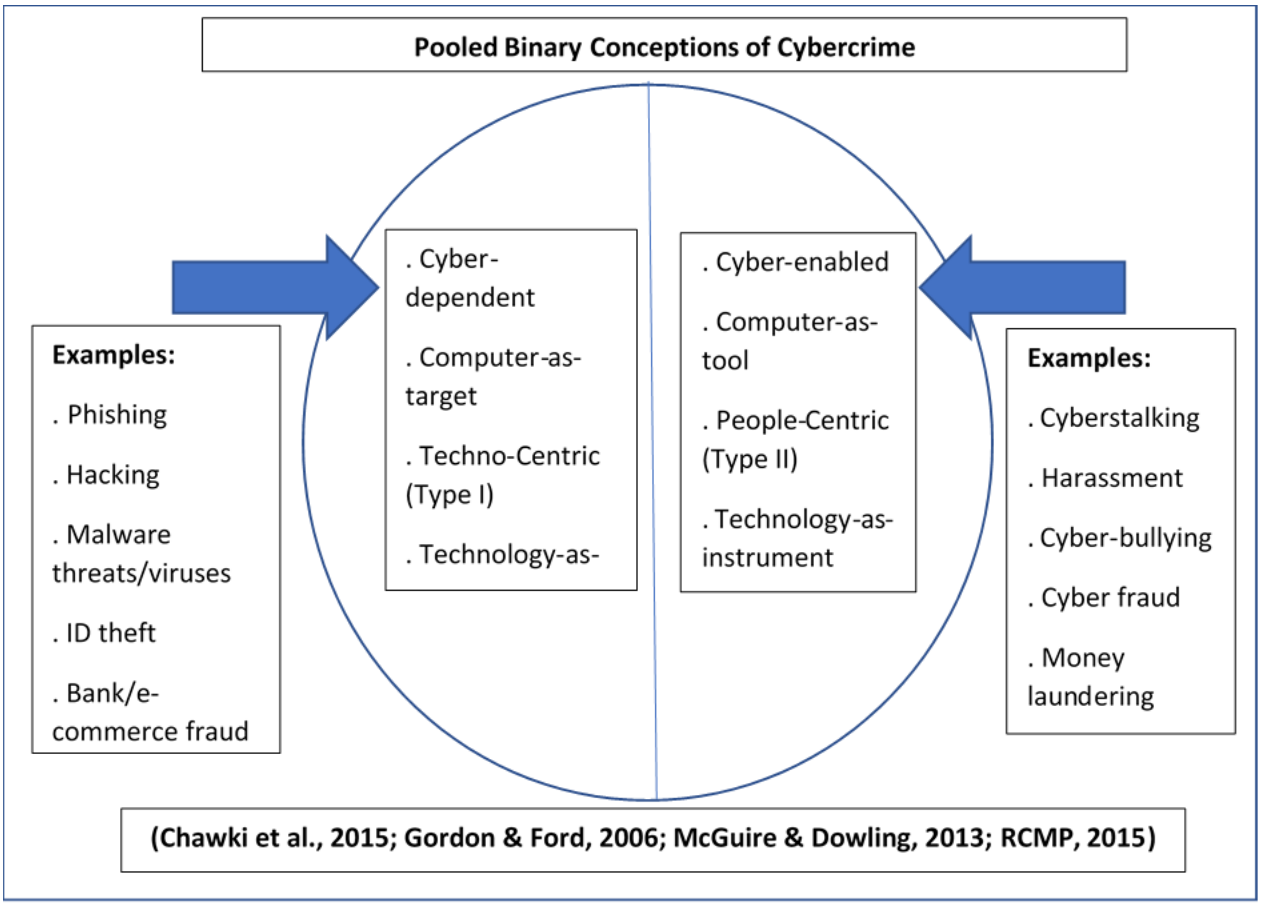


Fig. 1 The Continuum of Cybercrime. Areas defined as Cybercrime are very broad in nature – some crimes have only a peripheral cyber element, whereas others exist only in the virtual world

Source: Gordon and Ford (2006, p. 15)

Figure 2.3 represents a pooled binary conception of cybercrime as advanced in the literature. The conceptions have been termed binary models (Ibrahim, 2016) because each of the authors examined cybercrime as comprising two main strands. The two broad strands, though termed differently by the authors, speak to the same understanding. Figure 2.3 represents an attempt to combine the various propositions into a unity.

Figure 2.3. *Pooled Binary Conceptions of Cybercrime*



Source: Author's Construct, 2022

The above conceptions of cybercrime represent an overview of the attempts at definitions in the literature. Two main observations can be discerned from the proposed definitions as reviewed above. The first is that they represent broad or generalized perspectives. The implication from the comprehensive view, then, is that the term "cybercrime" is a broad and generalized one. The second observation is that cybercrime represents a continuum, with technology and people as the two ends of the continuum. This framework, referred to as the dual or binary model of cybercrime (Ibrahim, 2016), makes for ease of classification.

A harmonious definition of cybercrime, however, has yet to be achieved. This present work aligns and operates with the definition proposed by Kshetri (2010). Kshetri offers a practical definition of cybercrime “as a criminal activity in which computers or computer networks are the principal means of committing an offense or violating laws, rules, or regulations" (2010, p. 3). Due to two factors, Kshetri's (2010) definition is most appropriate within the perspective of the current investigation.. The first is that the definition refers to using computers or computer networks in criminal activity, which is similar to most definitional attempts. Second, and most importantly, the definition’s reference to "committing an offense or violating laws, rules, or regulations" (p. 3) is flexible, holistic, and encompassing. This is because the activity concerned may violate an established law, as one codified in the legal statutes of the land. Alternatively, the act in question may not necessarily violate an established law but goes against a rule or a regulation. The flexibility also means that the definition can be utilized across several domains or geographical boundaries. In this way, Kshetri’s definition allows for the identification of a cybercrime under different guises.

2.2.1 Accounting for the Definitional Challenge

Some scholarly and policy circles have discussed the absence of a universally acclaimed definition of cybercrime. Through the discussions, certain factors have been examined as contributing to cybercrime’s definitional conundrum. Foremost among the reasons is cybercrime’s global or boundless nature (Ibrahim, 2016). The boundary-defying characteristic of cybercrime refers to the fact it is not circumscribed within a given geographical space. One of the unique features of cyber-based crimes is their global nature (Yar & Jewkes, 2010), i.e., they are committed across geographical space and time and can simultaneously involve multiple actors and targets. Related to this problem and the absence of a universal definition is what

Kshetri (2010) has termed the "inter-jurisdictional comparisons of cybercrimes" (p. 3). Countries have varying views regarding which acts constitute cybercrimes. To clarify this point, Kshetri (2010) points to differences in what is “obscene in Arab countries,” but “socially acceptable in Western countries” and the differences between “an obscene" webpage in the UK and Scandinavia (p. 3). Variations may be influenced by countries’ socio-cultural and religious world views and, given the socio-cultural and religious differences between countries, the default consequence is moving toward country- or region-specific conceptions of cybercrime. These conceptual differences make comparative studies of cybercrimes between countries challenging in the larger frame.

The apparent institutional variety among countries, including preferences and restrictions also affects the definitional difficulty of cybercrime (Kshetri, 2010, p. 8). Examining North America and Europe may reveal further nuances to this problem. For example, Werth (2009, cited in Kshetri, 2010) pointed out that "while British, French, and German laws prohibit contents on the Internet related to race hatred or Holocaust denial, the US Constitution protects free speech" (p. 8). The definitional problem of cybercrime can also be traced to institutional heterogeneity, which contributes to the problem of inter-jurisdictional comparisons of cybercrime.

2.2.2 Estimating Cybercrime Prevalence: Underestimated, Accurate, or Overestimated?

Generally, it is held that cybercrime is on the rise as individuals, businesses, and governments increasingly utilize the internet and various forms of CMCs. Notwithstanding the affirmative view regarding cybercrime prevalence, it has also been argued that the reported prevalence of cybercrime is inaccurate (Bidgoli & Grossklags, 2016; Bilodeau et al., 2019; CBS,

2018; Goucher, 2010; Symantec, 2010). Some reasons have been advanced to support the erroneous picture of the prevalence of cybercrime.

The principal reason for the perceived inaccurate estimate of cybercrime prevalence can be traced to the lack of reporting of cybercrime incidents (Bilodeau et al., 2019; Chawki et al., 2015; Kshetri, 2010; Symantec, 2010). The argument is that most incidents of cybercrime go unreported. As a result, the default conclusion is that cybercrime, even though seen to be increasing, is still underestimated. Several factors that account for lack of reporting have been identified. According to Chawki et al. (2015), some of the reasons for the lack of cybercrime incident reporting include the "potential for reputational damage … the lack of a clear reporting mechanism and the perception that, even if crimes were reported, little can be done" (p. 12). Other reasons for victims' non-reporting of cyber-attacks, according to Symantec (2010), include the fact that victims are unaware of their victimization, victims are unaware the conduct involved is a crime, and victims may decide against reporting because of embarrassment or corporate responsibility.

The perceived inaccurate estimate of cybercrime prevalence has also been linked to reporting with a vested interest (Rush et al., 2009). Accordingly, some organizations with given interests have the potential to either over- or under-estimate the actual rate of cybercrime (Rush et al., as cited in Kshetri, 2010, p. 9). This is done to further the interests of such organizations. Information technology (IT) security organizations are notable entities in this realm, and they do so to give prominence to their work. To increase the need for customers to buy into the cyber security interventions of businesses, for example, companies can overestimate the actual rate of cybercrime. Such overestimation seeks to alarm consumers and increase their feelings of

vulnerability. Cyber security businesses can also show the efficacy of their products by underestimating the rate of cyber-attacks or their success following attempted attacks.

The perceived inaccurate estimate of the prevalence of cybercrime has also been linked to the confluence of "methodological, logical, conceptual, and statistical problems in estimating the level and pattern of cybercrimes" (Kshetri, 2010, p. 8). According to this view, the confluence of these problems means projecting the actual picture of cybercrime is always bound to be problematic. Methodologically, estimating cybercrime prevalence and related costs is tricky because cybercrime encompass "different combinations of direct, indirect, and opportunity costs such as actual money and intellectual property stolen, costs of fixing or replacing infected networks and equipment, lost work time, and intangible losses associated with the lack of customer confidence in doing business with the affected company" (GAO Reports June 22, 2007, cited in Kshetri, 2010, p.8). Getting at all these various dimensions for any episode of cyber-attack is almost impossible. The consequence is that the reality of cybercrime and its associated cost is inaccurate through either an under- or over-estimation. Kshetri (2010) argued that one of the issues impeding the ability to accurately measure the "cybercrime-related indicators in an economy and comparing them across jurisdictions . . . [is that] . . . the country of origination of a cyberattack is extremely fuzzy" (p. 8). This logical challenge is significant because cybercrime is a borderless crime. It evades physical boundaries, and perpetrators can launch attacks from one country that target victims in a different country. There is also conceptual ambiguity and heterogeneity regarding the definition of cybercrime (Grabosky, 2004; Kshetri, 2010; Werth, 2009). Such conceptual differences and heterogeneity mean that cybercrime is conceived differently worldwide, making an accurate picture of cybercrime prevalence a real challenge. Such differences, as Kshetri (2010) contends, make comparative studies of cybercrime difficult.

2.3 Prevalence of Internet/Computer Use

The contemporary era has seen the entry of the internet and other forms of CMCs into the basic fabric of daily life. Computer, and hence internet use, is on the upward surge with consumers now completing most of their daily routines online (Arango et al., 2012; Pratt et al., 2010; Fletcher, 2007; US Census Bureau, 2008; US Department of Commerce, 2008). Routines such as banking, communication, and shopping are undertaken online. The age of fluid liquid modern life espoused by Bauman (2000) particularly underscores the increased patronage of the internet. Convenience and constant change are the hallmarks of the current liquid era. Meanwhile, the internet makes such convenience possible because of cyberspaces' continuous state of flux.

Internet utilization is thought to be high among countries within Western and advanced economies. In the 28-member state European Union (EU-28), four-fifths (80 %) of all persons aged 16 to 74 within the EU-28 accessed the internet minimum once per week (Eurostat, 2017) and almost three-quarters (72 %) of all persons in the same age category accessed the internet daily (Eurostat, 2017). Such internet maximization in the EU-28 suggests a certain level of interconnectivity between people's daily routines and the internet. Alternatively, the high level of internet penetration in the EU-28 has brought about convergence in people's routines. As a tool of technology and a source of convenience, all categories of people, the young and old included, are thought to utilize the internet. Based on data from the Bureau of Statistics, Van Wilsem (2011) reported that over half of the population of countries with high internet connection densities, including the UK, and Germany, among others, shopped online in the past. In support of this, a Pew Research Center investigation discovered that almost eight in ten (79%) Americans shop online, with 15% doing so on a weekly basis (Smith & Anderson, 2016).

Notably, the first iteration of the Pew Research Center's survey about online shopping in 2000 found that only a little over two-in-ten (22 %) of Americans ever shopped online. Eurostat (2017) then found that more than half (57 %) of all persons aged 16 to 74 in the EU-28 placed an online order for goods or services for private use. On this side of the Atlantic, by the year 2015, Americans had spent more than $300 billion annually online, equating to "roughly 10 % of all retail purchases, excluding automobiles and fuel" (Smith & Anderson, 2016, p. 5). As online transactions remain high, the percentage of online sales as a proportion of total retail is expected to be substantive.

In Canada, internet use and penetration are not different than in Europe or other developed parts of the world. According to a recent survey, more than 35 million Canadians are internet users, with a digital audience projected to reach 38 million users (or 99 % of the Canadian population) by the year 2023 (Clement, 2019). Internet use in Canada comprises several modalities, such as desktop and laptop computers, smartphones, and tablets. For example, in 2018, among online Canadian adults, roughly nine-in-ten (or 88 %) used desktop or laptop computers to access the internet, with seven-in-ten (or 72 %) using smartphones (Clement, 2019). One of the advantages of the internet and other forms of computer-mediated communications is its flexibility in allowing users to accomplish different tasks. In this regard, a survey conducted in March 2019 of adult Canadian online consumers indicated that the vast majority (90%) devote time on the web reviewing or replying to emails, with more than seven in ten (71%) using online banking (Clement, 2019). Furthermore, Clement (2019) reports that, among Canadians who use the internet, the average weekly duration on the internet from 2015 to 2018 was 40.5 hours per week on all gadgets. In other words, Canadians spend the equivalent of five working days in a week on the internet across all devices.

The above prevalence of internet and computer use statistics underscores the ubiquitous nature of the internet. Though revealing, the statistics provide only a snapshot into the internet utilization by individuals and households.

2.4 Trends of Cybercrimes/Online Victimization

Rapid technological advancement is causing broad societal changes and is expected to affect social phenomena such as deviance and crime. As Adler and Adler (2006) observed, the definition of deviance changes over time in any society and across groups. Following Adler and Adler (2006), and with the modern liquid time à la Bauman (2000), changing definitions and boundaries of deviance are expected. Technological development is changing the interface of interaction from physical to cyberspace, suggesting we should expect an increasing number of deviant activities in cyberspace. In other words, deviant and criminal activities in cyberspace are by-products of technological development and are expected to increase. Following Beck (1992), such aberrant action in cyberspace is an unintended consequence of technological development, itself a product of modernization.

The nature of deviance and criminality in cyberspace has been examined by researchers. As computer and internet use continue to increase, computer crime and victimization from such crimes are likewise on the rise (Adler & Adler, 2006; Internet Crime Control Centre, 2006, 2007, 2008, 2009, 2010, 2011, 2012, 2013, 2014, 2015, 2016, 2017; Marcum et al., 2010; Mitchell et al., 2003; Pratt et al., 2010; Sanger et al., 2004; Van Wilsem, 2011; Ybarra et al., 2007). According to Adler and Adler (2006), the internet has impacted social deviance in three main ways: illicit markets, by opening forms of deviance to "people who would not ordinarily have access to it" (p. 141); internet fraud, by serving as "a source for the easy transmission of fraud,

with individuals and groups" finding innovative means "to access unsuspecting users" (p. 142); and internet communities, by serving as "a place where previously non-existing deviant subcultures can flourish" (p. 144).

A national survey of risk, impact, and prevention found that youth experience different forms of online victimizations while using the internet, including wanted or solicited and unwanted or unsolicited victimizations (Mitchell et al., 2003). The responses for unwanted victimization far outweighed wanted victimizations (Mitchell et al., 2003). Similarly, a study of the experiences of female juvenile delinquents revealed that over 80 % participate in internet chat rooms, with 70 % of such users experiencing online victimization, also referred to as sexual solicitation (Sanger et al., 2004). Additionally, a majority of the internet chat room users used the internet very frequently and regularly; indeed, 9.85 hours a week on average were spent in chat rooms by 87% of them. (Sanger et al., 2004). The experiences of unsolicited victimization of juvenile internet chatroom users strongly suggest that internet use frequency is correlated with a heightened risk of victimization in cyberspace.

Academics still do not properly comprehend the scope of cybercriminal victimization and its theoretical consequences in light of the changes that have altered criminality and the definitions of crime. In the meantime, cybercrimes have been getting much attention, particularly from the press and security groups. For instance, the Pew Internet and American Life Project Report revealed that 92 % and 87 % of Americans have concerns about child pornography and theft of credit card, while 69% are "very concerned" regarding online theft of credit card (Pew Research Center, 2001, pp. 7-8). Also, population figures from a fraud study in Australia showed that, respectively, 3.1 % and 2.4 % of Australians older than 15 had experienced identity fraud and bank or credit card fraud (Australian Bureau of Statistics, 2008).

Additionally, more than 3.6 million fraud events were reported by adults 16 and older in the Crime Survey for England and Wales for the year ending December 2018, a 12% rise from the survey year ending December 2017 (Office for National Statistics, December 2018, p. 56). Notably, 56% and 54%, respectively, of the total fraud cases for the survey years ending in September 2018 and December 2018 were both classified as "cyber-related," that is, cybercrimes (Office for National Statistics, September 2018, p. 56; December 2018, p. 56). Given the continuous surge in internet use across age cohorts for different activities, cases of identity theft and other forms of internet crimes are projected to grow into the future (Arango et al., 2012).

Concerns about the hazards of cyber fraud are warranted given the rise in the quantity and worth of digital purchasing over the past two decades and the resultant effect on internet use behaviors and motivations for internet use. Over 2.2 million households placed 13.4 million internet orders in 2001, according to StatsCan (2009). By 2007, this number had increased to around 70 million orders from 8.4 million Canadians who were 16 years of age or older. Due to this development, there are a lot of opportunities for cybercrime, such as identity theft and hacking into devices or stores to obtain credit or debit card information from customers. As a result, Grau (2008) found that Canadians refrain from making additional online purchases due to worries about credit card security. Conversely, these realities about the risk profile of online (internet) activity make it imperative to raise questions about people's continuous internet use and the potential ramifications on the behavioral conduct of internet users.

2.5 Victimization Effects on Cyber Risk Perception

A widely studied connection or theme is how victimization experiences affect perceptions about crime risk (Chadee et al., 2019; Abbott & McGrath, 2017; Logan & Walker,

2017; Gainey et al., 2011; Hale, 1996). Yet, results are mixed (Riek et al., 2015; Hale, 1996). On the one hand, some literature has found strong positive effects (Visser et al., 2013; Gainey et al., 2011; Rader et al., 2007; Wittebrood, 2002; Skogan, 1987; Tyler, 1984). On the other hand, other researchers have reported weak or no association between victimization and perceived risk (McGarrell et al., 1997; Liska et al., 1988). Meanwhile, crime victimization is experienced either through direct firsthand experience or vicariously through the experiences of others, including family, friends, and others.

In a study about the "Threat of Victimization" (Rader et al., 2007, p. 492), regression coefficients reveal that property crime victimization experience is a stronger predictor of perceptions of risk of criminal victimization ($B = .182$, $p < .001$). This means that respondents who experienced property crime victimization in the previous year estimated a higher probability of becoming a victim of crime. In a study of fear of crime using a telephone survey, Gainey et al. (2011) found that victimization has indirect as well as direct effects on risk perception and crime fear. The victims indicated feeling more terrified. In the indirect sense, respondents who experienced victimization tended to perceive elevated amounts of disorder and reduced degrees of trust, that culminated in elevated fear rates (pp. 132-133). After reviewing the research on crime fear and risk estimation, Tyler (1984) concluded that victimization experience, direct and indirect through friends and neighbors, influences crime fear and thus perceived risk. Accordingly, individuals with personal experiences with crime tend to perceive more risk and consequently exhibit heightened fear of crime. Equally, persons who have had an indirect experience of crime, through friends and neighbors, perceive more risk and fear crime more. On his part, using a series of regression analyses, Skogan (1987) found a consistent and robust pattern between victimization and fear. He concluded that "victimization affects both fear-related

attitudes and behavior in a clear and consistent manner" (Skogan, 1987, p. 135). He also concluded that victimization has a uniform effect across groups – the isolated, vulnerable, and the poor (Skogan, 1987, p. 149). Similarly, Visser et al. (2013) discovered that victimization, criminal fear, and sentiments of insecurity are strongly positively associated across European countries (p. 292). This indicates that victims of crime report more fear of crime and perceive more risk of victimization than non-victims.

In their analysis of the National Crime Survey (NCS) dataset, Liska et al. (1988) found a weak or small observed effect of fear on city crime rates and personal victimization (p. 832). They attributed the observed weak effect to the equally small number of persons who experienced victimization over the past year before the survey. Only 13 % of the 6,500 respondents in the subsample experienced one or more victimizations (Liska et al., 1988, pp. 832-833). Similarly, McGarrell et al. (1997) found that victimization (direct) had no significant effect on fear. They found only one-fifth of respondents reported having experienced victimization in the past six months (p. 484). This means that even though respondents reported that they perceived more crime risk and expressed fear, such perceptions of risk and feelings of fear were not related to actual criminal victimization.

Notably, the above studies and findings relate to place-based or physical crimes (e.g., physical assault, burglary, larceny-theft, automobile theft, racial and sexual harassment, and robbery, among others). Could the predominantly mixed findings between victimization and risk perception of conventional crimes be observed also in the cyber realm? The relationship between cybercrime victimization and risk perception has only been examined in a few research (exceptions include: Abdulai, 2020; 2016; Alshalan, 2006; Riek et al., 2015). As more crimes are committed in cyberspace with the internet age, examining the interaction between victimization

and risk perception in the cyber realm is crucial. My previous research was one of few studies exploring this cyber criminology area (see Abdulai, 2016). The few studies in this area have looked at victimization and fear and have not included risk perception. The caveat in most of these works is that fear and risk perception have been presented as almost the same. Theoretically, however, fear and risk perception have been viewed as different constructs (Ferraro, 1995).

In the field of cyber victimization, Riek et al. (2015) found that experience of cyber victimization preceded the perceived risk of cybercrime in the EU. In other words, European internet users with previous experience of cybercrime victimization perceive more risk of cybercrime. In my previous research (Abdulai, 2016), I found that students with an experience of credit or debit card fraud victimization tended to perceive more risk and feared becoming victimized again. Likewise, in his study of cybercrime fear and victimization among US households, Alshalan (2006) found a positive association between cybercrime victimization experience and people's fear. Alshalan also discovered an interaction between victimization experience and gender: women with prior experience perceived more risk and were more likely than others to fear cybercrime.

Thus, the above review reveals an important gap in the current literature on cyber criminology: a lack of research regarding the effects of cybercrime victimization on cyber risk perception. Filling the identified gap serves as one of the critical niches of this current research.

2.6 Perceptions of Cyber Victimization and Internet Use

Whereas fear of crime and victimization research abound, studies into the consequences of risk perception on behavior are limited (Rader et al., 2007; Rader, 2004). Researchers have

examined the impacts of perception of the risk of criminal victimization on behavior in terms of constrained behavior, including avoidance and defensive action (Rader et al., 2007; Rader, 2004; Ferraro, 1995).

Similar to much of the research in cyber criminology, there is limited research that has examined the consequences of cyber risk perception on the behavior of internet or technology users. A few exploratory studies in this area include Riek et al. (2015), Böhme and Moore (2012), and Saban et al. (2002). Riek et al. (2015) examined the consequences about perception of cybercrime risk in terms of avoiding services on the internet. By deploying structural equation modeling on a cross-sectional pan-European sample, Riek et al. found that cybercrime risk perception negatively impacts what he refers to as the three online services categories, namely online banking, shopping, and social networking (2015, p. 261). The implication is that there are significant reductions in the use of the three internet services by individuals who perceived a higher risk of becoming cybercrime victims. Thus, by avoiding the three online services, the behavior of such persons has been constrained by their high perceived cyber risk (Rader et al., 2007; Rader, 2004). Such behavioral constraint places people at a disadvantage by limiting their maximization of the benefits of the information and networked society. However, Riek et al.'s (2015) study only examined an aspect of constrained behavior (service avoidance) and did not examine defensive behavior as a consequence of cyber risk perception. Also, the fact that the study was based on cross-country data could have masked some intra-country differences. Unlike Riek et al. (2015), the current study incorporates both aspects of constrain behavior to reflect Canadians internet use behavioral responses to the risk of cyber victimization.

In a similar study in the EU, Böhme and Moore (2012) examined consumer internet use (online banking, shopping, and other activities) in response to cybercrime victimization. Their

analysis revealed that cybercrime experience, concern about cybercrime, and media exposure reduce consumer likelihood to use online services. In other words, through direct experience, worry, or media exposure, cybercrime leads to online service avoidance among consumers. Here again, this study focused on only an aspect of constrained behavior - service avoidance - and failed to look at the consequences of defensive behavior, which is considered in the present research.

On their part, Saban et al. (2002) studied the behavioral ramifications of cybercrime on consumers. Their analysis showed consumer experience with cybercrime negatively influences internet use, irrespective of gender, by reducing the "informational value of the internet," "repeat online purchases," and "the overall value of the internet as a viable marketing channel" (p. 34). In other words, the study established that cybercrime experience affects consumer internet behavior. Meanwhile, the study is not explicit on whether such behavioral impact pertains to internet service avoidance or defensive internet behavior, á la Rader et al. (2007) and Rader (2004). However, the study did suggest that reducing consumer internet behavior has more impact in the line of service avoidance.

Böhme and Moore (2012) and Saban et al. (2002) neglected a crucial aspect of constrained behavior by failing to consider defensive behavior as a response to cyber risk perception and victimization. The defensive part of constrained behavior is vital in technology (internet) use. Such a perspective is important because internet use has become central in the fabric of modern life, to the extent one can begin to see it as almost an act of compulsive behavior. Outright service avoidance may be neither possible nor desirable in the contemporary world. However, defensive behavior in response to cyber risk perception and victimization will ensure consumers minimize their risk while they continue to make the most of internet services.

2.7 Cost of Cybercrimes - for Businesses, Individuals, and Governments

As cybercrimes are on the rise with further advancements in technological developments, individuals, businesses, and governments have suffered tremendously. Individuals and businesses have to contend with the ever-changing landscape of viruses, malware, and phishing daily. Businesses and governments have to contend with the persistent threat to the security of sensitive corporate and national security information. Securing the critical infrastructures of nations has become a primary concern for governments. Cyberwars have also become real threats, especially following the 2007 and 2008 cyberattacks on Estonia and Georgia, respectively.

2.7.1 Cost to Individuals

Individuals, as the primary consumers of the internet or CMCs, experience impactful cyber security incidents. Similar to businesses, individual victims of cyber security incidents experience some costs resulting from their victimization. Typically, individuals experience monetary or financial losses from their encounters with cyber security incidents. According to Norton Cyber Security Insights Reports Global Results, consumers who experienced cybercrime globally lost $172 billion, with the average victim losing $142 (Symantec Corporation, 2018, p. 13). The Norton report covered an adult population of 3.1 billion in 20 countries. Cybercrime victimization results in immense financial costs.

Individuals also experience additional, non-financial, costs due to their cybercrime victimization. One of cybercrime's non-monetary costs is the time lost by individuals or consumers after victimization (Symantec Corporation, 2018). According to the Norton Cyber Security Insights report, "the average cybercrime victim spent nearly 24 hours (23.6 hours)

globally (or almost three full work days) dealing with the aftermath" (Symantec Corporation, 2018, p. 14). In the current postmodern competitive capitalist regime, time is of the essence as it is at the heart of efficiency. So, productivity is affected when cybercrime victims take this much time from their routine. The actual cost of the lost hours can only be seen with an attempt to quantify the lost productive hours.

People's feelings of dread and worry related to cybercrime also constitutes a non-financial cost. According to Accenture's 2017 Canada Cybercrime survey, an overwhelming number of Canadians (eight-in-ten or 80 %) are concerned about cybercrimes, with more than half of respondents indicating that such "concern about cybercrime is limiting their use of online services" (Accenture, 2017, p. 1). Concern about cybercrime victimization keeps Canadians from shopping more online (Grau, 2008). With concern about cybercrime victimization limiting utilization of the internet by individuals, businesses, and governments, the implication is that life in the postmodern contemporary era is affected. Such significance is premised on the rapid and massive penetration of the internet into the daily fabric of postmodern individuals, businesses, and governments. Internet penetration, according to Poushter et al., (2018), is "measured by internet use or smartphone ownership" (p. 5). Accordingly, some evidence indicates internet penetration is increasing even among developing economies despite the global digital divide (Poushter et al., 2018).

2.7.2 Cost to Businesses/Organizations

Even though this current study focuses on individuals, it is still essential to shed some light on how businesses and organizations also experience cybercrime. The rationale is also premised on the idea that internet and computer-mediated communication is utilized by organizations, with individuals working from the frontline.

According to a 2019 Juristat report, more than one-fifth (21 %) of Canadian businesses experienced impactful cyber security incidents in 2017 (Bilodeau et al., 2019). By disaggregation, such significant incidents affected 19 % of small businesses, 28 % of medium-sized enterprises, and 41 % of major corporations (Bilodeau et al., 2019, p. 5). Meanwhile, business consequences of increased and sophisticated cybercrime attacks are high, with organizations increasingly spending more to deal with attacks (Accenture Security, March 6, 2019). In the year 2018, for instance, affected organizations lost an average of $9.25 million from cyber-attacks, losing $2.96 million from business disruption and $3.8 million from information loss (Accenture Security, March 6, 2019). Small-scale businesses or start-ups with more limited resources, then, can be expected to face much more significant impacts from business disruption and information loss.

In the case of Canadian businesses, Bilodeau et al. (2019) also found that employees of more than half (54 %) of the businesses which were affected by cyber-attacks could not perform their day-to-day work (p. 6). Also, while about one-third (30 %) of such enterprises incurred additional repair or recovery costs, close to 10 % of businesses reported losing revenue because of such impactful cyber security attacks (Bilodeau et al., 2019, p. 6). Additionally, some businesses reported reputational damage because of the incidents (Bilodeau et al., 2019). The cost to reputation is intangible and might appear less important; however, it is essential for business viability. Reputational damage has an indirect effect on businesses in terms of reduced revenues. To remain in business under such situations, enterprises must take proactive measures to win back customers' trust. Unsurprisingly, "4 % of businesses had to reimburse external parties or make ransom payment" and some businesses (2 %) had already lost their clients in suppliers, customers, or partners (Bilodeau et al., 2019, p. 6).

As a result of such impactful cyber security incidents, businesses need to adopt measures to minimize their vulnerability to these cyber security incidents. As such, according to the Juristat report (Bilodeau et al., 2019), Canadian businesses have become proactive in adopting cyber security measures to protect their businesses, customers, and partners. Anti-malware software is the popular cyber security measure adopted by a majority (76 %) of Canadian businesses to "protect against viruses, spyware, ransomware, and other similar attacks" (Bilodeau et al., 2019, p. 12). An overwhelming majority (94 %) of Canadian firms earmarked some funds to prevent and detect cyber security incidents in 2017, spending $78,000 on average to implement such measures (Bilodeau et al., 2019, p. 10).

Even though the cost of cybercrimes to businesses is substantive, there is also the question of to what extent businesses report their encounters with cyber security incidents to the police. Generally, the view is that the actual scope of cybercrimes is underestimated because most incidents go unreported (Bilodeau et al., 2019; Chawki et al., 2015; Kshetri, 2010). As an illustration, within Canada, only 10 % of businesses that experienced cyber security breaches reported their experiences to the police (Bilodeau et al., 2019). Companies and victims of cyber-attacks may feel reluctant or refuse to disclose their experiences with impactful cyber-attacks for various reasons. A consequence of such reluctance is that the true extent of cybercrimes will continue to be shrouded in mystery. Consequently, an accurate estimate of losses from impactful cyber-attacks is currently impossible.

From the above review of the cost of cybercrimes to businesses and organizations, there are different dimensions to the issues and effects of victimization. These issues and effects are relevant to this study’s research questions because businesses and other organizations are corporate entities whose experience of cybercrimes is similar to individual internet users. The

research questions will also serve as a yardstick to measure the differences in the experiences of individuals and businesses with cybercrimes.

2.7.3 Cost on Governments

Similar to the review of the costs of cybercrime on businesses, this section on government is imperative because the government is also an entity that utilizes the internet and other forms of computer-mediated communications in its daily activities or business of governance. Reflecting on governments' experience of cybercrime cost broadens the scope of information and understanding cybercrimes' menace.

Similar to individuals, businesses, and organizations, governments face their share of concerns and costs resulting from cyber-attacks. One of the main areas of concern or costs of cybercrimes for governments is the impact on political and national security (Kshetri, 2010). As the government is the number one guarantor of peace and national security, this area of interest for governments is compelling. Cybercrime's political and national security impacts are intertwined because the realm of politics is linked with a sovereign country's security. As a result, cyber-attacks on a country's critical infrastructure and other vital installations threaten national and political stability. For example, the US Department of Homeland Security has reported numerous cyberattacks against US federal agencies (Kshetri, 2010, p. 6). The much-publicized cyber-attacks on Estonia in 2007 and Georgia in 2008 project the political and national security cost of cybercrimes on governments. A recent case that can be viewed as similar to the Estonian and Georgian cases is the much-debated "Russian meddling/interference" in the 2016 and 2020 United States (US) presidential elections. The "Russian meddling," real or putative, has been described by some politicians and intelligence community members as cyber warfare, reflecting an attack on US national interest. Over here in Canada, the government has

also had concerns about cyber security. There have been numerous breaches in government entities in Canada e.g., the recent Canada Revenue Agency (CRA) breaches. For context, in September 2020, the CRA discovered through a forensic audit that over 48,000 accounts from the over 14 million user accounts had been compromised with cyber breaches (Canada Revenue Agency, September 2020). Seen in this way, cybercrimes (cyber-attacks) pose a significant challenge, and thus cost, to governments because of their potential consequences.

2.8 Reporting Cybercrime Victimization

Given the costs of cybercrime victimization, one would expect that victims and prospective victims would want to report their experiences of suspicious actions in cyberspace. However, cybercrime reporting generally is a problem that permeates under-developed societies and extends to their developed counterparts (Goudriaan et al., 2004). A preponderance of research has generally focused on crime reporting. As most crimes have transitioned into cyberspace, a sizeable chunk of research has, up to this point, concentrated on cybercrime victimization reporting. These studies have examined the challenge in informing the police and other agencies about cybercrime and the factors that contribute to the general lack of interest in reporting (Bidgoli & Grossklags, 2016; Goodman & Brenner, 2002; Goucher, 2010; van de Weijer et al., 2019; Wall, 2008; Yar, 2013).

Most cybercrime victims do not contact the authorities about their experiences. For instance, only 13% of victims in the Netherlands in 2017 disclosed their experiences to the police. In the Netherlands in 2017, for example, only 13 % of victims reported their victimization to the police (CBS, 2018). In their qualitative studies, Burgard and Schlembach (2013) and Bidgoli (2015) also found hesitancy to report victimization among cybercrime victims. These

findings are worrying because it means the scourge of victimization is likely only to increase in trajectory.

The hesitancy to report cybercrimes has also led to research to understand the factors behind such reluctance (for example, please see Goucher, 2010; Wall, 2008; Yar, 2013). A survey of some of the literature about the reasons for cybercrime victims and prospective victims' lack of reporting of cybercrime encounters includes the following:

i. Perceived offense seriousness affects reporting of cybercrimes: that is, victims' perception that the cybercrime experienced is less severe than other potential cybercrimes (Wall, 2008; Yar, 2013).
ii. Victims' lack of trust in the reporting process, distrust in the police, self-blaming, and shunning of the label of a "victim" have been identified as reasons for underreporting cybercrimes (Goucher, 2010, p. 17).
iii. Victims may be initially unaware of being victimized (Goodman & Brenner, 2002; Wall, 2008; Yar, 2013). Due to the nature of cybercrime, some people become victimized without knowing and only realize it several days or weeks after receiving e-bills.
iv. Victims may fear reprisal, especially when the offender is known to them. Reprisal may occur, for example, through cyberstalking or cyber-harassment (Bidgoli & Grossklags, 2016, p. 2).
v. There are a multitude of agencies to which to report; for instance, Cross et al. (2016) discovered in their Australian research that some victims fail to notify the police because of the existence of multiple agencies to whom victims can report their experiences. In these situations, victims tend to lack knowledge of appropriate channels to which to

report (Bidgoli & Grossklags, 2016, p. 4). Consequently, the reporting process is impeded rather than becoming facilitated.

While the above factors relate more directly to individual cybercrime victims and prospective victims, several factors have been identified to account for businesses' lack of reporting cybercrime incidents. In the specific case of Canadian companies, however, the following factors have been outlined in the Juristat report (Bilodeau et al., 2019, p. 7):

i. Over half (53 %) of businesses had incidents resolved internally, i.e., non-report due to internal resolution.
ii. Over one-third (35 %) had incidents resolved through IT consultants or contractors, i.e., non-report due to resolution by IT consultants or contractors.
iii. Nearly a third (29 %) failed to report because they viewed the impact to be minimal, i.e., non-report due to underestimation of the impact.
iv. Over a quarter (26 %) of businesses did not think of involving the police.
v. Non-reporting because of lack of trust in the police and judiciary system was identified by 13 % of businesses.
vi. Non-reporting due to an unclear incident reporting system affected 4 % of businesses.
vii. Non-reporting due to a lack of satisfaction with the initial police response impacted 2 % of businesses.

Some research has also explored the determinants of cybercrime reporting among those who choose to report their experiences. For example, in their study of cybercrime victimization reporting, the following factors predicted cybercrime reporting behavior (van de Weijer et al., 2020, p. 26):

i. Type of cybercrime – They discovered in their study that respondents seem more inclined to report credit card fraud than other cybercrimes.

ii. Offense seriousness - more severe offenses were often reported, and the opposite was also true (OR = 2.86, p<.01).

iii. Role of victim-offender relationship – Where the victim knew the offender personally, crimes were less likely to be reported (OR = 0.74, p < 0.01).

iv. Age – While age significantly predicted reporting, with older respondents more frequently intending to notify the police than younger ones (OR=1.02, P<.001), it was noted that gender, marriage, parenting, educational level, employment, and income had no significant effect on reporting.

v. Victimization experience – Victims who had never previously informed the police of their experiences were less likely to report in the research (OR = 0.73, p<.05) than respondents without prior experience. In contrast, past victims who had previously registered their experiences were more likely (OR =1.65, p<.01) than non-victims to indicate a willingness to contact the authorities.

vi. Attitude toward police (OR=1.17, p<.01) and fear of being a victim of cybercrime victimization (OR=1.19, p<.05) – Respondents who had a positive attitude toward the police and were afraid of victimization were associated with a higher likelihood of notifying the authorities.

Notwithstanding the challenges of reporting cybercrime, reporting cybercrime has associated advantages. In their study of "*End user cybercrime reporting,"* Bidgoli and Grossklags (2016) identified some merits of reporting cybercrime, including the following (p. 2):

i. Reporting cybercrime has an educational function by serving as a source of diverse forms of data, e.g., cybercrime prevalence, their forms and characteristics, as well as the harm or loss they cause (e.g., emotional, monetary, mental).

ii. Evidence from reporting on cybercrime can be used to formulate preventive measures to educate users.

iii. Law enforcement can use reporting data to correctly resolve the crime for the victim, including apprehending the offender or recovering the stolen property.

2.9 Insights from the Literature and Implications for the Current Study

The review of the literature provides some insights and implications for the direction of the current work. For example, this study will be among the first to focus on cybercrime generally, as opposed to a specific type of cybercrime. Also, much like traditional place-based crimes, there is conflicting evidence in the literature regarding the association between sociodemographic factors, perception of fear, and the probability of being a victim of cybercrime. Women, for instance, express heightened fear of online interpersonal victimization, cyberbullying and harassment, as well as general concerns about computer viruses, theft, and hacking (Henson et al., 2013; Virtanen, 2017; Pereira et al., 2016) but never of online identity theft, viruses or scams (Robert, Indermaur, & Spiranovic, 2013; Yu, 2014).

My MA work revealed that people's perceptions of risk and fear of becoming a victim of credit or debit card fraud were unaffected by their gender (Abdulai, 2016). Similarly, Reisig et al. (2009) argue that gender makes no difference in risk perceptions and fear of non-contact crimes. On the other hand, Alshalan (2006) found an interaction effect of gender on victimization experience; thus, women with prior victimization experience are most inclined than other women

to fear cybercrime. These mixed or inconclusive studies regarding the impact of sociodemographic factors, specifically gender, on risk perception and fear of distinct types of cybercrimes point to a void in the literature. Findings from the current study will be compared with those of previous studies to discover potential sources of variances.

The literature on victimization experience and risk perceptions of cybercrime are inconclusive and in their infancy. The association between victimization and risk perceptions about traditional crimes has been the subject of extensive and well-established research (examples include Visser et al., 2013; Russo & Roccato, 2010; Fox et al., 2009; Rader et al., 2007; Wittebrood, 2002; Weinrath & Gartrell, 1996; Skogan, 1987; Tyler, 1984). The same cannot be said for cybercrimes. Findings from the few studies regarding victimization experience and cybercrime fear vary. As an illustration, Henson et al. (2013) discovered that victimization is linked to a considerable fear of interpersonal victimization on the internet by a close partner rather than by a stranger. Also, Yu (2014) discovered that victim experience is unrelated to fear of web scam but cyberbullying and computer viruses. These limited findings from the literature regarding the various metrics and variables of interest point to a niche that this study seeks to fill through a nationwide study in Canada.

The literature review has revealed that some studies have looked at constrained behavior, encompassing avoidance and defensive behaviors as a behavioral ramification of risk perception. Such studies, including Rader et al. (2007) and Rader (2004), have predominantly focused on conventional crimes. The few cyber-related studies (for example, see Riek et al., 2015; Böhme & Moore, 2012; Saban et al., 2002) have either only weakly or partially focused on an aspect of constrained behavior or neglected to look at the impact explicitly in terms of either avoidance or defensive behavior, or both. Therefore, the current study will extend the literature to examine the

consequences of both victimization and risk perception of cybercrime on internet users' avoidance and defensive behaviors.

Insights from Alshalan's (2006) study of victimization and fear using survey methodology had implications for the current study's design and data collection method. Methodologically, this study's focus on individual users of the internet and computer-mediated communications is informed by the theoretical insights from Beck's (1992) Risk Theory and Coleman's (1990) Rational Choice (see Chapter 3). Specifically, in terms of methodology, Alshalan's (2006) work brought out two key issues that corroborate Risk Theory and Rational Choice: the suitability of targeting individual users of the internet and the suitability of the survey method of data collection for studies of the nature. Consequently, this study collected data from individual internet users using a survey instrument.

Chapter Three: Theoretical Approaches to Cybercrime Risk/Victimization - Theoretical Framework

3.0 Introduction

In this chapter, I review some theoretical literature and present the theoretical framework for the study. The theoretical framework aims to explain why Canadian internet users continue to use various forms of computer-mediated communication despite the fear and inherent risk of victimization in cyberspace. In other words, has the perception of cybercrime risk changed how Canadians use the internet? Criminal victimization is a much-researched area in socio-criminological studies, especially under fear of crime studies (Abdulai, 2020; Collins, 2016; Farrall et al., 2012; Ferraro, 1995; Ferraro & LaGrange, 1987; Garofalo, 1981; Hale, 1996; Hinkle, 2015; Lee & Mythen, 2017; May et al, 2010; Rader et al., 2007, Riek et al., 2015; Sreetheran & Van Den Bosch, 2014). However, most of such research is focused on crimes perpetrated in the physical world, that is, place-based or conventional crimes (Collins, 2016; Farrall et al., 2012; Ferraro, 1995; Ferraro & LaGrange, 1987; Garofalo, 1981; Hale, 1996; Hinkle, 2015; Lee & Mythen, 2017; May et al., 2010; Rader et al., 2007). The default focus on place-based crimes could reflect the origins of crime. However, with the evolution of societies in line with social change and advancement in technological developments, an extension of crime from the physical realm to other realms of action (cyberspace) becomes automatic. The modus operandi of cyber criminality has meant traditional socio-criminological theories do not sufficiently explain the problem of cybercrime and its associated issues; hence they need to be reconsidered and amended in this context or new theories all together are needed. That is to say, cybercrime occurs virtually in cyberspace and across geographical boundaries where anonymity and flux are prevalent. These defining attributes explain the non-suitability of traditional socio-

criminological theories, which have a more suitable application for crimes in physical space. In this chapter, first, I examine and discuss some relevant theoretical perspectives with an emphasis on how they apply to the problem of the current study. Theories reviewed include Beck's (1992) theory of a risk society, Coleman's (1990) rational choice theory, and Bauman's (2000) liquid modernity and liquid fear theory. Next, I discuss sociology's age-old theoretical tension between structure and agency and how cybercrime risk fits the debate. I follow this in the next section by moving the focus away from the two extreme poles in the debate to the middle ground, using Giddens' (1984) structuration with insights from Stones's (2005) strong structuration brackets. Finally, I present the integrated theoretical framework guiding the current research.

3.1 Theory of a Risk Society

The risk society theory is a critical late modernist theory that critiques the contradictory nature and impact of the development of scientific knowledge and advancement. Primarily, this theory places ideas of risks as its central focus due to the tremendous techno-scientific advances in the modern era. Beck (1992) asserted that "the consequences of scientific and industrial development are a set of risks and hazards, the likes of which we have never previously faced" (p. 2). Therefore, in Beck's view, the dangers and side effects of technological and industrial advancements are not constrained by time or space, and none can be held accountable for such risks.

Cybercrimes, which are crimes conducted using computers as a tool or object, are crimes that transcend space and time and can be perpetrated concurrently in several places. These defining attributes of cybercrime make scientific developments related to the computer inherently risky. In 'Becksian' language, the dangers of cybercrimes are limited neither in time nor space. Considering these inherent risks, however, Beck calls for optimism. He argued that

radicalised rationality, which views reflexivity as a crucial component in the evolution of civilizations, can be used to manage the impacts of the dangers (Beck, 1992). Radicalized rationality describes a situation where individuals exhibit heightened or exceptional calculation, whereas reflexivity refers to agents developing a questioning attitude, being active, and not merely giving into structure.

Significantly, Beck's theory suggests a fundamental shift in the broader social and technological milieu in which people have been positioned in late modernity as active agents. The society is a unique social structure that operates on axial principles that are distinct (Beck, 1992). The distribution of "bads or hazards" and individualism's fundamental dominance are the central tenets of risk society (Beck, 1992, p. 3). These axial tenets lend credence to the transformations in both the social and technological spheres. The “bads or dangers” refers to Beck’s perspective about the nature of the unintended consequence of techno-scientific developments, thus contradictory with negative ends. An example that illustrates how “bads or dangers” are distributed within risk society is the Chernobyl nuclear disaster in 1986. The transformed technological context of the current era has placed technology and its tools and products on a central pedestal. The utilization of the internet has become a crucial aspect of late-modern life. Beck’s submission that a tenet of the risk society is its structuring through individualism makes his theory methodologically individualistic. Individualism within the risk society is embedded in the changed (and changing) social context, a radical displacement of the status quo experienced in pre-modernity and modernity. As such, the methodological standpoint of Beck’s theory is instructive for data collection in the current study. Rather than focusing on groups, the inclination is a focus on individual actors because they are active users with an agency, not passive recipients. Such emphasis on individuals is because internet users (actors or

participants in the study) choose to use the internet for different purposes and to varying frequency levels, thus asserting their agency.

In this author's previous research on cybercrime victimization experience and fearfulness (Abdulai, 2020), the non-predictive significance of socio-demographic variables on credit or debit card theft was accounted for by pointing to the nature of risk in late modern society. Risk has significantly increased in late modernity, an increase that is inspired by and experienced as a result of technical improvements. The system immanence of risk (Beck, 1992) means risk is inescapable irrespective of an individual's socio-demographic categorization. Additionally, Abdulai (2020) underscored that cybercrime is not place-bound; it occurs in cyberspace without the victim and perpetrator ever meeting. As a result, neither the victim's physical appearance nor any other demographic information is considered. Using insights from the risk society theory, Abdulai presented that technological advancements have rendered risk a flux phenomenon and transformed the nature of risk from the conventional physical realm to the non-conventional cyber domain. As a result, he argued that Beck's risk theory is a valid theoretical starting point to explain cybercriminal victimization. The danger connected with using the internet can be better understood using Beck's thesis. Additionally, the theory can help shed light on some of the predictors of these risks.

Risk society theory leaves some gaps in understanding the interconnections between motivation and knowledge of the risk of internet use and its consequent victimization. Beck's theory thus explains only part of the current study's problem. Consequently, this study adapts aspects of Beck's risk society theory as part of a comprehensive, integrated theoretical framework. Specifically, Beck's theory will be used to understand people's risk perception and fear of cybercrime victimization vis-à-vis their use of the internet and computer-mediated

communications. However, since Beck's theory does not offer reflective insights into actors' internet use patterns, motivations for use, and knowledge of risk, components of a different theoretical perspective will be incorporated to make sense of the other foci of the study.

3.2 Rational Choice Theory

The Rational Choice theory (Coleman, 1990) accounts for the behavior of individual actors and agents instead of group action. As a result, individualism forms the core of the theory. Essentially, Rational Choice thesis holds that individuals are rational and calculating actors who primarily make decisions informed by self-interest and optimality (Coleman, 1990). Actors also consider individual preferences and the opportunities or constraints unique to each person (Coleman, 1990). Given that broader social actions result from the aggregation of individual actions, rational choice theory indirectly accounts for group action by explaining individual motives for action.

The empirical utility of the Rational Choice model is the emphasis on actors' connection to and interest in resources, as they pattern their interest maximization drives through what he called "the transfer of control over one's action to another … made unilaterally, not as part of exchange" (Coleman, 1990, p. 198). Individuals transfer control to maximize their utilities, producing or maintaining social equilibrium. This empirical research path was driven by Coleman's (1990) conviction that:

> Actors are connected to resources (and thus indirectly to one another) through only two relations: their control over resources and their interest in resources. Actors have a single principle of action, that of acting to maximize their realization of interests. Such action can be simply consummatory, to realize the

> actor's interest; if it is not, the maximization principle leads most often to a single kind of action - exchange of control (or rights to control) over resources or events (Coleman, 1990, p. 37).

Methodologically, Coleman developed the Coleman boat or the schematic diagram of the macro-micro-macro data collection model (1990, p. 8-10). The model prescribes that researchers unpack the three stages of rational action which motivate actors'' momentary and unilateral transfer (of) control over their data to cybercriminals. For my research, this would necessitate the interrogation of:

1. the macro environment (the component of structure) and how these pattern actors' internet use action orientations (the preferences and beliefs that pattern individual action),
2. how actors' action orientations pattern or influence individual action, and
3. how cybercriminals' activities produce micro-level outcomes that feed into the macro environment to (re)create conditions for future action.

In other words, the above is the macro-micro-macro model of action as they relate to motivations for internet use.

Individual actors are typically the unit of analysis within the environment of internet usage and other CMCs. Consumers of online shopping, for instance, are individuals who choose to go online instead of physically walking into stores. Customers who utilize online banking for banking needs are individuals who decide to go online rather than walk into banking floors to undertake business-related transactions. Similarly, patrons of internet chatrooms act as individual actors instead of meeting up with and interacting with the other individuals on the other side of

the computer. Furthermore, present-day students and researchers do much research online instead of combing through stacks of journals and manuscripts from library shelves.

Meanwhile, by using the internet for varied purposes, businesses and governments constitute units of analysis, even though individuals act for and on their behalf. Companies and organizations carry out transactions through electronic communications (the internet). Businesses also store sensitive financial and client information and other confidential documents on various computer media and platforms. Governments use the internet to conduct the business of governance. Critical infrastructure such as power grids, water, and armaments are controlled with the internet. The situation generally holds for all computer and internet use forms. Given its individualistic focus, Rational Choice theory operates from the epistemological standpoint of interpretivism. With interpretivism, the idea is that "people act on the basis of the meanings that they attribute to their acts and to the acts of others" (Bryman et al., 2012, p. 9).

Actors' (individual internet users) association or connection to and interest in resources (the internet and its related tools and products) shape their decisions regarding internet use, which underpins the practical utility of Coleman's rational choice model within the context of the current study.

The challenge with Rational Choice as an explanatory framework for cybercrime is that it does not account for the structural (the technological) component due to its overarching emphasis on individualism. Rational Choice makes it possible to gauge the plausible reasons actors use cyberspace for different ends as individuals. However, such behavior occurs within a context patterned by societal structures. Also, Rational Choice does not speak to the source or root of cybercrime – a by-product of technological advancement. Notwithstanding the challenge, Rational Choice theory can serve as a helpful explanatory framework to understand internet

users' actions and motivations for using the internet, an essential component of this study. Based on the specific push or pull factor, actors' motivations may generally be classed into two main types – intrinsic and extrinsic – based on a probable understanding of the source of actors' decisions.

3.3 Liquid Modernity and Liquid Fear

Bauman's concept of liquid modernity relates to the transition out of a 'heavy' and 'solid' hardware-centred society to a 'light' and 'liquid' software-inspired one (Bauman, 2000, pp. 1-8). Liquid modernity is characterized by transformation, change, and a dismantling of boundaries regarding the status quo. In other words, fluidity and flux are essential hallmarks of liquid modernity. In this way, Bauman's conception of the current era as liquid modernity is not unlike Beck's theorization of the risk society. Further, for Bauman, some common aspects of the modern era are fragility, temporariness, the vulnerability of life, and the inclination to constant change. This is opposed to the previous conception of change as a temporary means to realizing a more stable end. In this way, Bauman converges with Beck's assertion that techno-scientific development has rendered change a constant theme and thus uncertainty (Beck, 1992).

Consequently, according to Bauman (2006), liquid modern time is characterized by instability, ambiguity, and endemic uncertainty. Though a source of opportunity, such uncertainty has also created pervasive fear in the liquid modern era. The flux and uncertainty in liquid modernity also create opportunities for persons with criminal intentions to commit cybercrimes by exploiting the vulnerabilities both among technologies and unsuspecting potential victims. Therefore, the ambiguity or uncertainty of security in cyberspace, which has created opportunities to commit cybercrimes and landed some internet users as victims of online victimization, can be viewed as a consequence of Bauman's liquid modern time. Cyberspace has

contributed to the dismantling of physical boundaries. It has empowered internet users – both unsuspecting good-intentioned and ill-intentioned users – to traverse multiple boundaries at any given time and in the comfort of homes, offices, libraries, etc. While the pervasive uncertainty in the liquid time and thus cyberspace mean unsuspecting internet users may entertain some fear while engaging in online transactions, users with deviant motives use the flux of liquid time and cyberspace to traverse boundaries from the comfort of their own chosen spaces. The fear or uncertainty considered by internet users is linked to the fact that the space of internet activity – cyberspace – is in constant flux (liquid in "Baumanian" terminology).

The utility of Bauman's theorization for this study lies in how ideas of fluidity and change patterns internet use, cybercrime risks, cybercrime victimization experiences, and the intent to and actual commission of cybercrimes. In other words, Bauman's theorization is helpful for understanding the environment in which fluidity and change have emerged. The internet facilitates the perpetuation of liquid time by allowing people to engage in social action at a distance and beyond geographical boundaries – in cyberspace. Meanwhile, cybercrime risk can be understood as a correlate of endemic uncertainty, a characteristic of the liquid modern time. Such risk also manifests due to internet users' agency in the fluid era. And like risk, cybercrime victimization can be seen as a consequence of living and acting in the uncertainty of liquid time. The state of flux occasioned by the liquid era means internet users can hardly control the consequences of their actions in cyberspace. Then, the result of using the internet is that users live in a constant state of (liquid) anxiety because the fear is out there, though not necessarily tangible relative to the fear of conventional crime victimization. Alternatively, such fears may also be tangible because of the knowledge - directly or indirectly - that many people have about forms of victimization by cybercrimes.

However, the challenge with Bauman's theory is that, like Beck, it does not immediately explain actors' motivations for engaging on the internet. Also, Bauman's theory has no explanatory power regarding internet users' behavioral responses – avoidance and defensive – to cybercrime risk and fear of victimization. As rational and reflexive agents, how do internet users react to the consequences of living in a liquid time in using the internet? Additionally, Bauman's theory has been criticized as overly theoretical, lacking empirical work to underscore its application and validity (see Lee, 2006).

3.4 Cybercrime Risk Within Structure and Agency Discourse of Sociology:

This study is built on the foundational sociological principles of structure and agency, principles that have been at the heart of much sociological theorizing. As a result, it is imperative to review and situate cybercrime victimization within the theoretical nexus of structure and agency.

The structure versus agency debate has been an enduring theme in the social sciences, especially sociology. The controversy dates to the work of the classical theorists (the founders) of sociology and is prevalent among contemporary theorists. Inferences from Archer (1996) and Giddens (1984), among other social theorists, suggest that the structure and agency conundrum constitute a most significant theoretical dilemma. The crux of this argument "concerns the issue of to what extent we as actors have the ability to shape our destiny as against the extent to which our lives are structured in ways out of our control; the degree to which our fate is determined by external forces" (McAnulla, 2002, p. 271). In other words, do human beings merely give in to the dictates of broader social forces, or do they consciously exercise choice and discretion over their actions? Do people have options and control when it comes to internet use? Do they also have a choice regarding the consequences of their actions in cyberspace? Also, do they have

discretion regarding subsequent conduct in cyberspace after experiencing the results of their previous actions? These questions reflect the debates about structure and agency in social action.

Generally, there exist three main strands of the structure and agency debate. The structure perspective, the first strand, emphasizes the decisive nature of social structures in constraining individual behavior. Durkheim's (1938) and Parsons' (1954) theorizing represent this position. In their works, the beliefs, values, sense of choice, norms, and identity – in a sense, an individual's worldview – can be traced to society (Calhoun et al., 2012; Joas & Knobl, 2009; Turner, 2014). Individual action, accordingly, is a product of society or structure. For instance, in his *Rules of Sociological Method*, Durkheim (1938) advanced the concept of social facts - powerful external forces, which coerce and motivate individual action. Norms and values (structure) are examples of social facts which are part of the social system and thus propel individual action in society. However, a challenge of structure theorizing is that when social control in the form of sanctions is no longer functioning or weak, individual actors are likely to follow their passions because of their innate self-seeking nature. In physical and cyber spaces, deviance and criminality become the outcome of such scenarios. A second limitation is that structural or structuralist arguments propose an extreme and too rigid causal determinism of social life, often contradicted by social experience.

The second strand, the agency perspective, emphasizes the decisive role of actors in social action, that is, in the creation and transformation of structures. Utilitarian theorists such as Weber (1978) and James Coleman (1990) represented agency proponents. The agency perspective gives credence to the role of individuality and speaks to actor autonomy to self-regulate their behavior. The agency perspective underpins the liberalist notion of freedom wherein individuals freely agree on the normative standard and how to safeguard their

fundamental freedoms, thus representing typical agency thinking (Calhoun et al., 2012; Joas & Knobl, 2009; Turner, 2014). Unlike the structure strand, according to agency proponents, society is a product of individual action. In his sociological theory, Weber (1978) asserted that *Verstehen*, translated as "interpretive understanding" or “sympathetic understanding” (Bryman et al., 2012) of the actor within any action context, should constitute a crucial task for sociologists. In his action theory, Weber stressed the importance of the acting individual, the interactions between actors, and the ensuing subjective interpretations which arise from such interactions. In Weberian sociology, one may find that rational-oriented actors engage in cybercrime instead of the cyberinfrastructure influencing them into cyber criminality based on calculating their potential benefits against the cost.

Similarly, internet use will emanate from actors’ estimates of the calculus of benefits and costs. So, if internet users decide that the benefits of using the internet far outweigh the risk or prospect of victimization, they may choose to access it. However, the utilitarian perspective has also attracted criticism because of its over-reliance on human agency. The main problem is that not all human actions are goal-oriented such as, for example, altruistic behavior.

The third and final perspective of the debate argues that structure and agency play equally important roles in social action. The third perspective emphasizes the dialectical interaction between structure and agency in the human social experience and is represented by Giddens' (1984) structuration theory (Calhoun et al., 2012; Joas & Knobl, 2009; Turner, 2014). Giddens incorporated both structure and agency in his action theory without according primacy to either component. In his structuration theory, Giddens argued that a structure possessed a dual nature. Rather than see structure and agency as two sets of disparate phenomena (a dualism), he argued the two should be seen as representing a duality (p. 25). By this, Giddens meant that “social

structure is used by active agents; in so using the properties of structure, they transform or reproduce this structure" (Turner, 2014, p. 139). In other words, two possible outcomes result when actors use social structure: they either produce the same structure (reproduction) or transform the structure (transformation). In this way, unlike Durkheim's concept of social facts, which envisions structures as external, structures from Giddens' (1984) structuration are internal to the activities of agents as they recreate such structures by their actions (p. 25). Also, implicitly, active agents have power or influence over structures in the transformational sense. Additionally, agents can be both human and non-human, and for Giddens, all agents have (at least some) control in the transformational sense (Calhoun, 2012, p. 277).

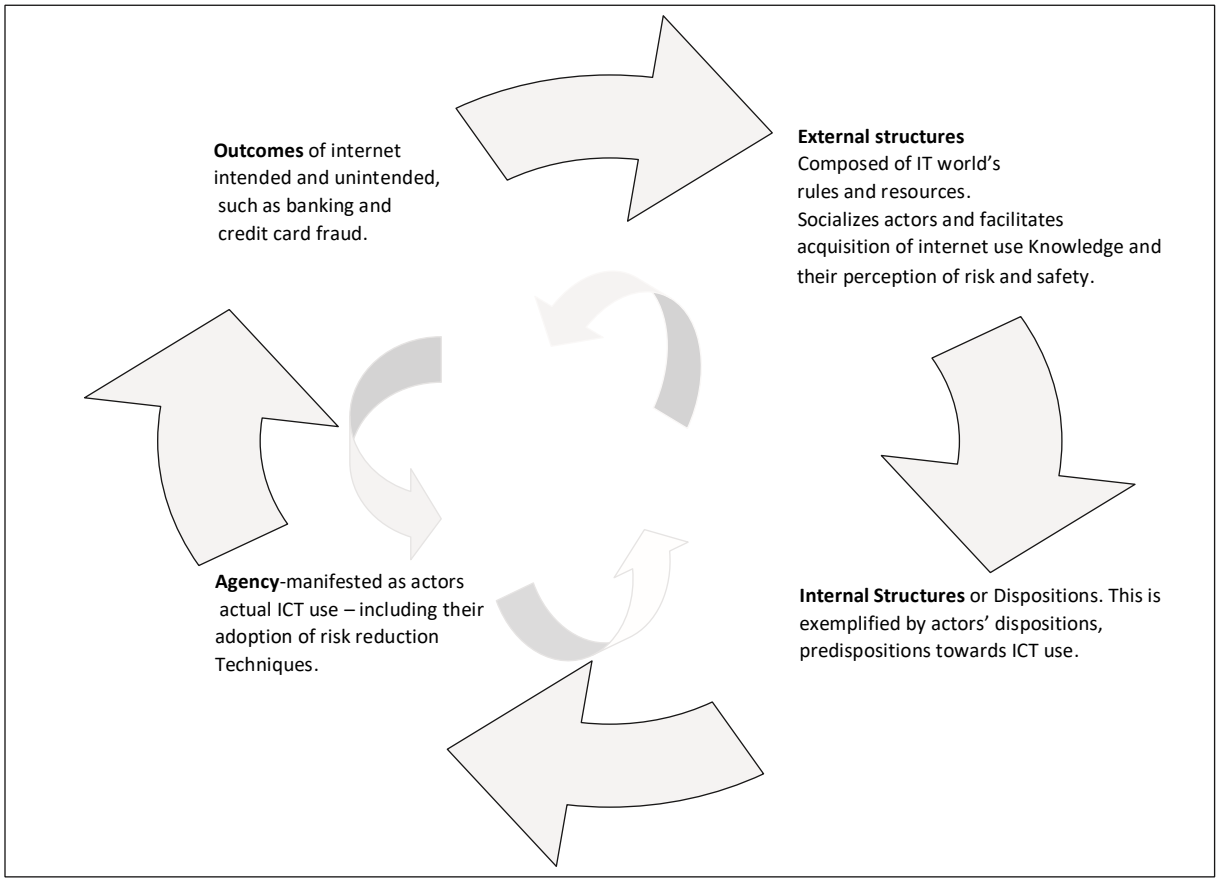
Giddens (1984), in *The Constitution of Society,* conceived of structure as constituting both rules and resources employed by agents in "interaction contexts" that span "space" and "time" (Turner, 2014). Using guidelines and resources, actors maintain or replicate structures in space and time. This clarification or addition by Giddens is analytically significant because it helps explain the interaction process and thus contributes to the understanding of social action.

However, structuration theory has also attracted some criticism. First, Giddens (1984) is criticized as too agential; that is, he accords agents with much primacy and appears to conflate both agency and structure (Archer, 1996). However, this criticism, is likely due to an inadequate or incorrect reading of Giddens. Giddens developed the structuration theory to mediate the strict dichotomy of structure and agency discourse. Another criticism of structuration is that it is too theoretical, and that Giddens (1984) failed to provide practical research guidelines about how researchers can use structuration in empirical research. In response to this criticism, Stones (2005) reworked structuration theory for empirical research in response to the above criticisms. Stones's (2005) reworking of structuration theory provides researchers with concrete research

brackets. Stones (2005) drew ideas from Margaret Archer, Pierre Bourdieu, and others to offer the Strong Structuration Theory (SST) as practical guidelines. Figure 3.1 shows the structuration cycle of cybercrime. The figure is an adaptation of Okonkwo's (2013, p. 14) "recursive sexual risk-taking influence cycle," which was developed using insights from Stones's Strong Structurationist research brackets.

Using the internet on a computer provides an example through which to see how structures and agents interact as envisaged by structuration theory, which informs this research. In Figure 3.1, one can see that the Information Technology (IT) world's rules and resources, such as anti-cybercrime guides, the computer, the internet, and allied security protocols and software, constitute external structures to actors. They socialize actors' internal structures or dispositions and predispose them towards the utilities and relative safety of the online world for convenient shopping, banking, e-commerce, and research. Drawing on these predispositions, actors purposively (employing agency) use desktop and laptop computers, phones, and tablets to go online, which produces both intended (e.g., convenient banking) and or unintended *outcomes* (e.g., cyber–fraud) - the analytical last stage of the structuration cycle. The knowledge of these intended and unintended outcomes (convenient banking and cyber fraud) filters back into the external structure through the media and peer ideologies to renew the structuration cycle anew.

Figure 3.1. Recursive cybercrime influence cycle



Source: Adapted from Okonkwo, 2013, p.14

This current study argues against an extreme position on the debate. In current times (late modern times, according to Beck), the reality of social life and the consequences of transformations in the social and technological realms have ensured that a dichotomy of structure and agency is no longer tenable. It is essential to recognize that the various perspectives represent dominant theoretical persuasions at various times in the historical trajectory. Like Kuhn (1970) argued, the different strands of the structure and agency debate represent paradigms that attempt to proffer convincing or adequate explanations for problems of the day. Theories serve as explanatory tools for action and society.

3.4.1 Cybercrime Ecosystem as Structuration

The innovation-based framing of the evolution of cybercrime is fitting because crime generally, and cybercrime especially, is a crime of innovation, resulting from advancements in techno-scientific innovation. In advancing an innovation-based framework for understanding cybercrime, Kraemer-Mbula et al., (2013) examined the evolution of cybercrime using insights from innovation, business, and ecological studies. Kraemer-Mbula et al. (2013) borrowed from the concept of a "digital business ecosystem" to assert that "financial cybercrime is an "interconnected" business, with different roles and interests of the constituents of this network" (p. 542). Apart from cybercriminals, other parties to the "cybercrime ecosystem" include lawful enterprises like IT security companies, banks, and financial services. As one group innovates to keep the system – e.g., the banking system – working by developing security tools and protocols, another group innovates to disrupt or circumvent these security measures (Kraemer-Mbula et al., 2013, p. 542). Other crucial components of the "cybercrime ecosystem" are the intent to commit and the actual commission of crimes.

From this perspective, the "cybercrime ecosystem" concept appears to reflect or be inspired by the analysis of agency-structure linkages in social action, which Giddens' structuration has exemplified. As presented in the recursive cybercrime influence cycle in Figure 3.1, parties to the "cybercrime ecosystem," such as IT security firms, constitute external structures to actors (individuals, businesses, and governments). These structures socialize actors' internal structures or dispositions and expose them to information regarding cyberspace's services, opportunities (positive and negative), safety for e-transactions, academic work, critical infrastructure, etc. Also embedded in actors' internal structures or dispositions are the intent to commit and the actual commission of crimes. Reflecting on their predispositions, actors

purposively (i.e., agency) use the internet for different activities which produce outcomes, intended (e.g., convenient banking and shopping) and unintended (e.g., cybercrime victimization) – the analytical last stage of the structuration cycle. Alternatively, some actors also purposively (i.e., employing agency) take advantage of the internet to commit cybercrimes by seizing on the opportunities to exploit vulnerabilities both among the technologies and the potential victims. Knowledge of the outcomes, especially the unintended ones (cybercrime victimization), filters back into the external structure through outlets such as customer complaints or self-reported victimizations and media reports. With this new information, the structuration cycle starts anew with the IT industry producing new security patches, anti-virus, and anti-malware tools and informing actors about their effectiveness. In this way (cycle), parties to the "cybercrime ecosystem," in the words of Kraemer-Mbula et al. (2013), "perversely, have a shared fate, as if participating in a game of innovation leapfrogging as one set of actors in the ecosystem attempts to counter the advances and responses of another set of actors" (p. 542).

The conceptualization of the evolution of the cybercrime industry as an "ecosystem" borrowing insights from a "digital business ecosystem" has revealed the mutual interdependence and interconnectedness of the different parties, external structures, agents (positive agency), and cybercriminals (negative or deviant agency), each with different roles and interests. Using structure properties in their interactions, active agents, including cybercriminals, transform or reproduce the same structure. Straddling these parties is the intent to commit and the actual commission of cybercrimes, thus an essential link in the "cybercrime ecosystem."

The structure and agency tensions and linkages in sociology have implications for social research, especially for this current work. As Beck (1992) implied on the risk society, there has been a significant shift in the broader social and technological environment in which people

found themselves as instrumental in late modernity. Such transformations have positioned individuality (i.e., actor agency) at the core of social action. Meanwhile, the transition out of a 'heavy' and 'solid' to a 'light' and 'liquid' society has ushered in constant flux and a dismantling of boundaries regarding the status-quo (Bauman, 2000, pp. 1-8). Thus, the flux and uncertainty in liquid modernity breed pervasive fear while creating opportunities to commit cybercrimes. Giddens (1984) theory moderates the apparent tensions by recognizing a dialectical interaction between structure and agency. To this end, rather than seeing structure and agency as two extremes or disparate phenomena (a dualism), Giddens (1984) argued they ought to be seen as representing a duality (p. 25), meaning active agents use social structure to either transform or recreate (reproduce) the same structure (Turner, 2014, p. 139). Consequently, one of the implications of the structure-agency discourse in the current work is the reasons for actors' use of the internet and CMCs based on structure-agency tensions and constraints on reporting cybercrime based on socio-demographic variables.

The current study adopts a middle-ground perspective, using insights from the discussions above, an integrated lens teasing out applicable principles, and concepts from different theoretical perspectives. While Beck (1992), Coleman (1990), and Bauman (2000) provide a useful overall framework or complex to understand the environment in which risk, fluidity, and individualism have emerged, Giddens's (1984) orientation complements it, and together they aid a better understanding of structure-agency linkages in internet use, victimization, and behavioral responses. Significantly, this study is established around the nexus of structure and agency and examines the paradox of internet use and victimization and consequent behavioral responses and motivations for use.

3.5 Integrated Theoretical Framework

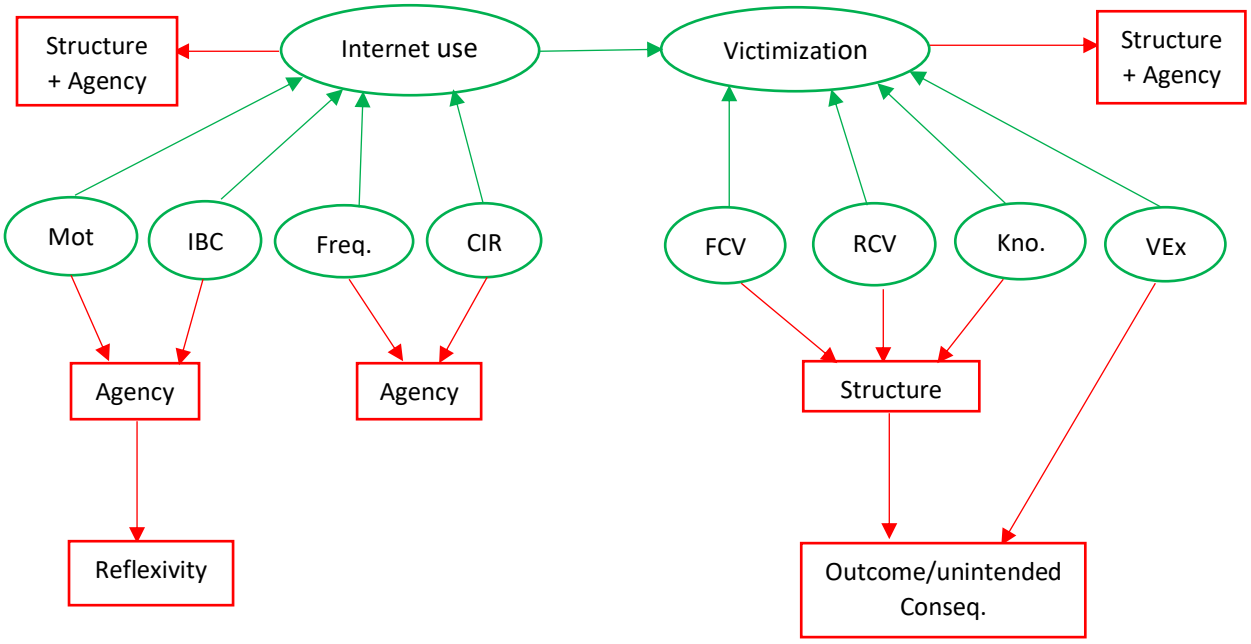
The theoretical framework, which is derived from a pre-existing theory(ies) within a disciplinary domain, serves as the 'blueprint' enabling research (Grant & Osanloo, 2014; Adom et al., 2018). The framework reflects the proposed hypotheses in an investigation. The framework also sets the direction of a study and grounds it on theoretical constructs (Adom et al., 2018). The theoretical framework's role in research has been compared to an analogy of a traveler's map or plan (Sinclair, 2007; Fulton & Krainovich-Miller, 2010). This way, the theoretical framework provides direction for the researcher.

The theoretical framework comprises critical aspects of a theory, such as the theoretical principles, constructs, concepts, and tenants (Grant & Osanloo, 2014). By incorporating distinct parts of a theory, the theoretical framework serves as the conducting unit, connecting and giving impetus to research. A graduate student must effectively select the theory or sets of theories that form the body of knowledge of the issue being studied in the context of their research (Adom et al., 2018). Accordingly, "the student is expected to make a unique application of the selected theory so as to apply the theoretical constructs to his/her dissertation study" (Adom et al., 2018, p. 438). A nuanced application of a theory or sets of theories in a research makes the scholarly contribution visible. Together with the conceptual framework, the theoretical framework seeks "to make research findings more meaningful, acceptable to the theoretical constructs in the research field and ensures generalizability" (Adom et al., 2018, p. 438).

The theoretical principle guiding this study is social action - structure-agency linkages and their related social or interactive nature - regarding internet use and cybercrime victimization and how it is influenced by and linked to structure, agency, reflexivity, and outcomes or unintended consequences. The theoretical principles and concepts are based in and teased out

from various theories reviewed previously in sections 3.1 to 3.4, including Beck's (1992) risk society theory, Coleman's (1990) rational choice theory, Giddens' (1984) structuration, and Stones' (2005) structuration brackets. The associated concepts relating to the theoretical principles are cybercrime incident reporting, motivation for internet usage, knowledge of victimization risk, internet usage frequency, and risk of cybercrime victimization. The remaining concepts include internet use behavior constraint, victimization experience, and fear of cybercrime victimization. As shown in Figure 3.2, the theoretical principle and associated concepts have been mapped to their respective empirical correlates.

Figure 3.2. Integrated Theoretical Framework



Source: Author's Construct, 2022.

Key:

CIR – Cybercrime Incident Reporting FCV – Fear of Cybercrime Victimization

Freq. – Frequency of Internet Use

IBC – Internet Behavior Constrain (Avoidance and Defensive)

Kno. – Knowledge of Cybercrime Risk Mot. – Motivation for Internet Use

RCV – Risk of Cybercrime Victimization VExp. – Cybercrime Victimization Experience

Figure 3.2 shows the integrated theoretical framework adopted for this study. The framework depicts the main theoretical concepts and their empirical correlates related to the

current study, shown in red rectangles and green oval shapes. The framework shows the paths of interactions between the correlates of structure, agency, reflexivity, and outcomes or unintended consequences. The framework further shows how the concepts connect to internet use and cybercrime victimization - empirical correlates of the theoretical principle of social action. The framework also demonstrates how each construct relates to the broader themes of internet use and cybercrime victimization.

3.5.1 Operational Descriptions of Theoretical Concepts and their Empirical Correlates

For this study, and to appropriately clarify the theoretical framework, I provide an operational description to elicit how the constructs relate to elements of the integrated theoretical framework and their application in the study.

1. Cybercrime Incident Reporting – Agency/Active Agency

Incident reporting involves actors (internet users) consciously deciding to inform the responsible agencies or platforms (for example, the Canadian Centre for Cyber Security, the National Cybercrime and Fraud Reporting System, and the police, among others) about their encounters with cybercrime incidents. Exercising the choice of reporting means internet users have an active role in the social action of reporting cybercrime incidents.

2. Motivation for Internet Use – Agency/Instrumental Rationality/Reflexivity

Internet users have various motives or factors informing their internet use actions. As rational actors, people use the internet to increase their utility; such utility is informed by their association with or interest in the internet and its related tools and products. In this way, internet users demonstrate their agency in an instrumental or purposive sense and reflexively, without simply acting as automatons.

3. Knowledge of Risk – Structure/Rules and Resources/External Structure

The external structure, which comprises cyberspace, or the internet platform, produces rules and resources about the operations of the IT world. These rules and resources socialize and facilitate internet users' acquisition of internet knowledge and perceptions or knowledge of risk and safety in cyberspace. Consequently, internet users' knowledge about cybercrime risk and perceptions of safety constitutes the structure.

4. Frequency of Internet Use – Agency

Frequency relates primarily to actor agency. In other words, it relates to the regularity with which internet users access the internet. Using the internet is an instance of an active agency; thus, internet use frequency measures the level of activity in cyberspace.

5. Risk of Cybercrime Victimization – Structure/Outcome/Unintended Consequences

Risk is built into cyberspace, and is a product of technological development, meaning risk is inherent in structure as cyberspace constitutes the internet's virtual structure. Also, risk is an outcome when people access the internet, which can also be experienced as an unintended consequence.

6. Internet Use Behavior Constraint (IBC) – Agency/Reflexivity

IBC typifies actors' behavior responses – avoidance and defensive – to risk, fear, and experience of cybercrime victimization. This way, people are active in the social action of internet use behavior and are reflexive because they reflect and calculate the consequences of their actions in cyberspace and how they can stay safe.

7. Victimization Experience – Structure + Agency/Outcome

Victimization consists of structure and agency because internet users demonstrate agency by accessing the internet, itself a component of a structure. By so doing, they stand the chance of becoming victimized. Additionally, victimization experience is an outcome or unintended consequence of people's internet use decisions.

8. Fear of Cybercrime Victimization – Structure/Outcome

Like risk, fear is built into the structure of the internet. Some internet users experience the fear of victimization when they use the internet. Such fear is wired into the fabric of the internet and is also experienced as an outcome or unintended consequence of action in cyberspace.

3.6 Summary and Conclusion

To summarize, in this chapter, I have reviewed relevant theoretical literature in socio-criminological research, focusing on their application to the problem in the current study. I reviewed Beck's (1992) theory of a risk society, which presents risk as an unintended consequence of rapid technological development. Cybercrime, a product of technological development, is a typical phenomenon in the risk society. The discussion revealed that Beck's theory implies a significant transformation in the broad social and technological environment wherein active agents (individuals) have been situated. Thus, individualism factors as a predominant feature in the risk society, making the theory methodologically individualistic. Whereas Beck's theory helps to understand the risks associated with the internet and the predictors of such risks, it is less helpful to understand the interconnections between motivation and awareness about risk associated with internet usage and its consequent victimization.

The chapter also reviewed the theory of rational choice by Coleman (1990) and revealed individualism to be at its core. As discussed, the empirical utility of Coleman's rational choice

model pertains to his emphasis on actors' connection to and interest in resources as patterning their interest maximization drives. Thus, actors' (individual internet users') association or connection to and interest in resources (the internet and its related tools and products) shapes their decisions or motivations about internet use. However, rational choice does not speak to the root of cybercrime – a by-product of technological development.

Bauman's (2006) liquid modernity is characterized by transformation, change, and the dismantling of boundaries, features consistent with the realities facilitated by the internet-dominated age. Change, far from being temporary to a stable end, is a constant feature and, thus, creates endemic uncertainty. The risk of cybercrime is understood as a correlate of endemic uncertainty resulting from action (agency) in the liquid (computer) era. However, Bauman's theory does not account for actors' internet use motivations and their behavioral responses to the constant flux and uncertainty (fear and risk of cybercrime).

I also presented the structure and agency debate in Sociology and situated the current study within it. The discussion and analysis isolated the three distinct strands of the debate. There were methodologically individualist structure and agency and the more robust structure-agency perspectives. Whereas the structure perspective emphasizes the saliency of structure in determining individual action, the agency perspective arrogates causation primarily to agency. Although each strand is important and offers insights into action and society, the more robust sociological perspective, structuration theory, arose as an attempt to moderate the debate. This conclusion was reached by utilizing the various strands of the debate to explain the problem of cybercrime in society. Giddens' (1984) perspective of the structure-agency debate (structuration theory) affords equal importance to structure and agency. However, it has come under fire for confusing structure and agency and neglecting to offer recommendations for empirical study.

Although Stones (2005) reworked Giddens' original formulation in response to various criticisms of structuration theory, the structure-agency debate has not abated.

Finally, after reviewing the relevant theories and examining their application to the problem in the current study (including both their strengths and weaknesses), I adopted an integrated theoretical framework as the best approach to guide my analysis and understand my research problem. The framework adapts relevant principles and concepts from the theories reviewed in sections 3.1 to 3.4: Beck's risk society theory, Coleman's rational choice theory, Giddens' structuration, and Stones' structuration brackets.

Chapter Four: Methodology

4.0 Overview

This research focuses on understanding the apparent paradox observed in internet use, the risk of cybercrime victimization, and the resultant behavioral responses, including the implications regarding avoidance and defensive internet use. Additionally, the study also aims to explain the factors that motivate Canadians' use of the internet. This chapter describes my research methodology. First, I present the research questions and hypotheses underlying this research. Next, I discuss the research design and follow up with a note about respondents and the sample selection. I then follow this with a discussion about pre-testing the survey instrument and details about the study variables and their operational definitions. Next, I discuss data collection. The conceptual and analytical frameworks are then presented, along with details about the analytical models and strategy, in the section that follows. I conclude with ethical considerations and a brief discussion on reflexivity and the motivation for the research.

4.1 Research Questions and Hypotheses

This study sought to understand why, notwithstanding the fear and persistent or inherent risk of victimization in cyberspace, do Canadians continue to use the internet? In other words, has the perception of cybercrime victimization changed how people use the internet? This overarching question is the base of this study. As such, all the accompanying variables and other components are to be understood with this overarching question.

This study examined a series of specific research questions to answer the main research question:

1. What association do socio-demographic characteristics have with the risk of cybercrime victimization?
2. What is the relationship between prior cybercrime victimization experience and the fear of future cybercrime victimization?
3. What is the association between cybercrime victimization experience and the perceived risk of cybercrime?
4. In what ways do victimization experiences constrain internet use behavior?
5. In what ways does cybercrime incident reporting affect fear of cybercrimes?
6. How does internet use frequency constrain internet use behavior?
7. What are the motivations for internet use among Canadian adults?

Consequently, to respond to the underlying research questions associated with the research, the following hypotheses were developed and tested:

1. Socio-demographic factors are associated with the risk of cybercrime victimization.
2. Prior victims of cybercrime are expected to be more fearful of cybercrime than persons without victimization experience.
3. Prior victims of cybercrime are expected to perceive more risk of cybercrime than persons without victimization experience.
4. Cybercrime victims are more prone to exhibit internet behavior constraints:
    a. Cybercrime victims are more prone to resort to avoidance internet behaviors than non-victims of cybercrime.
    b. Cybercrime victims are more prone to adopt defensive internet behaviors than non-victims of cybercrime.
5. Cybercrime incident reporting is associated with the fear of cybercrime.

6. Frequent users of the internet are more inclined to exhibit internet behavior constraints:
    a. Frequent internet users are more inclined to engage in avoidance internet behaviors than less frequent users.
    b. Frequent internet users are more inclined to adopt defensive internet behaviors than less frequent users.

4.2 Research Design

This study combined quantitative and qualitative analyses using a quasi-mixed method study design. The study is exploratory, and quantitative and qualitative data were collected in a single survey.

4.2.1 Mixed Method Research

Mixed methods research design has a long history in Sociology. It is referred to in earlier sociological literature as a multi-method research design (please see the works of Lipset et al., 1956; Becker et al., 1961)**.** Mixed methods research comprises the third strand of research designs in sociology (Creswell, 2003; Morgan, 2007; Pearce, 2007). The first two are the qualitative and quantitative streams, which relate to the metaphysical and positivist paradigms (Morgan, 2007; Pearce, 2012). According to the metaphysical paradigm, efforts at objective measurement are pointless because there is no absolute truth, whereas the positivist paradigm asserts that reality is objective and can be measured (Pearce, 2007, p. 832). Conversely, the pragmatic paradigm recognizes the existence of a single "real world" and that each human has unique perceptions of it (Pearce, 2007, p. 833).

The pragmatic approach (the third strand) hints at a role for structure and agency wherein structure resonates with the view of a 'world' out there. Meanwhile, agency aligns with humans'

role in framing or conceiving that 'world.' From this stance, there is alignment of the pragmatic (mixed method) approach with the theoretical posture of this study. In the view of Morgan (2007), the mixed methods stream arose as a response to the paradigm wars, which saw researchers fight for supremacy between qualitative and quantitative designs. In other words, mixed methods approach represents the triad, and it came to the fore to mediate the tensions between the dyad of quantitative and qualitative research designs. Recent examples of mixed-method research design in Sociology include a research on gender, migration, and HIV risks (Parrado, McQuiston, & Flippen, 2005) and the Three-City study (Cherlin, Burton, Hurt, & Purvin, 2004). Also, see Adams & Trinitapoli (2009), Andrews (2001), Perry (2009), and Trinitapoli (2007) for other contemporary sociological works that have used mixed methods.

The mixed-method design is built around pragmatic epistemology, a framework that acknowledges and combines aspects of quantitative and qualitative methods (Pearce, 2012). As the name suggests, pragmatism conveys ideas of practicality or expedience and is concerned with finding the balance between the ideal and the real and between knowledge and action (Kelly & Cordeiro, 2020). It is not practical to expect feasible outcomes for research questions with qualitative dimensions by using solely closed-ended survey instruments and quantitative analysis. In this way, Bourdieu's (2004) call to methodological polytheism (p. 101) is useful. By methodological polytheism, a researcher is encouraged to see each method's strengths and choose among the best method(s) to answer the research question(s).

A mixed-method design aligns with the perspective of this study. The current study operates from the understanding that a rigid inclination to either structure or agency is not overly helpful for understanding and explaining social action and instead this study employs a hybrid framework that acknowledges and uses elements of both quantitative and qualitative approaches.

This design choice resonates with Morgan's (2007) argument that strict adherence to the dichotomous strands of qualitative and quantitative is overly rigid, while Lierberson (1992) terms it "a Durkheimian conflict" (p. 2). The dichotomous discourse impacts the quality of social research as adherents of each strand attempt to discredit the study of the other to elevate the relevance of their favored approach (Morgan, 2007).

As argued in this study, social action within the context of internet use, and the consequences of acting, such as risk and actual victimizations, represent a synchronous interplay between the forces of structure and agency. Hence, pluralism or multiplicity is preferred rather than strict adherence to an either-or discourse. In other words, this study follows the methodological polytheism that has been encouraged by Bourdieu (2004). Following this study's theoretical posture, flexibility in choosing research designs and combining the appropriate number thereof is a component of this study. In line with the mixed method design and to effectively incorporate the qualitative analysis, I employed what may be called *qualizing* instead of *quantizing*. In other words, in this study, some quantitative data collected through an online survey is transformed into qualitative data to analyze some of the underlying motivations for internet users to patronize the internet.

As a middle-ground design, mixed methods research enjoys some advantages over either strictly quantitative or qualitative approaches. The mixed-method approach calls for what Morgan (2007) terms 'abduction' (p. 71) involving a constant dialectic between the inductive (qualitative) and deductive (quantitative) process of theory development. This approach is more practical because research rarely follows a pure path without veering into aspects of another approach (Axinn & Pearce, 2006; Hanson, 2008). Also, unlike the metaphysical (qualitative) or positivist (quantitative) paradigms, the pragmatic approach explicitly accepts that absolute

subjectivity or objectivity is impossible to achieve (Pearce, 2012, p. 833). In the mixed method literature, this recognition is termed intersubjectivity (Morgan, 2007) and describes researchers' work that strives for objectivity while allowing for a subjective dimension (Hanson, 2008; Morgan, 2007). In other words, intersubjectivity, as used here, conveys a similar implication to Morgan's concept of abduction. The notions of intersubjectivity and 'abduction' resonate with reflexivity, a term central to the works of Bourdieu (2004), Giddens (1984), and Beck (1992). Reflexive sociology realizes how researchers' behaviors, understandings, and interpretations influence the people and environments they are researching and their discoveries (Thomas, 1923, as cited in Pearce, 2012, p. 833).

Additionally, in response to criticism that findings from the qualitative method cannot be generalized as opposed to the supposed generalizability of positivism, the pragmatic paradigm acknowledges that all data types can be "transferable" (Pearce, 2012, p. 833). Empirically speaking, each research needs to be evaluated for its unique merit (Small, 2009). By arguing this way, mixed methods design operates with the tacit acknowledgment that aspect(s) of each study can have some form of application in a different context rather than offering the prospect of a wholesale application (as espoused in the quantitative paradigm).

4.3 Respondents

In collaboration with the Canadian Hub for Applied and Social Research (CHASR) and Ekos (a Canadian professional research vendor who supplies samples and interfaces with participants), a national (Canadian) sample was recruited meeting the sampling criteria – Canadian residents, 18 years and above, and users of the internet. Ekos recruited the sample by curating a subset of eligible participants from their existing panel. Ekos recruits' participants

through random digit dialing, where respondents who answer their phones are invited to opt into Ekos' participant pool. Ekos used a random selection method to procure a representative sample of Canadian respondents from this process. It was from this pool that Ekos sent targeted emails based on the participants' demographics.

4.4 Sample Selection

The study's population universe is the population of all internet-using Canadian residents. Because of the impossibility of reaching out to all the members of this given population, a nationally representative sample of internet using Canadian residents was used for the research. A decision was made to utilize Ekos' sample pool for convenience and expedience. Notably, the sample is highly generalizable because of the rigorous probability-based sampling methods used to constitute the sample pool.

4.5 Pre-testing

Before rolling out the full launch of the survey, it was piloted first through a soft launch to a limited number of test respondents (n=6). The reasons for the soft launch, among others, was to ensure that the questions measured what they were intended for, i.e., validity and that the questions and responses were consistent. The test respondents included both Anglophone and Francophone respondents, representing the linguistic demographic divide of Canada.

4.6 Variables and Operational Definitions

4.6.1 Dependent Variables

The study has four sets of dependent variables:

1. Fear of Cybercrime – This variable was measured at the scale level by asking respondents to indicate how fearful they felt about becoming a victim of cybercrime during the past month. Respondents indicated their level by choosing from a five-point Likert scale ranging from not at all fearful to extremely fearful (please see survey questionnaire in Appendix A). In other words, fear of cybercrime was measured on a continuum, from not at all to extremely fearful.
2. Risk of Cybercrime – This variable assessed respondents' perceived risk of cybercrime victimization. The variable was measured at the scale level and compared violent crimes with cybercrime. Respondents were asked whether they agree they feel more at risk of cybercrimes than violent crimes. Respondents indicated their level of agreement by choosing from a five-point scale ranging from strongly agree to strongly disagree (please see survey questionnaire in Appendix A). In other words, respondents perceived risk of cybercrime was measured on a continuum, from strongly agree to strongly disagree.
3. Avoidance Behavior – This is a behavioral response (impact on behavior) and measured the internet activities that respondents have refrained from to stay safe online. Avoidance behavior was measured for concern about online/internet transactions, fear of cybercrime, cybercrime experience, and internet use frequency. Following Rader et al. (2007), avoidance behavior was measured in each situation by asking respondents two questions. Using a 5-point Likert scale, from "not at all" to "extremely," respondents were asked to indicate the extent to which concern about internet transactions, fear of cybercrime, victimization experience, and internet use frequency has prevented them from doing things they would like to do on the internet. Respondents who chose anything between "a little" to "extremely" (which means that concern about internet transactions, fear of

cybercrime, victimization experience, and internet use frequency has had some impact on their internet activities) were asked a follow-up question about the activities that they have refrained from doing (please see survey questionnaire in Appendix A).

A binary index variable for Avoidance Behavior was created first using an average item score of 1 across questions 8, 15, 25, and 33 (that is, questions relating to Avoidance Internet behavior – please see survey questionnaire in Appendix A for questions and their corresponding numbers). Next, the average score was dichotomized into 1 and 2, where 1 identified anybody not using avoidance internet behavior and 2 for persons who used avoidance internet behavior.

4. Defensive Behavior – Like avoidance behavior, defensive behavior is also a behavioral response and measured whether respondents engaged in precautionary or protective actions when using the internet because of cybercrime. Like avoidance behavior, defensive behavior was measured for concern about online/internet transactions, fear of cybercrime, cybercrime experience, and internet use frequency. Following Rader et al. (2007), defensive behavior was measured in each situation by asking respondents two questions. Using a 5-point Likert scale, from "not at all" to "extremely," respondents were asked to indicate the extent to which concern about internet transactions, fear of cybercrime, victimization experience, and internet use frequency has caused them to take specific actions when using the internet to minimize their risk of cybercrime.

   Respondents who chose anything between "a little" to "extremely" (which means that concern about internet transactions, fear of cybercrime, victimization experience, and internet use frequency has caused them to take some actions) were asked a follow-up question to indicate some of the steps that they have incorporated to minimize their risk

of cybercrime victimization when using the internet (please see survey questionnaire in Appendix A).

The internet constrains behavior variables – avoidance and defensive behaviors - measured changes in internet use among internet users (respondents).

An index defensive behavior variable was computed using an average item score of 1 across questions 10, 17, 27, and 32 (that is, questions relating to defensive behavior - please see survey questionnaire in Appendix A for questions and their corresponding numbers). However, Q27 attracted a large number of missing responses, with about ¾ of the sample skipping Q27. As a result, in computing the average item variable for the four questions, Q27 was omitted for persons who did not answer it, giving an average of 1 to 5. Next, the average was re-dichotomized to identify respondents with a mean item score < = 1.75 as individuals not using defensive internet behavior. This now gives 89/403 reporting a relative absence of defensive internet behavior.

4.6.2 Independent Variables

Like the dependent variables, this study has several independent variables, all linked to the research questions. The variables included the following:

1. Socio-demographic (control variables) - These variables included gender, age, education, ethnicity, marital status, family income, and occupation.
2. Cybercrime Victimization Experience – This variable was measured at the nominal level by asking respondents to indicate whether they had experienced any sort of cybercrime in the previous year. Respondents who experienced cybercrime chose “Yes,” whereas those without experience chose “No.” Respondents who were unsure whether they had any

experience chose “Not sure.” Respondents who answered either “No” or “Not sure” were asked no further questions about victimization and reporting.

3. Cybercrime Incident Reporting – This variable examined respondents’ reporting of their cybercrime experiences to the police. Respondents were asked to indicate whether they reported their cybercrime experience to the police. The question was asked only to respondents who had experienced cybercrime in the past 12 months. Responses included “Yes,” “Sometimes,” and “Not at all” categories. The “Sometimes” response option related to respondents who reported some but not all their experiences of cybercrime.
4. Knowledge of Cybercrime Risk – This variable assessed respondents’ perceived knowledge about the risk of cybercrime. The variable was measured at the scale level with two questions. The first question assessed respondents’ perceived knowledge about cybercrime risk by asking respondents to rate their current knowledge about cybercrime risk. Respondents chose from options including “Excellent,” “Good,” “Fair,” “Poor,” and “Very Poor.” The second question assessed the perceived prevalence of cybercrime risk by asking respondents to indicate their views about the level of cybercrime risk. Respondents chose “Increasing” if they thought cybercrime is becoming more prevalent and “Decreasing” if they felt it is becoming less pronounced. Respondents who thought cybercrime prevalence has remained unchanged chose “Stable,” while those who have no idea about cybercrime prevalence chose “Do not know.”
5. Frequency of Internet Use – This variable measured respondents' level of interaction with the internet. Respondents were asked to indicate their level of internet use. Respondents had the option to choose between “Once daily," "Several times in a day," "Weekly," and "Monthly" to reflect the intensity or level of interaction with the internet.

6. Motivation for Internet Use - This variable assessed respondents' reason(s) for using technology, in this case, the internet. Respondents were prompted to indicate their reason for using the internet with an open-ended question. The open-ended question was used to reveal respondents' views rather than restrict them to choosing from a list of preconceived ideas about motivations. Responses to the question were analyzed in thematic analyses to tease out the predominant underlying justifications for internet use. The responses were subsequently grouped according to the overarching common or recurring themes of motivation as they related to respondents' motivation sources.

4.7 Data Collection

This mixed-method study used a survey to collect data. A survey questionnaire was deployed through an online survey methodology to collect quantitative and qualitative data from respondents across Canada. The questionnaire incorporated closed-ended questions for the quantitative component and open-ended semi-structured questions for the qualitative component. The themes for the data collection were adapted from a review of the relevant literature and previous crime surveys, such as the Saskatchewan crime survey instrument (Centre for Forensic Behavioral Science and Justice Studies [CFBSJS], 2014) and the Special Eurobarometer Cyber Security survey (TNS Opinion & Social, 2015). Subsequent modifications were made to incorporate some relevant themes absent from the existing surveys. Adapting questions and scales from existing surveys and rolling out a pilot soft launch survey was significant to ensuring the validity of the survey tool and the reliability of the collected data. The survey was administered online using Voxco Online by collaborating with the CHASR at the University of Saskatchewan. The survey approach was used because of the exploratory nature of the study and the fact a survey method is a valuable tool for acquiring exploratory data (Yang et al., 2010).

The survey was administered online to a randomly selected sample of Canadian adults who are part of a panel built through random digit dialing. The survey was programmed and administered by the CHASR at the University of Saskatchewan. The CHASR programmed the survey using an online survey software or programming platform called Voxco Online. The CHASR holds a Voxco site license for research purposes. Voxco is a Canadian-owned business and their servers are situated in Canada; this is a key strength because it means the data are hosted and retained in Canada. In the age of privacy, Voxco Online's Canadian servers have implications for data security. Notably, respondents were informed about the location of Voxco Online and where their data would be retained in the consent documents. Following the design and programming of the survey in Voxco, data collection was facilitated by Ekos, a professional research vendor who supplies samples and interfaces with participants.

4.8 Conceptual Framework

As stated by Camp (cited in Adom et al., 2018), "the conceptual framework is a structure which the researcher believes can best explain the natural progression of the phenomenon to be studied" (p. 439). The framework highlights how the researcher will examine the research problem and presents an integrated lens of seeing the problem under study (Adom et al., 2018; Liehr & Smith, 1999). Aside from outlining the research direction, the framework also establishes the research in theoretical constructs (Adom et al., 2018).

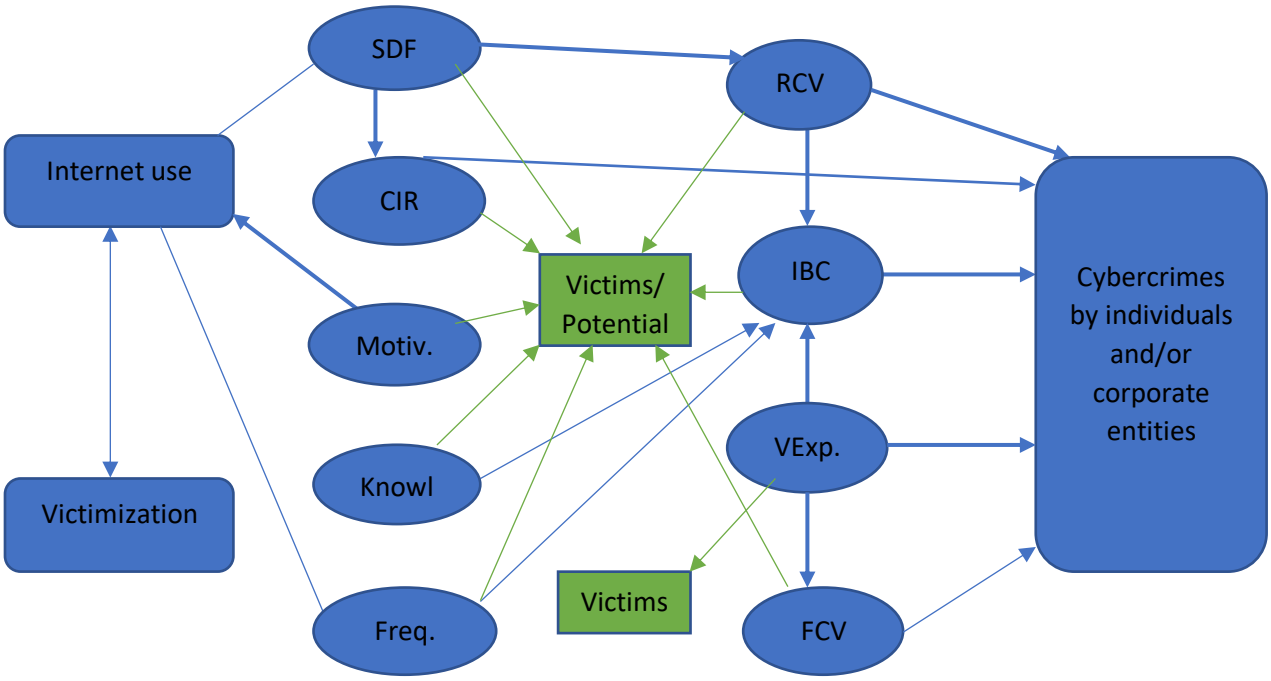
The primary variables in the research are logically described by the conceptual framework in terms of their interactions. Such a logical description of the relationships provides a mental map of the association between a study's constructs. Adom et al. (2018) suggested that the overarching goal of the conceptual and theoretical frameworks is to "make research findings

more meaningful, acceptable to the theoretical constructs in the research field and ensures generalizability" (p. 438). In Imenda's (2014) view, both the theoretical and conceptual frameworks provide the lifeblood of a research study. As a result, readers find it challenging to assess the scholarly viewpoint and the factors supporting the researcher's claims while reading a research work that lacks a theoretical or conceptual background. (Adom et al., 2018, p. 438).

Scholars are generally unanimous about the conceptual framework's centrality in research. The framework's importance is unmistakable and offers advantages to the researcher and research process. The conceptual framework allows the researcher to define and explore their perspective of the problem to be studied (Grant & Osanloo, 2014). Akintoye (2015) made the controversial claim that the conceptual framework is mostly used when current theories fail to establish a reliable foundation for the analysis. Nonetheless, the conceptual framework plays a vital role by providing the researcher with a mental map of the relationships between constructs in the study.

Figure 4.1 represents this study's conceptual framework, which is derived from the literature on cyber-victimology and internet use themes. The main variables culled from the literature include fear of crime, victimization risk, constrained behavior, victimization experience, crime reporting, motivation for internet use, and the socio-demographic factors related to crime and victimization. Conceptual frameworks can be presented in a graphic or narration manner, showcasing the main variables or concepts to be researched and their presumptive links, according to Mills and Huberman (1994, p. 18). Following Mills and Huberman (1994), the current study's conceptual framework has been presented in a graphical form in Figure 4.1 and followed by a brief narrative.

Figure 4.1. Conceptual Framework



Source: Author's Construct, 2022.

Key:

SDF – Socio-demographic factors RCV – Risk of Cybercrime Victimization

CIR – Cybercrime Incident Reporting

IBC – Internet Behavior Constrain (Avoidance and Defensive)

Motiv. – Motivation for Internet Use VExp. – Cybercrime Victimization Experience

Knowl. – Knowledge of Cybercrime Risk FCV – Fear of Cybercrime Victimization

Freq. – Frequency of Internet Use

Figure 4.1 represents the Conceptual Model for the study. The model is a path diagram showing the patterns of hypothesized associations between the variables. The Conceptual Model includes ten constructs indicated in blue oval shapes: fear of cybercrime victimization, risk of

cybercrime, avoidance behavior, defensive behavior, socio-demographic factors, cybercrime victimization experience, cybercrime incident reporting, knowledge of cybercrime risk, frequency of internet use, and motivation for internet use. The two green rectangle shapes in the model's center indicate the participants targeted for the study. The two blue rectangles at the extreme left indicate the study's primary or bedrock themes: internet use and its unintended consequences as manifested in cybercrime victimization. Meanwhile, the elongated blue rectangle at the extreme right illustrates the definition or source of victimization – one originating either from individuals or corporate entities.

The blue solid line arrows reflect the paths of hypothesized relationships between the constructs. Conversely, the solid green arrows indicate the category of the internet user (study participant) to which each construct relates. In other words, the solid green arrows demonstrate whether a construct relates to one of a victim of cybercrime, a potential victim, or both. Together, the interplay between the constructs of structure and agency as depicted in the model reflects Canadian internet users' interaction with the internet, the unintended/consequences of so acting, and whether such acting has affected their internet use behaviors.

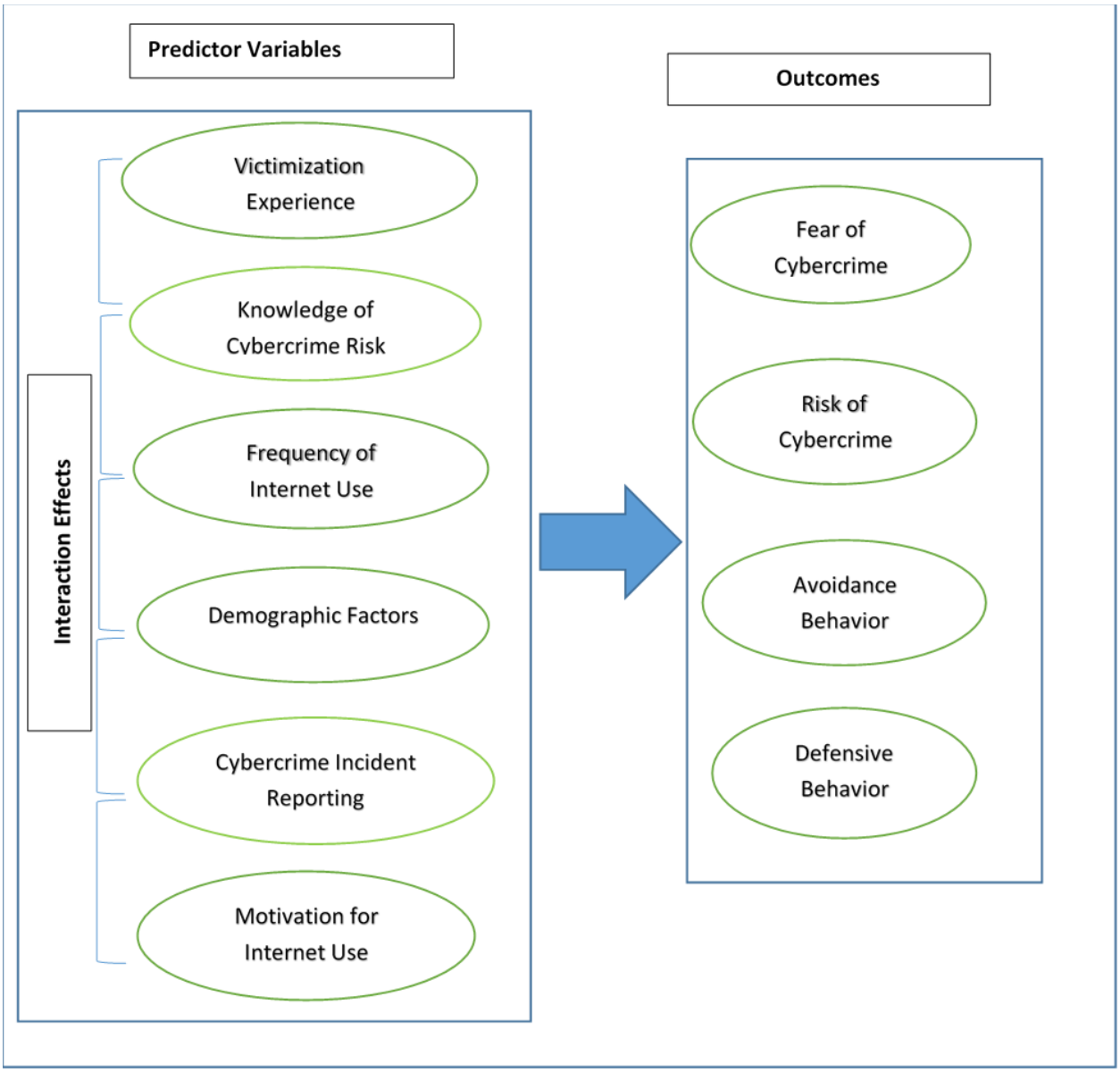
4.9 Analytical Framework

This section presents the analytical frames used in this study. The section comprises two main sub-sections: analytical models and analytical strategy.

4.9.1 Analytical Models

Figures 4.2 and 4.3 represent the analytical models utilized in this study.

Figure 4.2. Analytical model 1 - Relationship between Predictor and Outcome Variables and Interaction Effects

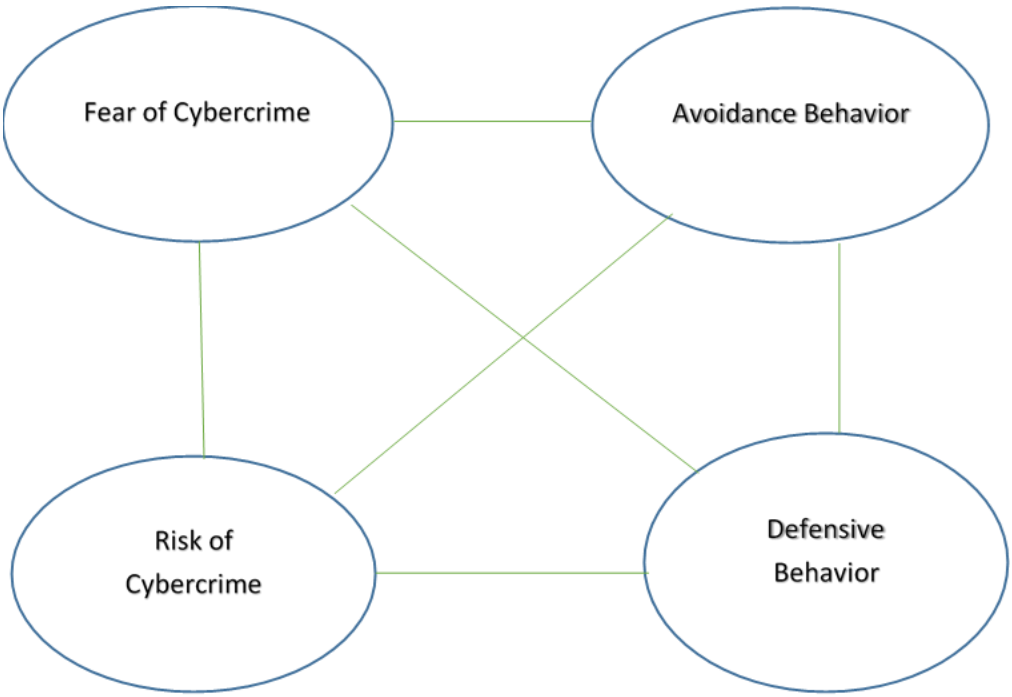


Source: Author's Construct, 2022.

Figure 4.2 represents the analytical model depicting the association between the predictor variables and outcomes. The model also shows a hypothesized interaction among the predictor

variables in the sense of how the independent variables interact among themselves to influence the outcome variables.

Figure 4.3. Analytical Model 2 – Correlation Matrix among Outcome variables



Source: Author's Construct, 2022.

Figure 4.3 represents the model (correlation matrix) showing the hypothesized relationship among the dependent variables – fear of cybercrime, risk of cybercrime, avoidance, and defensive internet use behaviors.

4.9.2 Analytical Strategy

This section comprises three sub-sections: descriptive analysis, statistical modeling analysis, and thematic analysis. The descriptive and statistical modeling analyses have been

carried out utilizing the Statistical Package for the Social Sciences (SPSS). The statistical analysis methods used are logistic regression.

4.9.2.1 Descriptive Analysis

Data is presented in frequency distribution tables to reveal respondents' socio-demographic identification based on age, gender, education, ethnicity, marital status, family income, and employment. Next, bivariate analysis (cross-tabulations) shows the relationship (distribution) in frequency and percentage between each outcome variable and all the predictor variables. In other words, bivariate analysis is conducted between cybercrime fear, cybercrime risk, avoidance behavior, and defensive behavior and all the predictor variables.

4.9.2.2 Statistical Modeling Analysis

This study used a stepwise modeling framework to develop models for all the outcome variables. This study's modeling framework is inspired by Hosmer et al. (2013) on the purposeful selection of variables for model building (pp. 89-94). The rationale for the planned selection of model covariates was to achieve model parsimony, that is, to arrive at a best-fitting model with as few variables as possible. Also, the resulting model is more numerically stable and is easier to use (Hosmer et al., 2013, p. 90).

The first step involved univariable analysis between the outcome and the predictor variables. Accordingly, for the first model, a univariable analysis was conducted between cybercrime victimization fear and socio-demographic factors, cybercrime fear and cybercrime victimization experience, and cybercrime victimization fear and incident reporting. A similar analysis was conducted for fear of cybercrime victimization and knowledge of cybercrime risk (perceived risk) and between the fear of cybercrime victimization and internet use frequency. The same analysis was repeated for the second, third, and fourth models between the risk of

cybercrime victimization, avoidance internet use behavior, and defensive internet use behavior and the predictor variables.

According to Hosmer et al. (2013), the univariable analysis identifies variable candidates for a first multivariable model. And following the works of Bendel and Afifi (1977) and Mickey and Greenland (1989) on linear and logistic regression, the threshold for acceptance at this step is that a variable's univariable test needs to have a p-value of less than 0.25 ($p<0.25$). As a result, all variables with the acceptable univariable test statistic ($p<0.25$) are noted from the first step. Additionally, it is suggested that a researcher may also include variables of known clinical importance or intuitively relevant variables (Hosmer et al., 2013, p. 91). Following Hosmer, Lemeshow and Sturdivant's suggestion, gender, with p-values of 0.72, 0.29, 0.87, and 0.97, have been added as a theoretically relevant variable for fear, risk, avoidance, and defensive internet behavior models (see Tables 5.7, 5.8, 5.9, and 5.10).

The second step was to "fit the multivariable model containing covariates identified for inclusion at step 1" (Hosmer et al., 2013, p. 91). This step involved conducting a first multivariable analysis for each model between the outcome and predictor variables, using only variables with the acceptable p-value from the first step (i.e., $p<0.25$). Also, variables deemed theoretically important may still be added, even though their p-value may not be less than 0.25, as per Hosmer et al. (2013). Accordingly, for the first multivariable model, multivariable analysis was conducted between fear of cybercrime victimization and all the predictor variables simultaneously. The second, third and fourth models also involved multivariable analysis between the risk of victimization, avoidance internet use behavior, and defensive internet use behavior and all the predictor variables simultaneously.

The third step involved examining the covariates from the second step to identify their importance. Variables whose p-value is not less than 0.05 (traditional significance level) are eliminated from the model, leaving only variables with a p-value <0.05 to constitute a new and smaller model (Hosmer et al., 2013, p. 91). Theoretically, important variables may still be selected and added to the new model, even though they may not meet the traditional significance level. The resulting new model is the preliminary main effects model.

The fourth step was re-introducing the non-significant variables identified at the univariable analysis stage, one at a time, into the main effects model. The resultant model from here becomes the final main effects model. At this stage, the model was now locked.

The final step involved testing for potential interaction effects among the variables at the final main effects stage. To do this, a set of potential variable combinations in the model that have a reasonable chance of interacting was created (Hosmer et al., 2013, p. 92).

Meanwhile, none of the hypotheses related-predictor variables for modeling avoidance internet behavior qualified for multivariable analysis in the study. As a result, the multivariable relationship between these predictors and avoidance internet use behavior could not be tested. Therefore, a final multivariable model for the avoidance of internet use behavior was run, including only the strongest (p-value<0.25) univariable predictors as a shorter model to test the remaining hypotheses.

4.9.2.3 Thematic Analysis

Thematic analysis is a qualitative approach to data analysis. While thematic analysis is viewed as a foundational method (Braun and Clarke, 2006), others see it as a basic skill within qualitative analysis (Holloway & Todres, 2003). Thematic analysis entails exploring a data set for recurring

patterns of meaning (Braun & Clarke, 2006, p. 11). The data set can include a series of interviews, focus groups, or a collection of texts. Thematic analysis is highly flexible: it can be used in a variety of theoretical and methodological frameworks (Braun & Clarke, 2006; King, 2004; Nowell et al., 2017). Braun and Clarke (2006) argue that thematic analysis is useful for a variety of "theoretical and epistemological approaches" and is "independent of theory and epistemology" (p. 78).

As indicated earlier, flexibility exemplifies thematic analysis. This study's thematic analysis was driven by the research question about motivation for internet use among internet-using Canadians. As a result, the decision about the salience or 'keyness' of the themes extracted from participants did not relate to the frequency of ideas underlying each theme. Instead, the question was to what extent a theme related to the research question under investigation. Braun and Clarke (2006) suggested that prevalence "in terms of space within each data item and of prevalence across the entire data set" (p. 82) is essential in coding themes. However, this study aligns with the view that there is no absolute rule for determining codes, a point also acknowledged by Braun and Clarke (2006).

The current research utilized a deductive, top-down, theoretical approach to coding themes. Unlike the inductive analytic approach, deductive theoretical analysis is informed "by the researcher's theoretical or analytic interest in the area, and is thus more explicitly analyst-driven" (Braun & Clarke, 2006, p. 84). Additionally, because coding is informed by a specific stated question in the research, as opposed to one resulting from the coding process (Braun & Clarke, 2006), the deductive focus of the analysis becomes apparent.

This study also employed thematic analysis at the semantic level instead of the latent level (Braun & Clarke, 2006; Boyatzis, 1998). Accordingly, in this study, "themes are identified

within the explicit or surface meanings of the data," as reported by participants (Braun & Clarke, 2006, p. 84). Therefore, I do not seek to explore participants' responses to uncover underlying ideas and assumptions beyond what is recorded in the data set. Beyond revealing the patterns in semantic or observed content, the analysis goes a step further to examine the significance and implications of the themes as they relate to the broader literature on motivations for internet use.

The thematic analysis in this study was done from the realist/essentialist epistemological framework. What can be said about research findings and how meaning is theorised are both governed by epistemology (Braun & Clarke, 2006). A realist analysis examines individual or micro-levels of reality. As a result, it "can theorize motivations, experience, and meaning in a straightforward way" (Braun & Clarke, 2006, p. 85). According to Braun and Clarke (2006), meaning, experience, and language are thought to have a largely unidirectional relationships; wherein "language reflects and enables us to articulate meaning and experience" (p. 85). As a result, participants' motivations for using the internet are seen to rest at the micro-level, reflecting mainly individual psychologies instead of being influenced by sociocultural forces and contexts. So, by operating from a realist/essentialist epistemological standpoint, exploring thematic analysis from the semantic level, this analysis does not seek to attribute underlying factors, assumptions, or social-structural factors to participants' internet use motivations.

By following the realist/essentialist thematic analysis from the semantic level, this study churned the following themes as reflecting participants' motivations for internet use:

1. Education and knowledge acquisition
2. Entertainment and having fun
3. Communication and social media access
4. Using the internet for commercial purposes

5. Work and personal-related use
6. News and information access
7. Other uses of the internet

Each of the above themes reflects an overarching idea about participants' internet use motivations. Each theme is derived from participants' responses without imputing underlying ideas and assumptions about their specific responses. Additionally, each theme emanated from the micro-level of reality and thus reflects micro-level understandings of participants' motivations for using the internet.

4.10 Ethical Considerations

As part of the project and before the actual data collection, this research was approved on May 29, 2020, by the Behavioural Research Ethics Board of the University of Saskatchewan, with two further extensions approved on May 24, 2021, and May 24, 2022 (see Appendix D for original approval certificate). Arrangements were put in place to relay any other incidental or unforeseen ethical dilemma to the advisory committee and to be resolved per the advice of the Research Ethics Board. Research participants were informed about the ethical obligations of the researchers (principal investigator and student) in relation to the application of data and the measures to preserve confidentiality and anonymity. An information page preceded the survey, which contained a brief description of the research and respondents' consent statements. After giving their consent to participate by clicking the proceed button, survey respondents could withdraw at any point during the survey.

Meanwhile, the study data is stored securely by CHASR at the University of Saskatchewan and the student researcher. CHASR will store the data on a secure University of

Saskatchewan shared drive. The IT department manages the servers and the shared drive is backed up daily. As the researcher, I have stored the study data on my student OneDrive account, a secure file storage and sharing service provided by the University of Saskatchewan to all students. The data will be kept for at least five years per the University of Saskatchewan guidelines before it is safely destroyed.

The outcomes of this study will be primarily used in a dissertation for the Ph.D. degree (as used here). Results will also be published in scholarly and peer-reviewed journals and shared in academic conference presentations.

4.11 Reflexivity

The same reflexivity that informed my previous study (see Abdulai, 2016) continued to motivate the current research. This study was influenced by my individual experiences, academic interests, and practical dilemmas. My origins as a student from the global South was essential to the research focus. I consider myself privileged to have experienced international travel and to have interacted with young people from both the global North and South. Through such experiences, I was able to see the relative possibilities and difficulties that young people from many cultures face. As a "third world" student from a modest family, I saw many of my peers and even a lot younger people turn to various paths in life when faced with the same obstacles that I did. These young people have regularly described the educational journey I and others like me have travelled as being lengthy and mostly fruitless. The young people are quick to point out a number of outstanding graduates who are stumbling around the streets looking for work. Alas, some of these young people waste hours at internet cafés engaging in different types of online

fraud. This brief background has greatly influenced my choice to investigate this particular research program.

As a result, this research is an extension of my MA thesis research which examined the predictors of the fear of cybercriminal victimization (credit or debit card theft). The intention was to explore the complex constructs of actors' fear and perceived risk of general cybercrime victimization, their knowledge about cybercrime prevalence, their continuous patterns of internet use, and their motivations for using the internet. The complex relationship and interrelationships between these constructs present a fascinating socio-criminological conundrum. My objective is to theoretically contextualize this occurrence and suggest a different theoretical and analytical framework. In pursuing this end, my goal is to understand the incidence of cybercriminal victimization better. Another objective is to gauge public knowledge of cybercrime and to establish distinctions with white-collar crime. My plan also includes examining lapses in cybersecurity policy and offering recommendations.

4.12 Limitations

The approach and outcomes of this study have several limitations. First, there is a potential limitation with the sample size. Given that the study is predominantly quantitative and Canada-wide, it is expected that a much larger sample would ensure far-reaching imputations and inferences about the Canadian population. Instead, a relatively lower sample size (403 responses) was utilized. The inability to reach a larger sample was due mainly to limited funding. Nonetheless, although relatively small, the sample size is statistically significant and representative enough for inferences about the Canadian population.

Secondly, the sample is skewed significantly in favor of White participants, with an overwhelming majority (89.1 %) falling under this group. However, this situation is only incidental to the sampling process and appears to be a function of the over-representation of Whites in the national population. The over-representation of White participants means that responses are likely to represent this group more.

Also, another sample size-related limitation is the number of Francophone-speaking responses in the study. The study generated 321 Anglophone Canadian responses compared to 82 Francophone Canadian responses. The unequal responses make it difficult to compare the two language groups across relevant statistical metrics in the analysis. However, the unequal distribution of responses between Anglophone and Francophone Canadian respondents is not a significant limitation because there is an unequal distribution between the two official language groups across Canada, with the Anglophone group outnumbering their Francophone counterparts.

Furthermore, the low number of responses generated by the qualitative question (309* responses) means the results cannot be generalized and should be interpreted with additional caution. Besides the low number of responses, the qualitative results also lack quality and depth (richness). Some participant responses were too brief to elicit significant meaning and aid in any meaningful in-depth analysis. The lack of depth in the responses was likely because the qualitative responses were collected with the quantitative data by using a survey questionnaire. Nonetheless, the qualitative responses provide useful exploratory information about internet-using Canadians' underlying motivations for internet use.

Another methodological limitation related to the qualitative data was the challenge of conducting detailed disaggregated pattern and trend analysis within and between groups about

Canadians' internet use motivations from the qualitative thematic analysis. This challenge was further heightened by the nature of the qualitative responses (brief, single words, phrases, and sentence responses) and the manual analysis utilized. However, unlike quantitative analysis, qualitative thematic analysis is not intended to provide disaggregated patterns with statistical implications.

Additionally, because the study was originally developed as purely quantitative research, it is possible the current study has not followed or applied all the principles of mixed method research design in full. Nonetheless, the qualitative aspect was not a significant focus of the study, hence would not constitute a major methodological limitation.

4.13 Summary and Conclusions

In this chapter, I described the methodology that guided this scholarly work. The research questions and associated hypotheses were presented, consisting of seven research questions with six hypotheses. The seventh question is the qualitative aspect of the study. Next, the mixed method was discussed. Referred to in earlier sociological literature as a multi-method research design (Lipset et al., 1956; Becker et al., 1961), it comprises the third strand of research designs in Sociology (Creswell, 2003; Morgan, 2007; Pearce, 2007). The other two are quantitative and qualitative designs (Morgan, 2007; Pearce, 2012). Mixed method research relates to the pragmatic approach and accounts for structure and agency, thus consistent with the goals of this current study.

The study sample consisted of Canadian internet users of at least 18 years of age. The survey questionnaire adapted questions from previous surveys and was pre-tested through a soft launch to guarantee the validity and reliability of the data. The study variables and their

operational definitions and measurements were also discussed. The chapter also presented the conceptual framework as a key structure to guide the research in terms of flow or sequence and to steep the study in theoretical constructs (Adom et al., 2018; Liehr & Smith, 1999). The analytical framework was also presented and consisted of analytical models and analytical strategy. The analytical models projected the relationship between the predictor variables and outcome and depicted the hypothesized interaction among the predictor variables. The analytical strategy consisted of descriptive analyses, statistical modeling, and thematic analyses. Whereas the descriptive and statistical modeling analyses pertained to the quantitative dimension and were conducted using SPSS, the thematic analysis related to the qualitative aspect and was conducted manually. Next, the chapter discussed ethical considerations, detailing the ethics application process, and explained data storage and results dissemination. Finally, I also discussed my reflexivity and revealed how a combination of individual experiences, academic interests, and practical dilemmas motivated the current research. The next chapter presents the results and analysis - an opportunity to see the methodology in practice.

Chapter Five: Results and Analyses

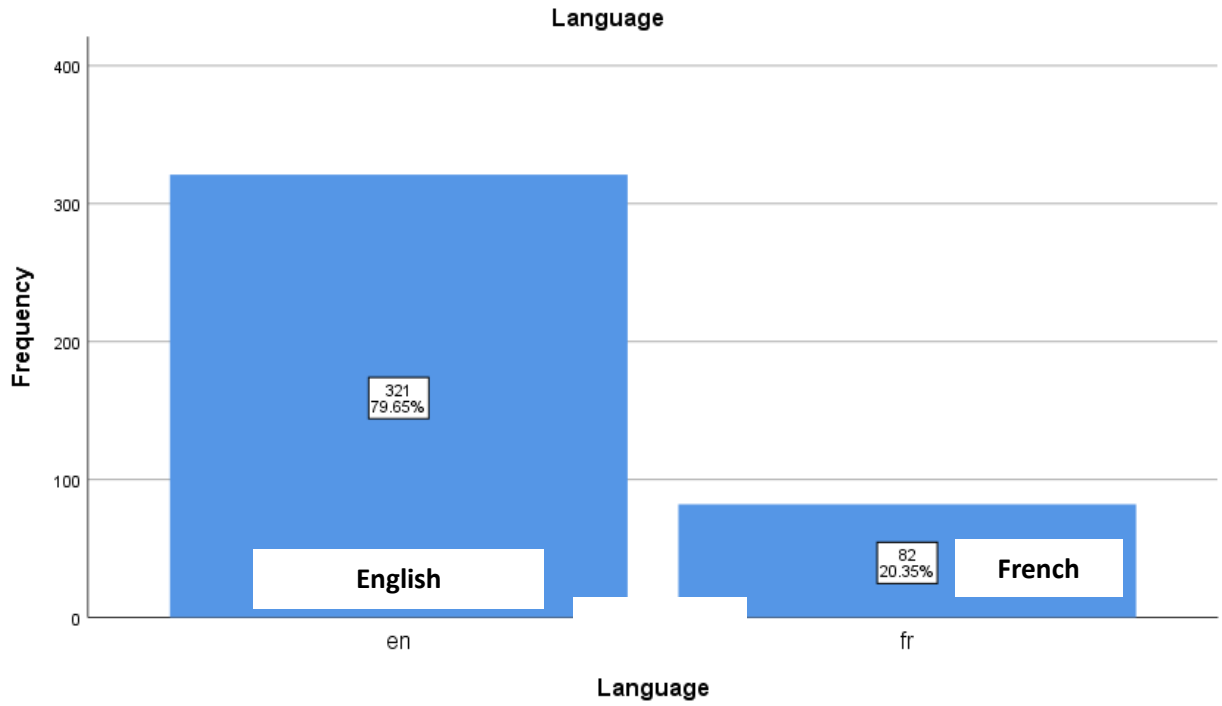
5.0 Introduction

This chapter presents the results of the statistical analysis carried out in the study. The issue motivating this research is why and how Canadian internet users continue to use various forms of computer-mediated communication despite the fear and inherent risk of victimization in cyberspace. In other words, has the perception of cybercrime risk changed how Canadians use the internet? The research problem of this study is examined using mixed method research design. The results are presented to align with the thematic focus of the study. In the first section, I describe the basic sample characteristics in terms of the socio-demographic profile. Next, I present the statistical modeling analysis involving the outcome variables on each predictor variable. I construct four models – to parallel the four outcome variables - representing the fear of cybercrime, risk of cybercrime, avoidance internet use behavior, and defensive internet use behavior. I follow this in the next section and present the results of hypotheses testing and conclude by presenting the analyzed conceptual framework.

5.1 Basic Sample Characteristics: Socio-demographics

Four hundred and three (403) participants responded to the study across Anglophone and Francophone Canada. Using the sample size calculator at the 95% confidence level, this number exceeds the initial objective of 384 (Creative Research Systems, 2012), and based on the Canadian population as of July 1, 2019 (Statistics Canada, 2019). Figure 5.1 reveals that of the total participants, about eight out of ten (79.65 %) or 321 people were English speakers, while two out of ten (20 %) or 82 people were French speakers. This shows that an overwhelming majority of respondents were English speakers.

Figure 5.1. Distribution of sample by official language



Analysis of the detailed socio-demographic profile of the sample is revealed in the frequency distribution in Table 5.1. The age distribution indicates that the sample profile is an adult population, with more than half aged 40 and above. A third of the respondents are below age 40, a group that may be described as young adults, while 25 % are between the ages of 40-52. The remaining respondents (39 %) are 53 years or older. In terms of gender, Table 5.1 reveals an almost balanced representation with 52.7 % males. Regarding education, under half (46.8 %) of the sample attained a minimum of university education, while more than half (53.2 %) had less than university education. In terms of ethnicity, an overwhelming majority (89.1 %) of the sample was White. Regarding marriage, more than two-in-ten (23.9 %) were single, the majority (45.3 %) were married, close to one-in-ten (9.5 %) were separated, 15.9 % were living in common-law, and the remaining (5.5 %) were widowed.

Table 5.1

Socio-demographic Analysis

Socio-Demographic	Frequency	Valid Percentage (%)
Age (n = 401)		
18-32	82	20.4
33-39	62	15.5
40-46	49	12.2
47-52	53	13.2
53 and older	155	38.7
Gender (n = 395)		
Male	208	52.7
Female	187	47.3
Education (n = 402)		
Less than university	214	53.2
University and above	188	46.8
Ethnicity (n = 403)		
Non-white	44	10.9
White	359	89.1
Marital status (n = 402)		
Single	96	23.9
Married	182	45.3
Separated	38	9.5
Common-law	64	15.9
Widowed	22	5.5
Family income (n = 394)		
<$50,000	94	23.9
>=$50,000 but <$75,000	85	21.6
>=$75,000 but <$125,000	116	29.4
>=$125,000	99	25.1
Employment status (n = 403)		
Employed	231	57
Not employed	172	42.7

Source: Field Data, 2022

Regarding family income, there was quite a fair distribution among the different income thresholds, each cut-off hovering within 20 % and a simple majority (29.4 %) who were making

between $75,000 and less than $125,000. And finally, less than half (42.7 %) of the respondents were not employed.

5.2 Frequency Distribution of the Outcome Variables by the Predictor Variables

5.2.1 Frequency Distribution of the Fear of Cybercrime by the Predictor Variables

The crosstabulation in Table 5.2 presents an analysis of the distribution of fear of cybercrime across the predictor variables. Regarding age and fear, among respondents who felt not at all fearful, fewer than three-in-ten were aged 18-32 and 33-39, while three-in-ten were 53 years and older. For those who felt a little fear, the majority, representing 35 %, were aged 53 years and older, and half of the moderately fearful respondents (50 %) represented the same age cohort again. Of respondents who felt very much fear, close to one-in-two (47 %) were aged 53 years and older, while less than one-in-ten (6 %) were in the 33-39 age group. And of the extremely fearful ones, four-in-ten (40 %) were aged 18-39 and 53 years and older.

Regarding gender and fear, close to an even representation of males and females answered not at all fearful (52 % and 48 % respectively), while half (52 %) of males were a little fearful. Of those expressing moderate fear and very much fear, more than half (56 and 53 %, respectively) were males. Of the extremely fearful respondents, 56 % were females. Table 5.2 indicates that males outnumber females across the metrics of fear, while the reverse is true only in the extreme fear category.

Table 5.2

Combined Crosstabulation of Fear of Cybercrime Victimization by the Predictor variables

Predictors	Fear of cybercrime n (%)						Chi-square (p-value)	Cramer's V (p-value)
	Not at all	A little	Moderately	Very much	Extremely	Total		
Socio-Demographics:								
Age							22.55 (0.13)	0.12 (0.13)
18-32	26 (27.7)	37 (20.4)	13 (15.5)	5 (15.6)	1 (10)	82 (20.4)		
33-39	20 (21.3)	29 (16)	8 (9.5)	2 (6.3)	3 (30)	62 (15.5)		
40-46	6 (6.4)	24 (13.3)	12 (14.3)	5 (15.6)	2 (20)	49 (12.2)		
47-52	12 (12.8)	27 (14.9)	9 (10.7)	5 (15.6)	0 (0)	53 (13.2)		
53 and older	30 (31.9)	64 (35.4)	42 (50)	15 (46.9)	4 (40)	155 (38.7)		
Gender							0.69 (0.95)	0.04 (0.95)
Male	48 (51.6)	93 (52.0)	47 (56)	16 (53.3)	4 (44.4)	208 (52.7)		
Female	45 (48.4)	86 (48)	37 (44)	14 (46.7)	5 (55.6)	187 (47.3)		
Education							1.17 (0.88)	0.05 (0.88)
Less than university	52 (55.3)	91 (50.3)	48 (55.8)	18 (56.3)	5 (55.6)	214 (53.2)		
University and above	42 (44.7)	90 (49.7)	38 (44.2)	14 (43.8)	4 (44.4)	188 (46.8)		
Ethnicity							10.64 (0.03)	0.16 (0.03)
Non-white	7 (7.4)	19 (10.5)	9 (10.5)	5 (15.6)	4 (40)	44 (10.9)		
White	87 (92.6)	162 (89.5)	77 (89.5)	27 (84.4)	6 (60)	359 (89.1)		
Marital Status							28.02 (0.03)	0.13 (0.03)
Single	29 (30.9)	46 (25.4)	14 (16.3)	5 (16.1)	2 (20)	96		
Married	34 (36.2)	79 (43.6)	52 (60.5)	16 (51.6)	1 (10)	182 (45.3)		
Separated	9 (9.6)	15 (8.3)	9 (10.5)	2 (6.5)	3 (30)	38 (9.5)		

Predictors	Fear of cybercrime n (%)						Chi-square (p-value)	Cramer's V (p-value)
	Not at all	A little	Moderately	Very much	Extremely	Total		
Common-law	18 (19.1)	31 (17.1)	7 (8.1)	6 (19.4)	2 (20)	64 (15.9)		
Widowed	4 (4.3)	10 (5.5)	4 (4.7)	2 (6.5)	2 (20)	22(5.5)		
Family Income							10.98 (0.53)	0.10 (0.53)
<$50,000	19 (20.4)	41 (23.2)	21 (24.4)	8 (27.6)	5 (55.6)	94 (23.9)		
>=$50,000 but <$75,000	24 (25.8)	34 (19.2)	19 (22.1)	5 (17.2)	3 (33.3)	85 (21.6)		
>=$75,000 but <$125,000	26 (28)	58 (32.8)	23 (26.7)	9 (31)	0 (0)	116 (29.4)		
>=$125,000	24 (25.8)	44 (24.9)	23 (26.7)	7 (24.1)	1 (11.1)	99 (25.1)		
Employment status							15.51 (0.004)	0.20 (0.004)
Employed	58 (61.7)	117 (64.6)	40 (46.5)	13 (40.6)	3 (30)	231 (57.3)		
Not employed	36 (38.3)	64 (35.4)	46 (53.5)	19 (59.4)	7 (70)	172 (42.7)		
Other Predictors: Victimization experience							29.26 (<0.001)	0.19 (<0.001)
Yes	10 (10.6)	33 (18.2)	22 (25.6)	13 (40.6)	4 (40)	82 (20.3)		
No	77 (81.9)	126 (69.6)	50 (58.1)	12 (37.5)	4 (40)	269 (66.7)		
Not sure	7 (7.4)	22 (12.2)	14 (16.3)	7 (21.9)	2 (20)	52 (12.9)		
Cybercrime incident reporting							14.45 (0.27)	0.11 (0.27)
Very likely	39 (41.5)	57 (31.5)	32 (37.2)	14 (43.8)	6 (60)	148 (36.7)		
Likely	42 (44.7)	89 (49.2)	38 (44.2)	12 (37.5)	1 (10)	182 (45.2)		
Unlikely	11 (11.7)	32 (17.7)	12 (14)	4 (12.5)	2 (20)	61 (15.1)		
Very unlikely	2 (2.1)	3 (1.7)	4 (4.7)	2 (6.3)	1 (10)	12 (3)		
Knowledge of cybercrime risk							42.92 (<0.001)	0.19 (<0.001)
Excellent	13 (13.8)	8 (4.4)	2 (2.3)	3 (9.4)	4 (40)	30 (7.4)		
Good	28 (29.8)	76 (42)	33 (38.4)	7 (21.9)	4 (40)	148 (36.7)		

Predictors	Fear of cybercrime n (%)						Chi-square (p-value)	Cramer's V (p-value)
	Not at all	A little	Moderately	Very much	Extremely	Total		
Fair	38 (40.4)	88 (48.6)	43 (50)	17 (53.1)	2 (20)	188 (46.7)		
Poor	15 (16)	9 (5)	8 (9.3)	5 (15.6)	0 (0)	37 (9.2)		
Internet use Frequency							22.10 (0.04)	0.14 (0.04)
Once daily	8 (8.5)	12 (6.6)	14 (16.3)	0 (0)	0 (0)	34 (8.4)		
Several times in a day	81 (86.2)	168 (92.8)	71 (82.6)	30 (93.8)	10 (100)	360 (89.3)		
Weekly	3 (3.2)	1 (0.6)	1 (1.2)	1 (3.1)	0 (0)	6 (1.5)		
Monthly	2 (2.1)	0 (0)	0 (0)	1 (3.1)	0 (0)	3 (0.7)		

Regarding education and fear, of internet users feeling not at all fearful, a little over half (55 %) had less than a university education. There is a reasonably even representation among those expressing little fear, with 50.3 % having less than a university education. Table 5.2 reveals that respondents with less than university education outnumbered those with a university or higher education along the continuum of fear. More than half (56 %) had less than a university education for the moderately and very much fearful respondents. In contrast, about 56 % had less than a university education for the extremely fearful.

Regarding ethnicity and fear, of the respondents answering not at all, a little, moderately, and very much fearful, a unanimous majority (93, 90, 90, and 84 % respectively) were White. And for the extremely fearful internet users, more than half or six-in-ten (60 %) were White. Table 5.2 reveals that along the continuum of fear of cybercrime, Whites dominated their non-White counterparts. The caveat here is that the sample was overwhelmingly White.

Regarding marital status and fear of cybercrime, of respondents who felt no fear at all, about three-in-ten were single (31 %) or married (36 %) and almost two-in-ten were in common-

law unions (19 %). Of respondents who felt a little fear, less than half (44 %) were married, and under one-in-ten (6 %) were widowed. Of those moderately fearful, more than half (61 %) were married, and one-in-ten (16 %) were single. Eight in ten (84 %) were not single for the very fearful. For the extremely fearful, two-in-ten (20 %) were single, in common-law, and widowed, while three-in-ten (30 %) were separated. The findings suggest that married people were more fearful of cybercrime than people in other relationship types.

Table 5.2 does not indicate a clear pattern of the distribution of fear among the different income levels; the seemingly close pattern is that respondents earning between $75,000 and less than $125,000 were in the majority in four out of the five fear thresholds. Regarding family income, of respondents who felt no fear, there was close to an even representation of the different income categories, with those earning between $75,000 and less than $125,000 holding a slight majority (28 %). For those who felt only a little fear, respondents earning between $75,000 and less than $125,000 were the majority (33 %). There is a fairly even representation of the different income levels for the moderately fearful, with 27 % of respondents earning between $75,000 and less than $125,000. For the very much fearful, the highest category (31 %) was the $75,000 but less than $125,000 income group, while the lowest (17 %) is the $50,000 but less than $75,000 income group. And for the extremely fearful, the majority group (56 %) earned less than $50,000, and the least (11 %) earned $125,000 or more.

Regarding employment status, of respondents answering not at all fearful and a little fearful, more than half (62 % and 65 %, respectively) were employed. And for the moderately, very much, and extremely fearful respondents, the not employed constituted the majority (54 %, 59 %, and 70 %, respectively). Table 5.2 reveals that the employed dominate at lower levels of fear (not at all fearful and a little fearful). However, as the threshold of fear increases from

moderate to extreme, the reverse holds, as the not employed tend to dominate. The inverse observation may suggest that employment is probably linked to feelings of security, where the not-employed feel vulnerable with higher levels of fear.

Regarding victimization experience and fear, of respondents who felt no fear, an overwhelming majority (82 %) had not experienced victimization. About seven-in-ten (70 %) were not victimized of those who reported a little fear. More than half (58 %) were not victimized for the moderately fearful, while one-in-four (26 %) were victimized. About 41 % were victimized for the very fearful, while a little over two-in-ten (22 %) were unsure about their victimization. Four-in-ten (40 %) were victimized and not victimized for the extremely fearful respondents, while two-in-ten (20 %) were unsure. Table 5.2 reveals that respondents not sure about their victimization were in the minority across all the levels of fear, while in all but one level of fear (very fearful) and partly in another (extremely fearful), respondents not victimized dominated. This finding suggests that internet users with no cybercrime experience tend to harbor more fear, contrary to the common-sense view.

In terms of cybercrime incident reporting and fear, of the internet users who felt no fear, an overwhelming majority (86 %) were either very likely or likely to report a cybercrime incident. In contrast, 12 % were unlikely to report. For those expressing a little fear, about 32 % were very likely to report an incident, nearly half (49 %) likely to report, while almost two-in-ten (18 %) were unlikely to report an incident. For the moderately fearful, 44 % were likely to report an incident, while less than one-in-ten (5 %) were very unlikely to report. For the very fearful, whereas eight-in-ten (81 %) were very likely or likely to report, about two-in-ten (19 %) were unlikely or very unlikely to report an incident. For those expressing extreme fear, an overwhelming majority (70 %) were very likely or likely to report a cybercrime incident. This

result indicates that respondents very unlikely to report an incident were in the minority along the continuum of fear. In contrast, in all but two fear levels, respondents likely to report an incident were in the majority. The results further demonstrated that at the highest levels of fear (very and extreme), respondents who were very likely to report dominated.

Regarding knowledge of cybercrime risk and fear, of respondents not feeling any fear, four-in-ten (40 %) had fair knowledge and one-in-ten (16 %) had poor knowledge of risk. The majority (49, 50, and 53 %, respectively) had a fair knowledge of risk for those expressing a little fear, moderate fear, and very much fear. At the same time, the minority possessed excellent knowledge of risk. For respondents expressing extreme fear, an equal number (40 %) had an excellent and good knowledge of risk, while two-in-ten (20 %) had a fair knowledge of risk. Table 5.2 indicates that respondents with fair knowledge tend to dominate all fear levels. This finding suggests that internet users with a fair knowledge of risk tend to be more cautious.

Regarding internet use frequency, an overwhelming majority (86 %) used the internet several times a day, while the least (2 %) used the internet monthly among those who reported no fear. For those with little and moderate fear, a unanimous majority (93 and 83 %, respectively) used the internet several times a day, and none used the internet monthly. For the very much and extremely fearful respondents, nine-in-ten (94 %) and ten-in-ten (100 %) used the internet several times a day. This result indicates that respondents using the internet several times a day are the majority in all cases of fear. This finding may suggest that respondents using the internet frequently tend to feel more vulnerable at each level of fear on the continuum.

5.2.2 Frequency Distribution of the Risk of Cybercrime by the Predictor Variables

The crosstabulation in Table 5.3 presents an analysis of the risk of cybercrime across the predictor variables. Regarding age and risk, of respondents who strongly agreed to feeling more at risk of cybercrime, most (44 %) were aged 53 years and older, and the minority (11 %) were 18-32. For those who agreed to feeling at risk, about four-in-ten (39 %) were aged 53 years and older, while one-in-four (25 %) were in the age range 40-52. Of respondents who felt neutral, 36 % were aged 18-32 years, and one-in-four (25 %) were 33-46 years old. For those who disagreed about feeling at risk, a quarter (25 %) were aged 33-39, 47-52, and 53 and older, respectively. For respondents who strongly disagree about feeling at risk, half (50 %) were in the age group 18-32 and 53 and older. Table 5.3 does not reveal an observable clear pattern of distribution risk levels across the age cohorts. The standout observation is that the two extreme age cohorts strongly disagreed about feeling at risk of cybercrime.

Regarding gender and risk, the results indicate a consistent pattern of reverse observations. More than half (55 and 53 % respectively) of respondents who strongly agreed and agreed they felt at risk were males. And of respondents who remained neutral and those who disagreed about feeling at risk, more than one-in-two (54 and 58 %, respectively) were females. Only males (100 %) disagreed with feeling at risk of cybercrime.

Regarding education and risk, of respondents who strongly agreed and agreed about feeling at risk, more than half (56 and 55 %) had a university education or more and less than a university education, respectively. Of respondents who remained neutral to the risk and disagreed with feeling at risk, more than six-in-ten (67 %) and almost six-in-ten (58 %) had less than a university education, respectively. Only respondents with a university education and above (100 %) disagreed about feeling at risk of cybercrime. Table 5.3 reveals that at the two

extremes on the risk continuum, internet users with a minimum of a university education tend to be in the majority. In contrast, lower than university education users tend to cluster in the middle of the risk continuum.

In terms of ethnicity, a unanimous majority of respondents who strongly agreed, agreed, and remained neutral about feeling at risk identified themselves as White (88, 90, and 87 %, respectively). Also, only respondents who identified as White (100 %) disagreed and strongly disagreed about feeling at risk of cybercrime. It is clear from Table 5.3 that internet users who identify as White tend to dominate across all the levels of risk.

Regarding marital status and risk, of the respondents who strongly agreed and agreed they feel at risk, more than one-in-two (58 %) and under half (42 %) were married. For respondents who answered neutral, seven-in-ten (74 %) were single or married. Of those who disagreed about feeling at risk, one-in-four (25 %) were single, married, separated, and in common-law, respectively. Only respondents identified as single (100 %) strongly disagree with feeling at risk of cybercrime. However, the distribution lacks a pattern in terms of a dominant group across the levels of risk. Internet users who are widowed tend to be in the minority at the first three levels of risk while totally absent at the last two (disagree and strongly disagree).

Table 5.3

Combined Crosstabulation of Perceived Risk of Cybercrime by the Predictor variables

Predictors	Risk of cybercrime n (%)						Chi-square (P-value)	Cramer's V (P-value)
	Strongly agree	Agree	Neutral	Disagree	Strongly disagree	Total		
Socio-Demographics:								
Age							21.92 (0.15)	0.12 (0.15)
18-32	14 (11)	43 (21.6)	22 (36.1)	2 (16.7)	1 (50)	82 (20.4)		
33-39	23 (18.1)	29 (14.6)	7 (11.5)	3 (25)	0 (0)	62 (15.5)		
40-46	16 (12.6)	24 (12.1)	8 (13.1)	1 (8.3)	0 (0)	49 (12.2)		
47-52	18 (14.2)	25 (12.6)	7 (11.5)	3 (25)	0 (0)	53 (13.2)		
53 and older	56 (44.1)	78 (39.2)	17 (27.9)	3 (25)	1 (50)	155 (38.7)		
Gender							3.88 (0.42)	0.10 (0.42)
Male	68 (55.3)	106 (53.3)	27 (45.8)	5 (41.7)	2 (100)	208 (52.7)		
Female	55 (44.7)	93 (46.7)	32 (54.2)	7 (58.3)	0 (0)	187 (47.3)		
Education							12.16 (0.02)	0.17 (0.02)
Less than university	55 (43.7)	111 (55.2)	41 (67.2)	7 (58.3)	0 (0)	214 (53.2)		
University and above	71 (56.3)	90 (44.8)	20 (32.8)	5 (41.7)	2 (100)	188 (46.8)		
Ethnicity							2.17 (0.71)	0.07 (0.71)
Non-white	15 (11.8)	21 (10.4)	8 (13.1)	0 (0)	0 (0)	44 (10.9)		
White	112 (88.2)	180 (89.6)	53 (86.9)	12 (100)	2 (100)	359 (89.1)		
Marital status							34.38 (0.01)	0.15 (0.01)
Single	17 (13.5)	51 (25.4)	23 (37.7)	3 (25)	2 (100)	96 (23.9)		
Married	73 (57.9)	84 (41.8)	22 (36.1)	3 (25)	0 (0)	182 (45.3)		
Separated	15 (11.9)	15 (7.5)	5 (8.2)	3 (25)	0 (0)	38 (9.5)		

Predictors	Risk of cybercrime n (%)						Chi-square (P-value)	Cramer's V (P-value)
	Strongly agree	Agree	Neutral	Disagree	Strongly disagree	Total		
Common-law	14 (11.1)	38 (18.9)	9 (14.8)	3 (25)	0 (0)	64 (15.9)		
Widowed	7 (5.6)	13 (6.5)	2 (3.3)	0 (0)	0 (0)	22 (5.5)		
Family income							18.89 (0.09)	0.13 (0.09)
<$50,000	22 (17.6)	52 (26.8)	17 (27.9)	1 (8.3)	2 (100)	94 (23.9)		
>=$50,000 but <$75,000	26 (20.8)	44 (22.7)	10 (16.4)	5 (41.7)	0 (0)	85 (21.6)		
>=$75,000 but <$125,000	36 (28.8)	55 (28.4)	21 (34.4)	4 (33.3)	0 (0)	116 (29.4)		
>=$125,000	41 (32.8)	43 (22.2)	13 (21.3)	2 (16.7)	0 (0)	99 (25.1)		
Employment status							0.62 (0.96)	0.04 (0.96)
Employed	73 (57.5)	114 (56.7)	37 (60.7)	6 (50)	1 (50)	231 (57.3)		
Not employed	54 (42.5)	87 (43.3)	24 (39.3)	6 (50)	1 (50)	172 (42.7)		
Other Predictors:								
Victimization experience							11.77 (0.16)	0.12 (0.16)
Yes	34 (26.8)	38 (18.9)	8 (13.1)	2 (16.7)	0 (0)	82 (20.3)		
No	74 (58.3)	135 (67.2)	48 (78.7)	10 (83.3)	2 (100)	269 (66.7)		
Not sure	19 (15)	28 (13.9)	5 (8.2)	0 (0)	0 (0)	52 (12.9)		
Cybercrime incident reporting							28.43 (0.01)	0.15 (0.01)
Very likely	58 (45.7)	65 (32.3)	20 (32.8)	4 (33.3)	1 (50)	148 (36.7)		
Likely	49 (38.6)	98 (48.8)	31 (50.8)	4 (33.3)	0 (0)	182 (45.2)		
Unlikely	15 (11.8)	34 (16.9)	8 (13.1)	4 (33.3)	0 (0)	61 (15.1)		
Very unlikely	5 (3.9)	4 (2)	2 (3.3)	0 (0)	1 (50)	12 (3)		
Knowledge of cybercrime risk							17.89 (0.12)	0.12 (0.12)
Excellent	17 (13.4)	6 (3)	5 (8.2)	2 (16.7)	0 (0)	30 (7.4)		
Good	47 (37)	73 (36.3)	22 (36.1)	5 (41.7)	1 (50)	148 (36.7)		

Predictors	Risk of cybercrime n (%)						Chi-square (P-value)	Cramer's V (P-value)
	Strongly agree	Agree	Neutral	Disagree	Strongly disagree	Total		
Fair	55 (43.3)	98 (48.8)	29 (47.5)	5 (41.7)	1 (50)	188 (46.7)		
Poor	8 (6.3)	24 (11.9)	5 (8.2)	0 (0)	0 (0)	37 (9.2)		
Internet use Frequency							9.29 (0.68)	0.09 (0.68)
Once daily	9 (7.1)	20 (10)	3 (4.9)	1 (8.3)	1 (50)	34 (8.4)		
Several times in a day	117 (92.1)	175 (87.1)	56 (91.8)	11 (91.7)	1 (50)	360 (89.3)		
Weekly	1 (.8)	4 (2)	1 (1.6)	0 (0)	0 (0)	6 (1.5)		
Monthly	0 (0)	2 (1)	1 (1.6)	0 (0)	0 (0)	3 (.7)		

Table 5.3 does not reveal a meaningful pattern regarding family income and risk in terms of the observed sequences. Of respondents who strongly agreed with feeling at risk, six-in-ten (62 %) earned a minimum of $75,000, while for those who agree, one-in-two (51 %) made a minimum of $75,000. For respondents who answered neutrally to feeling at risk, less than half (44 %) made less than $75,000. Whereas for respondents who disagreed with feeling at risk, half (50 %) earned less than $75,000, all those who strongly disagreed made less than $50,000.

Regarding employment status and risk, of respondents who strongly agreed and those who agreed with feeling at risk, more than half (58 and 57 % respectively) were employed. Of those who were neutral about feeling at risk, six-in-ten (61 %) were employed. Of respondents who disagreed and strongly disagreed, there was an exact representation (50 %) of the employed and not employed. This result reveals two observations: internet users employed and not employed are less unanimous when agreeing to or remaining neutral about risk, but they become unanimous (evenly represented) when disagreeing to feeling at risk. These results may suggest that the employed tend to feel more vulnerable to cybercrime than the not employed.

Table 5.3 reveals a consistent pattern of observed sequences between victimization experience and risk. For victimization experience and risk, half (58 %) of respondents who strongly agreed with feeling at risk have not been victimized, while more than half (67 %) of those who agreed have also not been victimized. An overwhelming majority (79 %) of respondents who were neutral to risk had no prior victimization experience. Also, while eight-in-ten (83 %) of respondents who disagreed with feeling at risk have not been victimized, all (100 %) of those who strongly disagreed have had no victimization. Across the levels of risk, internet users who have not been victimized tend to be in the majority. Curiously, they tend to agree and disagree with feeling at risk of cybercrime. It is also noteworthy that internet users who are uncertain about their victimization tend to be in the minority across almost all risk levels.

Regarding cybercrime incident reporting and risk, eight-in-ten (84 %) of respondents who strongly agreed with feeling at risk were very likely or likely to report a cybercrime incident. Of respondents who agreed, three-in-ten (32 %) were very likely to report, and about half (49 %) were likely to report. For respondents who answered neutral to risk, one-in-two (51 %) were likely to report, while a little over one-in-ten (16 %) were unlikely or very unlikely to report. Regarding those who disagreed, an exact representation (33 %) was very likely, likely, and unlikely to report an incident. Of those who strongly disagreed with feeling at risk, half (50 %) each were very likely and very unlikely to report. This result indicates that internet users who tend to feel more vulnerable to cybercrime are more likely to report an incident. Simultaneously, there is a split among persons who do not feel susceptible regarding their likelihood of reporting cybercrime incidents.

Table 5.3 reveals that internet users who are well-informed about cybercrime risk tend to feel more vulnerable, while those not well-informed tend to feel less vulnerable (agree and

neutral). Regarding knowledge of risk and feeling at risk, half (50 %) of the respondents who strongly agreed with feeling at risk were well-informed about risk (excellent and good). More than half (61 %) had a fair or poor knowledge of risk for respondents who agreed with feeling at risk. Of those who answered neutral to risk, less than half (44 %) were well-informed about risk. Regarding respondents who disagreed with feeling at risk, about six-in-ten (58 %) were well-informed. Of those who strongly disagreed with feeling at risk, half (50 %) had a good and fair knowledge of risk.

Regarding internet use frequency and risk, among respondents who strongly agreed and agree with feeling at risk, a unanimous majority (92 and 87 %, respectively) used the internet several times a day. For those who answered neutral and those who disagreed with feeling at risk, nine-in-ten (92 %) each used the internet several times a day. And among respondents who strongly disagreed, half (50 %) each used internet once daily and several times a day. Table 5.3 indicates that frequent internet users (use once daily or several times a day) tend to feel vulnerable to cybercrime compared to less frequent users. Curiously, this same group of users also appear to be neutral about feeling at risk and less vulnerable simultaneously.

5.2.3 Frequency Distribution of Avoidance Internet Use Behavior by the Predictor Variables

Table 5.4 reveals the basic descriptive information of avoidance behavior by the predictor variables. Regarding age and avoidance behavior, of respondents who answered yes to resorting to avoidance behavior in their internet use, most of them, representing 43 %, were aged 53 and older, and the least (13 %) were aged 33-39 years. For those who answered no to avoidance behavior, most (53 %) were part of the young age cohort between 18-39 years, while 47 individuals representing 39 %, were aged 47 and older. Regarding gender and avoidance internet behaviors, an almost even share of males and females (52 % and 48 % respectively) used

avoidance behavior, and a similar distribution (54 % and 46 % respectively) did not use avoidance internet behaviors. In both cases, Table 5.4 shows that males are the majority.

In terms of education and avoidance behavior, while more than one-in-two (58 %) persons who used avoidance behavior were males, more than one-in-two (57 %) persons who did not use avoidance behavior were females. The results show that each gender group dominates in one category, while no one gender group dominates in both categories of avoidance behavior.

Regarding ethnicity, of respondents who answered yes to using avoidance internet behavior, one-in-ten (11 %) identified as non-White while about nine-in-ten (89 %) were White. Similarly, of respondents who did not use avoidance internet behaviors, 12, representing 10 %, were non-White, while a unanimous majority (90 %) were White. Unlike education, Table 5.4 shows that one ethnic group (White) dominates in both avoidance behavior categories.

In terms of marriage and avoidance behavior, half of those who resorted to avoidance internet behavior (51 %) were married, while only 19 (7 %) were widowed. For those who answered no to avoidance internet behavior use, about three-in-ten (34 and 33 %) were single and married, respectively. In comparison, less than one-in-ten (6 and 3 %) were separated and widowed, respectively.

Table 5.4

Descriptive distribution of Avoidance behavior by the Predictor variables

Predictors	Avoidance behavior			Chi-square (*p*-value)	Cramer's V
	Yes n (%)	No n (%)	Total N (%)		
Socio-Demographics:					
Age (n = 401)				**22.13 (<0.001)**	**0.24 (<0.001)**
18-32	44 (15.7)	38 (31.4)	82 (20.4)		
33-39	36 (12.9)	26 (21.5)	62 (15.5)		
40-46	39 (13.9)	10 (8.3)	49 (12.2)		
47-52	41 (14.6)	12 (9.9)	53 (13.2)		
53 and older	120 (42.9)	35 (28.9)	155 (38.7)		
Gender (n = 395)				0.08 (0.78)	0.01 (0.78)
Male	143 (52.2)	65 (53.7)	208 (52.7)		
Female	131 (47.8)	56 (46.3)	187 (47.3)		
Education (n = 402)				**6.75 (0.01)**	**0.13 (0.01)**
Less than university	161 (57.5)	53 (43.4)	214 (53.2)		
University and above	119 (42.5)	69 (56.6)	188 (46.8)		
Ethnicity (n = 403)				0.21 (0.65)	0.02 (0.65)
Non-white	32 (11.4)	12 (9.8)	44 (10.9)		
White	249 (88.6)	110 (90.2)	359 (89.1)		
Marital status (n = 402)				**27.92 (<0.001)**	**0.26 (<0.001)**
Single	54 (19.3)	42 (34.4)	96 (23.9)		
Married	142 (50.7)	40 (32.8)	182 (45.3)		
Separated	31 (11.1)	7 (5.7)	38 (9.5)		
Common-law	34 (12.1)	30 (24.6)	64 (15.9)		
Widowed	19 (6.8)	3 (2.5)	22 (5.5)		
Family income (n = 394)				2.69 (0.44)	0.08 (0.44)
<$50,000	69 (25.4)	25 (20.5)	94 (23.9)		
>=$50,000 but <$75,000	57 (21.0)	28 (23.0)	85 (21.6)		
>=$75,000 but <$125,000	83 (30.5)	33 (27.0)	116 (29.4)		
>=$125,000	63 (23.2)	36 (29.5)	99 (25.1)		
Employment status (n = 403)				**8.21 (0.004)**	**0.14 (0.004)**
Employed	148 (52.7)	83 (68.0)	231 (57.3)		
Not employed	133 (47.3)	39 (32.0)	172 (42.7)		
Other Predictors:					

Predictors	Avoidance behavior			Chi-square (*p*-value)	Cramer's V
	Yes n (%)	No n (%)	Total N (%)		
Victimization experience (n = 403)				4.20 (0.12)	0.10 (0.12)
Yes	59 (21.0)	23 (18.9)	82 (20.3)		
Not sure	42 (14.9)	10 (8.2)	52 (12.9)		
No	180 (64.1)	89 (73.0)	269 (66.7)		
Cybercrime incident reporting (n = 403)				0.29 (0.96)	0.03 (0.96)
Very likely	104 (37.0)	44 (36.1)	148 (36.7)		
Likely	125 (44.5)	57 (46.7)	182 (45.2)		
Unlikely	43 (15.3)	18 (14.8)	61 (15.1)		
Very unlikely	9 (3.2)	3 (2.5)	12 (3.0)		
Knowledge of cybercrime risk (n = 403)				**8.63 (0.04)**	**0.15 (0.04)**
Excellent	14 (5.0)	16 (13.1)	30 (7.4)		
Good	103 (36.7)	45 (36.9)	148 (36.7)		
Fair	137 (48.8)	51 (41.8)	188 (46.7)		
Poor	27 (9.6)	10 (8.2)	37 (9.2)		
Internet use frequency (n = 403)				8.74 (0.37)	0.10 (0.37)
Once daily	26 (9.3)	8 (6.6)	34 (8.4)		
Several times in a day	250 (89.0)	110 (90.2)	360 (89.3)		
Weekly or more	5 (1.8)	4 (3.3)	9 (2.2)		

The results show a close-to-even distribution between the different income thresholds and the levels of avoidance behavior. Regarding family income and avoidance behavior, about two-in-ten (25, 21, and 23 %, respectively) of respondents who used avoidance internet behaviors earned less than $50,000, between $50,000 and less than $75,000, and equal to or more than $125,000, respectively. For respondents who answered no to avoidance behavior, more than one-in-two individuals representing 57 %, earned a minimum of $75,000, while more than four-in-ten persons, representing 44 %, made less than $75,000.

In terms of employment status and avoidance behavior, of respondents who answered yes to avoidance behavior, half (53 %) were employed, while close to half (47 %) were not

employed. And for those who answered no, about seven-in-ten (68 %) were employed while three-in-ten (32 %) were not. This result shows that in both categories of avoidance behavior, the employed are in the majority.

Regarding victimization experience and avoidance internet behavior, more than half (64 %) of those who answered yes to avoidance behavior had not experienced cybercrime victimization in the past year. In comparison, two-in-ten (21 %) had been victimized. The remaining 15 % were not sure about their victimization status. An overwhelming majority (73 %) had not experienced victimization for those who answered no to avoidance behavior. In comparison, about two-in-ten (19 %) had been victimized, and the rest (8 %) were unsure about their victimization status. Table 5.4 reveals a similar distribution pattern across the different victimization groups along the categories of avoidance behavior.

Table 5.4 shows a similar distribution pattern across different incident reporting groups along the binary categories of avoidance behavior. In terms of cybercrime incident reporting and avoidance internet behavior, of respondents who answered yes to avoidance behavior, while less than half (45 %) and three-in-ten (37 %) were likely and very likely to report an incident, respectively, one-in-ten (15 %) were unlikely to report. The rest (3 %) were very unlikely to report a cybercrime incident. For those who answered no to avoidance internet behavior, under half (47 %) and three-in-ten (36 %) were likely and very likely to report an incident, respectively. In comparison, one-in-ten (15 %) were unlikely to report, and the rest (3 %) were very unlikely to report a cybercrime incident.

Regarding knowledge of cybercrime risk and avoidance behavior, more than half (58 %) of respondents who answered yes to using avoidance behavior were not well-informed (fair and poor) about risk. On the contrary, for those who answered no to using avoidance behavior, an

even number (50 %) were well-informed (excellent and good) and not well-informed (fair and poor), accordingly.

Regarding internet use frequency and avoidance behavior, among respondents who answered yes to avoidance behavior use, a unanimous majority (89 %) used the internet several times a day. And for those who answered no to avoidance behavior use, another unanimous majority (90 %) also used the internet several times a day. Table 5.4 reveals that in both instances of avoidance behavior, about one-in-ten cumulatively reported once daily and weekly or more use.

5.2.4 Frequency Distribution of Defensive Internet Use Behavior by the Predictor Variables

Table 5.5 shows the basic descriptive information of defensive behavior by the predictor variables. Regarding age and defensive internet behavior, of respondents who answered yes to defensive behavior use, most of them, representing 41 %, were aged 53 and older, and the least (12 %) were aged 40-46 years. For those who answered no, most (46 %) belonged to the young age cohort (18-39 years), while 38 individuals, representing 43 %, were aged 47 and older. Table 5.5 shows a closer distribution between the young and older cohorts in terms of not using defensive internet behavior. Regarding gender and defensive internet behavior, more than half (53 %) of those who used and did not use defensive behavior were males. Table 5.5 shows that females were in the minority in both instances of defensive internet behavior use.

Regarding education and defensive behavior, more than one-in-two (53 and 55 %) of respondents who used and did not use defensive behavior, respectively, were males. And for ethnicity and defensive behavior, an overwhelming majority (89 and 90 %) of respondents who answered yes and no to defensive behavior use were males.

Table 5.5

Descriptive distribution of Defensive Behavior by the Predictor Variables

Predictors	Defensive behavior			Chi-square (*p*-value)	Cramer's V (p-value)
	Yes n (%)	No n (%)	Total N (%)		
Socio-Demographics:					
Age (n = 401)				5.79 (0.22)	0.12 (0.22)
18-32	60 (19.2)	22 (24.7)	82 (20.4)		
33-39	43 (13.8)	19 (21.3)	62 (15.5)		
40-46	39 (12.5)	10 (11.2)	49 (12.2)		
47-52	42 (13.5)	11 (12.4)	53 (13.2)		
53 and older	128 (41)	27 (30.3)	155 (38.7)		
Gender (n = 395)				0.001 (0.97)	0.002 (0.97)
Male	161 (52.6)	47 (52.8)	208 (52.7)		
Female	145 (47.4)	42 (47.2)	187 (47.3)		
Education (n = 402)				0.15 (0.70)	0.02 (0.70)
Less than university	165 (52.7)	49 (55.1)	214 (53.2)		
University and above	148 (47.3)	40 (44.9)	188 (46.8)		
Ethnicity (n = 403)				0.08 (0.78)	0.01 (0.78)
White	279 (88.9)	80 (89.9)	359 (89.1)		
Non-White	35 (11.1)	9 (10.1)	44 (10.9)		
Marital Status (n = 402)				**12.51 (0.01)**	**0.18 (0.01)**
Single	69 (22)	27 (30.3)	96 (23.9)		
Married	147 (47)	35 (39.3)	182 (45.3)		
Separated	35 (11.2)	3 (3.4)	38 (9.5)		
Common-law	43 (13.7)	21 (23.6)	64 (15.9)		
Widowed	19 (6.1)	3 (3.4)	22 (5.5)		
Family Income (n = 394)				2.10 (0.55)	0.07 (0.55)
<$50,000	77 (25.2)	17 (19.1)	94 (23.9)		
>=$50,000 but <$75,000	62 (20.3)	23 (25.8)	85 (21.6)		
>=$75,000 but <$125,000	89 (29.2)	27 (30.3)	116 (29.4)		
>=$125,000	77 (25.2)	22 (24.7)	99 (25.1)		
Employment status (n = 403)				2.11 (0.15)	0.07 (0.15)
Employed	174 (55.4)	57 (64)	231 (57.3)		
Not employed	140 (44.6)	32 (36)	172 (42.7)		

Predictors	Defensive behavior			Chi-square (*p*-value)	Cramer's V (p-value)
	Yes n (%)	No n (%)	Total N (%)		
Other Predictors:					
Victimization experience (n = 403)				3.01 (0.22)	0.09 (0.22)
Yes	65 (20.7)	17 (19.1)	82 (20.3)		
Not sure	45 (14.3)	7 (7.9)	52 (12.9)		
No	204 (65)	65 (73)	269 (66.7)		
Cybercrime incident reporting (n = 403)				3.27 (0.35)	0.09 (0.35)
Very likely	118 (37.6)	30 (33.7)	148 (36.7)		
Likely	140 (44.6)	42 (47.2)	182 (45.2)		
Unlikely	49 (15.6)	12 (13.5)	61 (15.1)		
Very unlikely	7 (2.2)	5 (5.6)	12 (3)		
Knowledge of Cybercrime risk (n = 403)				5.10 (0.16)	0.11 (0.16)
Excellent	25 (8)	5 (5.6)	30 (7.4)		
Good	120 (38.2)	28 (31.5)	148 (36.7)		
Fair	145 (46.2)	43 (48.3)	188 (46.7)		
Poor	24 (7.6)	13 (14.6)	37 (9.2)		
Internet use Frequency (n = 403)				2.70 (0.26)	0.08 (0.26)
Once daily	27 (8.6)	7 (7.9)	34 (8.4)		
Several times in a day	282 (89.8)	78 (87.6)	360 (89.3)		
Weekly or more	5 (1.6)	4 (4.5)	9 (2.2)		

Regarding marriage and defensive behavior, of those who used defensive behavior, more than four-in-ten (47 %) were married, while under one-in-ten (6 %) were widowed. For those who answered no to defensive behavior use, about four-in-ten (39 %) and three-in-ten (30 %) were married and single, while more than two-in-ten (24 %) were in a common-law relationship.

While the results reveal a fairly even distribution of respondents who used defensive internet behavior along the different family income thresholds, the distribution is distinct for respondents who answered no to defensive behavior along the family income groups. Regarding family income and defensive behavior, of those who answered yes to defensive behavior use, at least two-in-ten (20 %) belonged to each family income threshold. For respondents who did not

use defensive behavior, 49 individuals representing 55 %, earned a minimum of $75,000, while close to five-in-ten (45 %) earned less than $75,000.

Regarding employment status and defensive behavior, of respondents who answered yes to defensive behavior use, 174 respondents, representing 55 %, were employed, while 140 respondents, representing 45 %, were not employed. And for those not using defensive behavior, more than half (64 %) were employed, while three-in-ten (36 %) were not employed.

Regarding victimization experience and defensive internet behavior, for respondents who used defensive behavior, six-in-ten (65 %) had not been victimized. In comparison, two-in-ten (21 %) had experienced cybercrime victimization in the past year. For those who answered no to defensive behavior use, an overwhelming majority (73 %) had not experienced victimization, while about two-in-ten (19 %) had been victimized in the past year. Table 5.5 shows a similar distribution pattern across the different victimization groups along the categories of defensive behavior.

Regarding cybercrime incident reporting and defensive behavior, of respondents who answered yes to defensive behavior use, while four-in-ten (45 %) were likely and three-in-ten (38 %) were very likely to report an incident, less than one-in-ten (2 %) were very unlikely to report an incident. For those who answered no, under half (47 %) were likely and three-in-ten (34 %) were very likely to report an incident, while less than one-in-ten (6 %) were very unlikely to report a cybercrime incident. Here also, the results show a similar distribution pattern across the different incident reporting groups along the categories of defensive behavior.

Regarding knowledge of cybercrime risk and defensive behavior, of those who answered yes to defensive behavior, 140 respondents, representing 46 %, were well-informed (excellent

and good). In contrast, about half (54 %) were not well-informed (fair and poor). More than half (63 %) of respondents answered no to defensive behavior were not well-informed (fair and poor) about risk.

Regarding internet use frequency and defensive behavior, among respondents who answered yes to defensive behavior use, a unanimous majority (90 %) used the internet several times a day. And for those who answered no, a unanimous majority (88 %) used the internet several times a day.

5.3 Correlation Matrix among outcome variables

Table 5.6 shows the correlation matrix analysis among the four outcome variables – fear of cybercrime, risk of cybercrime, avoidance behavior, and defensive behavior. The Spearman correlation coefficient, the Pearson chi-square, and Cramer's V values were used to report the association's direction, strength, and significance among the outcome variables. The matrix reveals a significant positive correlation between fear and each risk of cybercrime and avoidance behavior and a significant negative correlation between fear and defensive behavior (p=0.28, $p<0.001$; p=0.40, $p<0.001$; p=-0.37, $p<0.001$). Though significant, however, the associations between fear and each of risk and defensive behavior are weak, while it is moderate between fear and avoidance behavior (χ^2=44.43, $p<0.001$, $ø_c$=0.17, $p<0.001$; χ^2=59.60, $p<0.001$, $ø_c$=0.39, $p<0.001$; χ^2=75.99, $p<0.001$, $ø_c$=0.43, $p<0.001$). Further, while the matrix reveals a significant positive and negative correlation, respectively, between risk and avoidance and between avoidance and defensive behavior (p=-0.17, $p<0.05$; p=-0.37, $p<0.001$), the reported associations are deemed weak (χ^2=15.99, $p<0.05$, $ø_c$=0.20, $p<0.05$; χ^2=53.78, $p<0.001$, $ø_c$=0.37, $p<0.001$).

Finally, the matrix indicates no correlation between risk and defensive behavior (p=-0.08, p=0.14).

Table 5.6

Chi-square test of association among outcome variables

Relationship	Rho (p-value)	Chi-square (p-value)	Cramer's V (p-value)
Fear of cybercrime vs. Cybercrime risk	0.28 (<0.001)**	44.43 (<0.001)**	0.17 (<0.001)**
Fear of cybercrime vs. Avoidance behavior	0.40 (<0.001)**	75.99 (<0.001)**	0.43 (<0.001)**
Fear of cybercrime vs. Defensive behavior	-0.37 (<0.001)**	59.60 (<0.001)**	0.39 (<0.001)**
Cybercrime risk vs. Avoidance behavior	0.17 (0.001)*	15.99 (0.003)*	0.20 (0.003)*
Cybercrime risk vs. Defensive behavior	-0.08 (0.14)	7.12 (0.13)	0.13 (0.13)
Avoidance behavior vs. Defensive behavior	-0.37 (<0.001)**	53.78 (<0.001)**	0.37 (<0.001)**

** Significant at 5% ** Significant at 1 %*

Figure 5.2. Analyzed/Finalized Analytical model 2

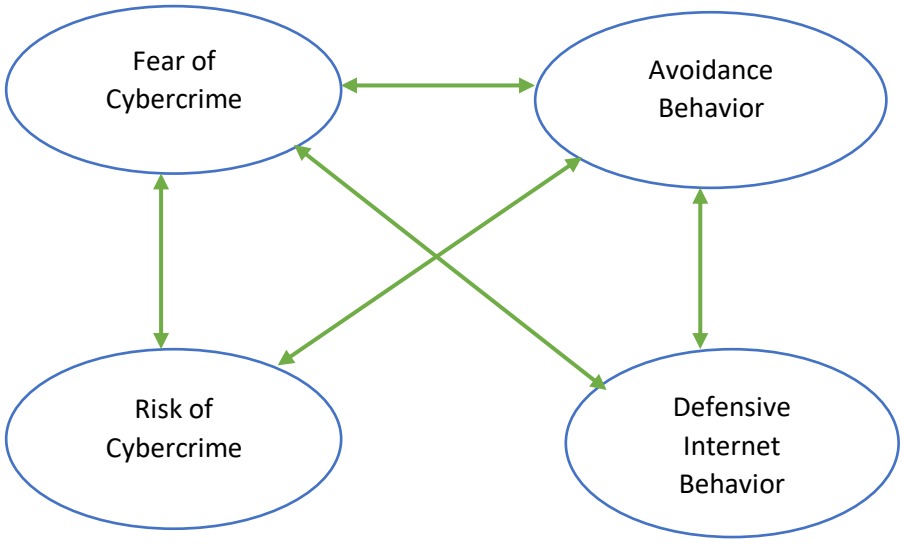


Figure 5.2 depicts analytical model 2 (see Figure 5.3 in chapter 5) in its analyzed or final form. Unlike in Figure 5.3, the arrowed lines in Figure 5.2 indicate the paths of significant associations between the outcome or dependent variables after the analysis. Figure 5.2 shows a significant association among the fear of cybercrime victimization, risk of cybercrime victimization, and avoidance internet use behavior. However, Figure 5.2 also reveals no association between the risk of cybercrime and defensive internet use behavior.

5.4 Univariable Analysis of Outcome Variables by the Predictors

The following sections present the univariable relationship between predictor and outcome variables. Unadjusted odds ratios (together with the associated 95 % confidence intervals) were used to describe the strength of the association and to determine statistical significance. A p-value threshold of 0.25 was used to select variable candidates for the multivariable modeling (Bendel & Afifi, 1977; Mickey & Greenland, 1989). The rest of this

section is organized as follows: Subsections 5.4.1 and 5.4.2 describe the univariable relationship between predictor variables and fear and risk of cybercrime victimization, respectively, while 5.4.3 and 5.4.4 describe the relationship between predictor variables and avoidance and defensive internet behaviors, respectively.

5.4.1 Univariable Analysis of Fear of Cybercrime

Table 5.7 represents the univariable model analysis of fear of cybercrime against the predictor variables. Regarding age, persons aged 33-39 had 1.05 times higher odds of developing the outcome (i.e., expressing fear of cybercrime) than those aged 18-32 (i.e., the reference group). This association, however, did not reach statistical significance at 5 % because the confidence interval contained 1 (95 % CI: 0.57, 1.95). However, being aged 40-46 was protective of fear because the odds associated with this age cohort were significantly lower than those aged 18-32 (OR = 0.41; 95 % CI: 0.22, 0.79). A similarly lower odds of expressing the fear of cybercrime was also observed among persons aged 47-52, although this did not reach statistical significance (OR = 0.73; 95 % CI: 0.39, 1.38). For the eldest respondents (i.e., age 53 and older), the odds of expressing the fear of cybercrime were statistically significantly lower and almost halved compared to those aged 18-32 (OR = 0.48; 95 % CI: 0.29, 0.80). Overall, age was a significant predictor of the fear of cybercrime in the univariable analysis; while being aged 40-46 and 53+ were protective for cybercrime fear, the age groups 33-39 and 47-52 were risk factors although not statistically significant.

In terms of gender, male internet users had lower odds of expressing fear than female internet users, although this association did not reach statistical significance at the 5 % confidence interval (OR = 0.94; 95 % CI: 0.65, 1.35). In the univariable analysis overall, gender was not a statistically significant predictor of fear of cybercrime.

Regarding education, internet users with less than a university education had lower odds of expressing fear than those with a minimum of university education. However, this relationship did not reach statistical significance at the 5 % confidence interval (OR = 0.96; 95 % CI: 0.67, 1.37). Like gender, overall, education was also not a statistically significant predictor of fear of cybercrime in the univariable analysis.

Regarding ethnicity, respondents who identified as White had almost twice the odds of expressing fear compared to non-White respondents, although this association did not reach statistical significance at the 5 % confidence interval (OR = 1.80; 95 % CI: 0.99, 3.23). Unlike gender and education, overall, ethnicity was a statistically significant predictor of fear of cybercrime in the univariable analysis, while being White was a predisposing factor of cybercrime fear.

Table 5.7

Univariable Model Analysis - Associations between Fear of Cybercrime and Predictor Variables

Predictors	Outcome: Fear of Cybercrime		
	β (Standard error)	**Unadjusted Odds Ratio (95% CI)**	**Univariable *p*-value**
Socio-Demographics:			
Age			**<0.05**
18-32	Ref		
33-39	0.05 (0.32)	1.05 (0.57, 1.95)	0.88
40-46	-0.89 (0.33)	0.41 (0.22, 0.79)	0.01
47-52	-0.32 (0.33)	0.73 (0.39, 1.38)	0.33
53 and older	-0.73 (0.26)	0.48 (0.29, 0.80)	0.01
Gender			0.72
Male	-0.07 (0.19)	0.94 (0.65, 1.35)	0.72
Female	Ref		
Education			0.81
Less than university	-0.04 (0.18)	0.96 (0.67, 1.37)	0.81
University and above	Ref		
Ethnicity			**0.05**
Non-white	Ref		
White	0.59 (0.29)	1.80 (0.99, 3.23)	0.05
Marital Status			**0.04**
Single	Ref		
Married	-0.65 (0.23)	0.52 (0.33, 0.83)	0.01
Separated	-0.58 (0.36)	0.56 (0.27, 1.13)	0.11
Common-law	-0.13 (0.30)	0.88 (0.49, 1.58)	0.66
Widowed	-0.76 (0.45)	0.47 (0.19, 1.12)	0.08
Family Income			0.55
<$50,000	-0.28 (0.27)	0.76 (0.45, 1.27)	0.29
>=$50,000 but <$75,000	0.07 (0.27)	1.07 (0.62, 1.83)	0.81
>=$75,000 but <$125,000	0.05 (0.25)	1.05 (0.64, 1.71)	0.86
>=$125,000	Ref		
Employment status			**0.002**
Employed	0.60 (0.19)	1.82 (1.26, 2.63)	0.002
Not employed	Ref		

Predictors	Outcome: Fear of Cybercrime		
	β (Standard error)	Unadjusted Odds Ratio (95% CI)	Univariable *p*-value
Other Predictors:			
Victimization experience			**0.000**
Yes	-1.10 (0.24)	0.33 (0.21, 0.53)	0.000
Not sure	-0.94 (0.28)	0.39 (0.23, 0.68)	0.001
No	Ref		
Cybercrime incident reporting			**0.24**
Very likely	0.95 (0.56)	2.59 (0.86, 7.80)	0.09
Likely	1.11 (0.56)	3.03 (1.01, 9.06)	0.05
Unlikely	0.93 (0.59)	2.53 (0.80, 8.03)	0.11
Very unlikely	Ref		
Knowledge of cybercrime risk			0.39
Excellent	0.09 (0.51)	1.10 (0.41, 2.97)	0.86
Good	-0.38 (0.36)	0.68 (0.34, 1.39)	0.29
Fair	-0.45 (0.36)	0.64 (0.32, 1.29)	0.21
Poor	Ref		
Internet use Frequency			0.66
Once daily	-1.36 (1.40)	0.26 (0.02, 3.99)	0.33
Several times in a day	-1.28 (1.37)	0.28 (0.02, 4.08)	0.35
Weekly	-0.59 (1.61)	0.56 (0.02, 13.12)	0.72
Monthly	Ref		

Overall, marital status was a statistically significant predictor of fear of cybercrime in the univariable analysis, while the various categories of marital status, relative to being single, were all protective of cybercrime fear. Respondents who identified as married had significantly lower odds of expressing fear than single respondents (OR = 0.52; 95 % CI: 0.33, 0.83). Also, separated persons had lower odds of expressing fear of cybercrime than single persons, although this association was not statistically significant at a 5% confidence interval (OR = 0.56; 95 % CI: 0.27, 1.13). Equally, respondents living in common-law relationships had lower odds of expressing fear of cybercrime than single respondents, although this relationship was not

statistically significant at the 5 % confidence interval (OR = 0.88; 95 % CI: 0.49, 1.58). Finally, widowed respondents had lower odds of expressing fear than single respondents, although the association did not reach statistical significance at the 5 % confidence interval (OR = 0.47; 95 % CI: 0.19, 1.12).

In terms of family income, persons who made less than $50,000 annually had lower odds of expressing cybercrime fear as compared to persons who made more than $125,000 per annum, although this association was not statistically significant at the 5 % confidence interval (OR = 0.76; 95 % CI: 0.45, 1.27). Similarly, individuals making between $50,000 and $75,000 annually had higher odds of expressing fear as compared to individuals who made more than $125,000 per annum, although this association did not reach statistical significance at the 5 % confidence interval (OR = 1.07; 95 % CI: 0.62, 1.83). Also, individuals who made between $75,000 and $125,000 had 1.05 higher odds of expressing cybercrime fear as compared to persons earning more than $125,000 per annum, although this association failed to reach statistical significance at the 5 % confidence interval (OR = 1.05; 95 % CI: 0.64, 1.71). Overall, family income was not a statistically significant predictor of fear of cybercrime in the univariable analysis, while family incomes between $50,000 and less than $125,000 were predisposing or risk factors for cybercrime fear.

Regarding employment status, being employed was a predisposing factor to cybercrime fear because the odds associated with this employment status were significantly higher than those not employed (OR = 1.82; 95 % CI: 1.26, 2.63). Overall, employment status was a statistically significant predictor of fear of cybercrime in the univariable analysis, while being employed was a predisposing factor of cybercrime fear.

In terms of victimization experience, persons victimized in the past year had significantly lower odds of expressing fear than persons without such experience (OR = 0.33; 99 % CI: 0.21, 0.53). Similarly, persons unsure about their victimization status also had significantly lower odds of expressing cybercrime fear than persons who had not been victimized (OR = 0.39; 99 % CI: 0.23, 0.68). Like employment status, overall, victimization experience was a statistically significant predictor of the fear of cybercrime in the univariable analysis, while being victimized and not sure of victimization status were protective factors of cybercrime fear.

Regarding cybercrime incident reporting, persons who were very likely to report a cybercrime incident had more than twice higher odds of expressing cybercrime fear than persons who were very unlikely to report. However, the association did not reach statistical significance at the 5 % confidence interval (OR = 2.59; 95 % CI: 0.86, 7.80). However, persons who were likely to report an incident of cybercrime had significantly higher odds of expressing cybercrime fear than persons who were very unlikely to report an incident (OR = 3.03; 95 % CI: 1.01, 9.06). In contrast, persons unlikely to report a cybercrime incident had higher odds of expressing cybercrime fear, although the relationship was not statistically significant at the 5 % confidence interval (OR = 2.53; 95 % CI: 0.80, 8.03). Overall, cybercrime incident reporting was not a statistically significant predictor of fear of cybercrime in the univariable analysis, while likely to report an incident was a significant risk factor of cybercrime fear.

Regarding the knowledge of cybercrime risk, persons with excellent knowledge had higher odds of expressing fear than those with poor knowledge, although the association was not statistically significant at the 5 % confidence interval (OR = 1.10; 95 % CI: 0.41, 2.97). However, for persons with good knowledge, the odds of expressing fear were lower than those with poor knowledge, although this association was not statistically significant at the 5 %

confidence interval (OR = 0.68; 95 % CI: 0.34, 1.39). Also, persons with only fair knowledge had lower odds of expressing fear than respondents with poor knowledge, although the relationship did not reach statistical significance at the 5 % confidence interval (OR = 0.64; 95 % CI: 0.32, 1.29). Overall, knowledge of cybercrime risk was not a statistically significant predictor of fear of cybercrime in the univariable analysis, while possessing excellent knowledge was a predisposing factor to cybercrime fear.

Regarding internet use frequency, persons who use the internet once daily had lower odds of expressing fear than persons who use the internet monthly, although the association failed to reach statistical significance at the 5 % confidence interval (OR = 0.26; 95 % CI: 0.02, 3.99). Also, persons who use the internet several times a day had lower odds of expressing fear than persons who use the internet monthly, although this association was not statistically significant at the 5 % confidence interval (OR = 0.28; 95 % CI: 0.02, 4.08). Similarly, for persons who use the internet weekly, the odds of expressing fear were halved as compared to persons who use the internet monthly, although the relationship was not also statistically significant at the 5 % confidence interval (OR = 0.56; 95 % CI: 0.02, 13.12). In the univariable analysis, the frequency of internet use was not a statistically significant predictor of fear of cybercrime.

5.4.2 Univariable Analysis of Risk of Cybercrime

Table 5.8 characterizes the univariable model analysis of the risk of cybercrime against the predictor variables. In terms of age, persons aged 33-39 had significantly lower odds of feeling at risk than those aged 18-32 (OR = 0.40; 95 % CI: 0.21, 0.75). Similarly, being aged 40-46 was protective of risk because the odds associated with this age cohort were significantly lower than those aged 18-32 (OR = 0.48; 95 % CI: 0.24, 0.93). Again, for persons aged 47-52, the odds of feeling at risk were significantly lower than those aged 18-32 (OR = 0.41; 95 % CI:

0.22, 0.79). A similarly significantly lower odds of feeling at risk was observed for the eldest age cohort (53 and older) compared to those aged 18-32. Overall, age was a significant predictor of cybercrime risk in the univariable analysis, while all the age groups, relative to the reference age cohort, were protective of cybercrime risk.

Regarding gender, male internet users had lower odds of perceiving risk than female internet users, although this association was not statistically significant at the 5 % confidence interval (OR = 0.82; 95 % CI: 0.56, 1.19). Overall, gender was not a statistically significant predictor of the risk of cybercrime in the univariable analysis.

Regarding education, the odds of feeling at risk among internet users with less than a university education was significantly higher than those with a minimum of university education (OR = 1.72; 95 % CI: 1.18, 2.50). Unlike gender, overall, education was a statistically significant predictor of the risk of cybercrime in the univariable analysis.

Regarding ethnicity, respondents who identified as White had higher odds of feeling at risk than non-White respondents, although this association was not statistically significant at the 5 % confidence interval (OR = 1.13; 95 % CI: 0.63, 2.03). Like gender, overall, ethnicity was not a statistically significant predictor of the risk of cybercrime in the univariable analysis, while being White was a predisposing factor of cybercrime risk.

Table 5.8

Univariable Model Analysis - Associations between Risk of Cybercrime and Predictor Variables

Predictors	Outcome: Risk of Cybercrime		
	β (Standard error)	**Unadjusted Odds Ratio (95% CI)**	**Univariable *p*-value**
Socio-Demographics:			
Age			**<0.05**
18-32	Ref		
33-39	-0.92 (0.32)	0.40 (0.21, 0.75)	0.00
40-46	-0.74 (0.34)	0.48 (0.24, 0.93)	0.03
47-52	-0.75 (0.34)	0.47 (0.24, 0.92)	0.03
53 and older	-0.95 (0.26)	0.39 (0.23, 0.64)	0.00
Gender			0.29
Male	-0.20 (0.19)	0.82 (0.56, 1.19)	0.29
Female	Ref		
Education			**<0.05**
Less than university	0.54 (0.19)	1.72 (1.18, 2.50)	0.00
University and above	Ref		
Ethnicity			0.69
White	0.12 (0.30)	1.13 (0.63, 2.03)	0.69
Non-White	Ref		
Marital Status			**<0.001**
Single	Ref		
Married	-1.06 (0.25)	0.35 (0.21, 0.56)	<0.001
Separated	-0.84 (0.38)	0.43 (0.21, 0.91)	0.03
Common-law	-0.39 (0.30)	0.68 (0.38, 1.23)	0.20
Widowed	-0.92 (0.44)	0.40 (0.17, 0.95)	0.04
Family Income			**0.09**
<$50,000	0.67 (0.27)	1.96 (1.15, 3.34)	0.01
>=$50,000 but <$75,000	0.40 (0.28)	1.50 (0.86, 2.60)	0.15
>=$75,000 but <$125,000	0.47 (0.26)	1.60 (0.96, 2.66)	0.07
>=$125,000	Ref		
Employment status			0.95
Employed	0.01 (0.19)	1.01 (0.70, 1.47)	0.95
Not employed	Ref		
Other Predictors:			
Victimization experience			**<0.05**
Yes	-0.67 (0.24)	0.51 (0.32, 0.83)	0.01
Not sure	-0.58 (0.29)	0.56 (0.32, 0.98)	0.05
No	Ref		
Cybercrime incident reporting			**0.17**
Very likely	-0.15 (0.57)	0.86 (0.26, 2.83)	0.79
Likely	0.26 (0.56)	1.30 (0.40, 4.22)	0.65
Unlikely	0.37 (0.60)	1.44 (0.42, 4.99)	0.54
Very unlikely	Ref		

Predictors	Outcome: Risk of Cybercrime		
	β (Standard error)	Unadjusted Odds Ratio (95% CI)	Univariable *p*-value
Knowledge of cybercrime risk			**0.25**
Excellent	-0.86 (0.47)	0.42 (0.16, 1.09)	0.07
Good	-0.13 (0.35)	0.88 (0.46. 1.69)	0.71
Fair	-0.07 (0.34)	0.93 (0.49, 1.77)	0.84
Poor	Ref		
Internet use Frequency			0.70
Once daily	-0.98 (1.12)	0.38 (0.05, 2.84)	0.38
Several times in a day	-1.08 (1.08)	0.34 (0.05, 2.37)	0.32
Weekly	-0.73 (1.32)	0.48 (0.04, 5.30)	0.58
Monthly	Ref		

Overall, marital status was a statistically significant predictor of cybercrime risk in the univariable analysis; while all the levels of marriage relative to being single were protective of cybercrime risk, being married, separated, and widowed was particularly significant. The odds of perceiving risk among the married were significantly lower than persons who identified as single (OR = 0.35; 95 % CI: 0.21, 0.56). Similarly, the odds of perceiving risk among separated respondents were significantly lower than single respondents (OR = 0.43; 95 % CI: 0.21, 0.91). Also, respondents in common-law unions had lower odds of feeling at risk than single respondents, although this association was not statistically significant at the 5 % confidence interval (OR = 0.68; 95 % CI: 0.38, 1.23). Equally, widowed respondents had significantly lower odds of feeling at risk than their single counterparts (OR = 0.40; 95 % CI: 0.17, 0.95).

Regarding family income, persons who made less than $50,000 annually had significantly higher odds (almost twice) of perceiving the risk of cybercrime than persons who made more than $125 (OR = 1.96; 95 % CI: 1.15, 3.34). Also, the odds of perceiving risk among persons who annually made between $50,000 and $75,000 was higher as compared to persons who make more than $125,000 per annum, although this relationship did not reach statistical

significance at the 5 % confidence interval (OR = 1.50; 95 % CI: 0.86, 2.60). Similarly, persons who made between $75,000 and less than $125,000 had higher odds of feeling at risk as compared to persons earning more than $125,000 per annum, although the association also failed to reach statistical significance at the 5 % confidence interval (OR = 1.60; 95 % CI: 0.96, 2.66). Overall, family income was a statistically significant predictor of cybercrime risk in the univariable analysis. The different family income cut-offs relative to the reference income threshold were all predisposing factors for cybercrime risk.

Regarding employment status, being employed was a predisposing factor of cybercrime risk perception because the odds associated with this group were higher than respondents who were not employed (OR = 1.01; 95 % CI: 0.70, 1.47). Overall, employment status was not a statistically significant predictor of cybercrime risk in the univariable analysis, while being employed was a predisposing factor of cybercrime risk.

Like family income, overall, victimization experience was a statistically significant predictor of the risk of cybercrime in the univariable analysis, while being victimized and not sure of victimization status were both protective factors of cybercrime risk. The odds of feeling at risk associated with persons victimized in the past year were significantly lower than persons without such experience (OR = 0.51; 95 % CI: 0.32, 0.83). Similarly, not being sure about victimization status was protective of cybercrime risk, as the odds associated with this group were significantly lower than persons who had not been victimized (OR = 0.56; 95 % CI: 0.32, 0.98).

Regarding cybercrime incident reporting, persons who were very likely to report an incident had lower odds of feeling at risk as compared to persons who were very unlikely to report, although this association was not statistically significant at the 5 % confidence interval

(OR = 0.86; 95 % CI: 0.26, 2.83). On the contrary, the odds of feeling at risk associated with persons who were likely to report an incident of cybercrime were higher than persons who were very unlikely to report, although the association was not statistically significant at the 5 % confidence interval (OR = 1.30; 95 % CI: 0.40, 4.22). Similarly, persons who were unlikely to report a cybercrime incident also had higher odds of feeling at risk than persons who were very unlikely to report, although this association did not reach statistical significance at the 5 % confidence interval (OR = 1.44; 95 % CI: 0.42, 4.99). Overall, cybercrime incident reporting was a statistically significant predictor of cybercrime risk perception in the univariable analysis; while very unlikely to report an incident was protective, both likely and unlikely to report were predisposing factors to cybercrime risk.

Regarding knowledge of cybercrime risk, the odds associated with persons with excellent knowledge were lower than respondents with poor knowledge. However, this association did not statistical significance at the 5 % confidence interval (OR = 0.42; 95 % CI: 0.16, 1.09). Also, having a good knowledge of risk was protective as the odds associated with this group were lower than respondents who had poor knowledge, although this association was not statistically significant at the 5 % confidence interval (OR = 0.88; 95 % CI: 0.46, 1.69). Similarly, persons with a fair knowledge of risk had lower odds of feeling at risk than respondents who had poor knowledge, although this association was not statistically significant at the 5 % confidence interval (OR = 0.93; 95 % CI: 0.49, 1.77). Overall, knowledge of cybercrime risk was a borderline statistically significant predictor of the risk of cybercrime in the univariable analysis. The levels of knowledge relative to the reference group (poor knowledge) were all protective of cybercrime risk perception.

Regarding internet use frequency, persons who used the internet once daily had lower odds of feeling at risk than persons who used the internet monthly, although this association was not statistically significant at the 5 % confidence interval (OR = 0.38; 95 % CI: 0.05, 2.84). Also, the odds of feeling at risk associated with persons who used the several times a day were lower than persons who use the internet monthly, although this association was not statistically significant at the 5 % confidence interval (OR = 0.34; 95 % CI: 0.05, 2.37). Likewise, for persons who used the internet weekly, the odds of feeling at risk was less than half as compared to persons who used the internet monthly, although this association was also not statistically significant at the 5 % confidence interval (OR = 0.48; 95 % CI: 0.04, 5.30). Overall, the frequency of internet use was not a statistically significant predictor of the risk of cybercrime in the univariable analysis, while all the levels of internet use frequency, relative to monthly use, were all protective of cybercrime risk.

5.4.3 Univariable Analysis of Avoidance Internet use Behavior

Table 5.9 shows the univariable model analysis of avoidance internet use behavior against the predictor variables. Regarding age, persons aged 33-39 years had higher odds of resorting to avoidance internet behavior than those aged 18-32, although this association was not statistically significant at the 5 % confidence interval (OR = 1.10; 95 % CI: 0.56, 2.15). Being aged 40-46 encouraged avoidance behavior use because the odds associated with this age group were significantly higher than those aged 18-32 (OR = 2.94; 95 % CI: 1.29, 6.73). Similarly, for persons aged 47-52, the odds of using avoidance internet behavior were significantly higher than those aged 18-32 (OR = 2.66; 95 % CI: 1.22, 5.82). Equally, persons aged 53 and older also had significantly higher odds of resorting to avoidance behavior than those aged 18-32 (OR = 2.74; 95 % CI: 1.54, 4.88). Overall, age was a significant predictor of avoidance behavior use in the

univariable analysis; all the different age cohorts, relative to the reference age group, encouraged avoidance internet use behavior.

In terms of gender, male internet users had lower odds of exhibiting avoidance behavior than female internet users, although the association did not reach statistical significance at the 5 % confidence interval (OR = 0.97; 95 % CI: 0.63, 1.49). Overall, gender was not a statistically significant predictor of avoidance behavior in the univariable analysis. Regarding education, the odds of exhibiting avoidance behavior among internet users with less than a university education were significantly higher than those with a minimum of university education (OR = 1.79; 95 % CI: 1.16, 2.76). Overall, education was a statistically significant predictor of avoidance behavior in the univariable analysis.

Regarding ethnicity, respondents who identified as White had lower odds of resorting to avoidance behavior than non-White respondents, although this association was not statistically significant at the 5 % confidence interval (OR = 0.90; 95 % CI: 0.44, 1.84). In the univariable analysis, ethnicity failed to statistically significantly predict avoidance behavior, while being White discouraged avoidance internet use behavior.

Table 5.9

Univariable Model Analysis - Associations between Avoidance behavior and Predictor Variables

Predictors	Outcome: Avoidance behavior		
	β (Standard error)	**Unadjusted Odds Ratio (95% CI)**	**Univariable *p*-value**
Socio-Demographics:			
Age			**0.001**
18-32	Ref		
33-39	0.10 (0.34)	1.10 (0.56, 2.15)	0.78
40-46	1.08 (0.42)	2.94 (1.29, 6.73)	0.01
47-52	0.98 (0.40)	2.66 (1.22, 5.82)	0.01
53 and older	1.01 (0.30)	2.74 (1.54, 4.88)	0.001
Gender			0.87
Male	-0.04 (0.22)	0.97 (0.63, 1.49)	0.87
Female	Ref		
Education			**0.01**
Less than university	0.58 (0.22)	1.79 (1.16, 2.76)	**0.01**
University and above	Ref		
Ethnicity			0.78
White	-0.10 (0.36)	0.90 (0.44, 1.84)	0.78
Non-White	Ref		
Marital status			**<0.001**
Single	Ref		
Married	1.02 (0.27)	2.76 (1.62, 4.71)	<0.001
Separated	1.24 (0.47)	3.44 (1.38, 8.59)	0.01
Common-law	-0.13 (0.32)	0.88 (0.47, 1.66)	0.70
Widowed	1.60 (0.65)	4.93 (1.37, 17.76)	0.02
Family income			0.46
<$50,000	0.46 (0.32)	1.58 (0.84, 2.95)	0.15
>=$50,000 but <$75,000	0.14 (0.31)	1.15 (0.62, 2.12)	0.66
>=$75,000 but <$125,000	0.36 (0.30)	1.43 (0.80, 2.55)	0.23
>=$125,000	Ref		
Employment status			**0.003**
Employed	-0.70 (0.23)	0.50 (0.32, 0.79)	**0.003**
Not employed	Ref		
Other Predictors:			
Victimization experience			0.26
Yes	0.22 (0.28)	1.25 (0.72, 2.16)	0.43
Not sure	0.61 (0.40)	1.84 (0.85, 4.02)	0.12
No	Ref		

Predictors	Outcome: Avoidance behavior		
	β (Standard error)	Unadjusted Odds Ratio (95% CI)	Univariable *p*-value
Cybercrime incident reporting			0.98
Very likely	-0.003 (0.71)	0.10 (0.25, 4.04)	0.996
Likely	-0.08 (0.71)	0.93 (0.23, 3.72)	0.91
Unlikely	-0.13 (0.75)	0.88 (0.20, 3.81)	0.87
Very unlikely	Ref		
Knowledge of cybercrime risk			**0.03**
Excellent	-1.20 (0.53)	0.30 (0.11, 0.86)	0.02
Good	-0.11 (0.42)	0.89 (0.40, 2.02)	0.79
Fair	0.04 (0.41)	1.04 (0.47, 2.31)	0.93
Poor	Ref		
Internet use frequency			0.37
Once daily	1.14 (0.82)	3.13 (0.63, 15.45)	0.16
Several times in a day	0.78 (0.72)	2.19 (0.54, 8.90)	0.28
Weekly or more	Ref		

Regarding marital status, persons identified as married had significantly higher odds (almost three times) of resorting to avoidance behavior than single persons (OR = 2.76; 95 % CI: 1.62, 4.71). Also, separated respondents had higher odds of resorting to avoidance behavior than the single persons, although the association did not reach statistical significance at the 5 % confidence interval (OR = 3.44; 95 % CI: 1.38, 8.59). Unlike the married and separated, respondents in common-law unions had lower odds of resorting to avoidance behavior than single persons, although the relationship was not statistically significant at the 5 % confidence interval (OR = 0.88; 95 % CI: 0.47, 1.66). But like the married and separated, the odds of resorting to avoidance behavior among the widowed were significantly higher (almost five times) than the single respondents (OR = 4.93; 95 % CI: 1.37, 17.76). Overall, marital status was a statistically significant predictor of avoidance behavior in the univariable analysis, while being married, separated, and widowed encouraged avoidance of internet use.

In terms of family income, persons who made less than $50,000 annually had higher odds of resorting to avoidance behavior than persons who made more than $125, 000, although the association did not reach statistical significance at the 5 % confidence interval (OR = 1.58; 95 % CI: 0.84, 2.95). Also, the odds of resorting to avoidance behavior among persons who annually make between $50,000 and $75,000 was higher than persons who made more than $125,000 per annum, although the association was not statistically significant at the 5 % confidence interval (OR = 1.15; 95 % CI: 0.62, 2.12). Similarly, persons who made between $75,000 and $125,000 had higher odds of resorting to avoidance behavior than persons earning more than $125,000 per annum, although this association was also not statistically significant at the 5 % confidence interval (OR = 1.43; 95 % CI: 0.80, 2.55). Overall, family income was not a statistically significant predictor of avoidance behavior in the univariable analysis. All the different family income thresholds, relative to the reference income cut-off, were motivating for avoidance internet use behavior.

Regarding employment status, being employed discouraged avoidance internet behavior use because the odds associated with this group were significantly higher than respondents who were not employed (OR = 0.50; 95 % CI: 0.32, 0.79). Overall, employment status was a statistically significant predictor of avoidance behavior in the univariable analysis, while being employed discouraged avoidance internet use behavior.

In terms of victimization experience, the odds of resorting to avoidance behavior associated with persons victimized in the past year were higher than persons without such experience, although this association was not statistically significant at the 5 % confidence interval (OR = 1.25; 95 % CI: 0.72, 2.16). Similarly, not being sure about victimization status was encouraging avoidance behavior use, as the odds associated with this group were higher

(almost twice) than persons who had not been victimized, although this association was not statistically significant at the 5 % confidence interval (OR = 1.84; 95 % CI: 0.85, 4.02). Overall, victimization experience was not a statistically significant predictor of avoidance behavior in the univariable analysis; the two victimization experience groups, relative to the reference group, encouraged avoidance internet use behavior.

Regarding cybercrime incident reporting, persons who were very likely to report an incident had lower odds of resorting to avoidance behavior than persons who were very unlikely to report, although this association was not statistically significant at the 5 % confidence interval (OR = 0.10; 95 % CI: 0.25, 4.04). Also, the odds of resorting to avoidance behavior associated with persons who were likely to report an incident of cybercrime were lower than persons who were very unlikely to report, although this association was not statistically significant at the 5 % confidence interval (OR = 0.93; 95 % CI: 0.23, 3.72). Similarly, persons who were unlikely to report a cybercrime incident also had lower odds of resorting to avoidance behavior than persons who were very unlikely to report, although this association was not statistically significant at the 5 % confidence interval (OR = 0.88; 95 % CI: 0.20, 3.81). In the univariable analysis, cybercrime incident reporting was not a statistically significant predictor of avoidance behavior. All the reporting levels, relative to the very unlikely to report, discouraged avoidance internet use behavior.

Regarding knowledge of risk, the odds of resorting to avoidance behavior associated with persons with excellent knowledge were significantly lower than respondents who had poor knowledge (OR = 0.30; 95 % CI: 0.11, 0.86). Similarly, having good knowledge of risk discouraged avoidance behavior as the odds associated with this group was lower than respondents who had poor knowledge, although this association was not statistically significant

at the 5 % confidence interval (OR = 0.89; 95 % CI: 0.40, 2.02). On the contrary, persons with a fair knowledge of risk had higher odds of resorting to avoidance behavior than respondents with poor knowledge, although the relationship did not reach statistical significance at the 5 % confidence interval (OR = 1.04; 95 % CI: 0.47, 2.31). Overall, knowledge of cybercrime risk was a statistically significant predictor of avoidance internet use behavior in the univariable analysis. Possessing excellent and good knowledge of risk was demotivating, while having a fair knowledge encouraged avoidance internet use behavior.

Regarding internet use frequency, persons who use the internet once daily had higher odds of resorting to avoidance behavior than persons who use the internet weekly or more, although this association was not statistically significant at the 5 % confidence interval (OR = 3.13; 95 % CI: 0.63, 15.45). Similarly, the odds of resorting to avoidance behavior associated with persons who use the internet several times a day were higher than with persons who use the internet weekly or more, although this association was not statistically significant at the 5 % confidence interval (OR = 2.19; 95 % CI: 0.54, 8.90). Overall, the frequency of internet use was not a statistically significant predictor of avoidance behavior in the univariable analysis, while both frequency levels, relative to the reference group, encouraged avoidance internet use behavior.

5.4.4 Univariable Analysis of Defensive Internet use Behavior

Table 5.10 reveals the univariable model analysis of defensive behavior against the predictor variables. In terms of age, persons aged 33-39 had lower odds of resorting to defensive internet behavior than those aged 18-32, although the association was not statistically significant at the 5 % confidence interval (OR = 0.83; 95 % CI: 0.40, 1.72). On the contrary, the odds of resorting to defensive behavior among persons aged 40-46 were higher than those aged 18-32.

However, the association did not reach statistical significance at the 5 % confidence interval (OR = 1.43; 95 % CI: 0.61, 3.34). Equally, age cohort 47-52 encouraged defensive behavior use because the odds associated with this age group were higher than those aged 18-32, although this association was not statistically significant at the 5 % confidence interval (OR = 1.40; 95 % CI: 0.61, 3.19). Also, persons aged 53 and older had higher odds of resorting to defensive behavior than those aged 18-32, although this association was not statistically significant at the 5 % confidence interval (OR = 1.74; 95 % CI: 0.92, 3.30). Overall, age was a significant predictor of defensive behavior use in the univariable analysis; while age 33-39 discouraged defensive internet behavior use, age 40 and older encouraged defensive internet behavior use.

Regarding gender, being male discouraged defensive behavior use as the odds associated with this group were lower than female internet users, although this association was not statistically significant at the 5 % confidence interval (OR = 0.99; 95 % CI: 0.62, 1.59). In the univariable analysis, gender was not a statistically significant predictor of defensive behavior.

Regarding education, the odds of exhibiting defensive behavior among internet users with less than a university education were lower than those with a minimum of a university education, although this association was not statistically significant at the 5 % confidence interval (OR = 0.91; 95 % CI: 0.57, 1.46). Overall, education was not a statistically significant predictor of defensive behavior in the univariable analysis.

Table 5.10

Univariable Model Analysis - Associations between Defensive behavior and Predictor Variables

Predictors	Outcome: Defensive behavior		
	β (Standard error)	**Unadjusted Odds Ratio (95% CI)**	**Univariable *p*-value**
Socio-Demographics:			
Age			**0.22**
18-32	Ref		
33-39	-0.19 (0.37)	0.83 (0.40, 1.72)	0.62
40-46	0.36 (0.43)	1.43 (0.61, 3.34)	0.41
47-52	0.34 (0.42)	1.40 (0.61, 3.19)	0.42
53 and older	0.55 (0.33)	1.74 (0.92, 3.30)	0.09
Gender			0.97
Male	-0.01 (0.24)	0.99 (0.62, 1.59)	0.97
Female	Ref		
Education			0.70
Less than university	-0.09 (0.24)	0.91 (0.57, 1.46)	0.70
University and above	Ref		
Ethnicity			0.78
White	-0.11 (0.39)	0.90 (0.41, 1.94)	0.78
Non-White	Ref		
Marital Status			**0.02**
Single	Ref		
Married	0.50 (0.29)	1.64 (0.92, 2.93)	0.09
Separated	1.52 (0.64)	4.57 (1.30, 16.10)	0.02
Common-law	-0.22 (0.35)	0.80 (0.40, 1.59)	0.53
Widowed	0.91 (0.66)	2.48 (0.68, 9.06)	0.17
Family Income			0.56
<$50,000	0.26 (0.36)	1.29 (0.64, 2.63)	0.48
>=$50,000 but <$75,000	-0.26 (0.34)	0.77 (0.39, 1.51)	0.45
>=$75,000 but <$125,000	-0,06 (0.33)	0.94 (0.50, 1.79)	0.85
>=$125,000	Ref		
Employment status			**0.15**
Employed	-0.36 (0.25)	0.70 (0.43, 1.14)	0.15
Not employed	Ref		
Other Predictors:			
Victimization experience			**0.23**
Yes	0.20 (0.31)	1.22 (0.67, 2.23)	0.52
Not sure	0.72 (0.43)	2.05 (0.88, 4.76)	0.10
No	Ref		
Cybercrime incident reporting			0.38
Very likely	1.03 (0.62)	2.81 (0.83, 9.48)	0.10
Likely	0.87 (0.61)	2.38 (0.72, 7.89)	0.16
Unlikely	1.07 (0.67)	2.92 (0.79, 10.81)	0.11
Very unlikely	Ref		

Knowledge of cybercrime risk			**0.18**
Excellent	1.00 (0.60)	2.71 (0.84, 8.76)	0.10
Good	0.84 (0.40)	2.32 (1.05, 5.12)	0.04
Fair	0.60 (0.39)	1.83 (0.86, 3.89)	0.12
Poor	Ref		
Internet use Frequency			0.29
Once daily	1.13 (0.79)	3.09 (0.65, 14.62)	0.16
Several times in a day	1.06 (0.68)	2.89 (0.76, 11.03)	0.12
Weekly or more	Ref		

Regarding ethnicity, being White was demotivating defensive internet behavior use as the odds associated with this group was lower than non-White internet users, although this association was not statistically significant at the 5 % confidence interval (OR = 0.90; 95 % CI: 0.41, 1.94). In the univariable analysis, ethnicity was not a statistically significant predictor of defensive behavior.

Regarding marital status, persons who identified as married had higher odds of turning to defensive behavior than single persons, although this association was not statistically significant at the 5 % confidence interval (OR = 1.64; 95 % CI: 0.92, 2.93). Also, separated respondents had significantly higher odds of turning to defensive behavior use than single persons (OR = 4.57; 95 % CI: 1.30, 16.10). However, respondents in common-law unions had lower odds of resorting to defensive behavior than single respondents, although this association was not statistically significant at the 5 % confidence interval (OR = 0.80; 95 % CI: 0.40, 1.59). Like the married and separated, the widowed had higher odds of resorting to defensive internet behavior than single persons, although this association was not statistically significant at the 5 % confidence interval (OR = 2.48; 95 % CI: 0.68, 9.06). Overall, in the univariable analysis, marital status was a statistically significant predictor of defensive behavior; while being married, separated, and

widowed was encouraging, being in a common-law union discouraged defensive internet use behavior.

Regarding family income, persons who annually made less than $50,000 had higher odds of turning to defensive behavior than persons who made more than $125,000, although this association was not statistically significant at the 5 % confidence interval (OR = 1.29; 95 % CI: 0.64, 2.63). On the contrary, the odds of resorting to defensive behavior among persons who annually made between $50,000 and less than $75,000 was lower than persons who made more than $125,000 per annum, although this association was not statistically significant at the 5 % confidence interval (OR = 0.77; 95 % CI: 0.39, 1.51). Similarly, persons who made between $75,000 and $125,000 had lower odds of resorting to defensive behavior than persons earning more than $125,000 per annum, although this association was also not statistically significant at the 5 % confidence interval (OR = 0.94; 95 % CI: 0.50, 1.79). Overall, family income was not a statistically significant predictor of defensive behavior in the univariable analysis. While incomes of less than $50,000 were encouraging, incomes between $50,000 and $125,000 discouraged defensive behavior use.

In terms of employment status, employed persons had lower odds of turning to defensive behavior use than those not employed, although this association was not statistically significant at the 5 % confidence interval (OR = 0.70; 95 % CI: 0.43, 1.14). Overall, employment status was a statistically significant predictor of avoidance behavior in the univariable analysis, while being employed discouraged defensive internet use behavior.

Regarding victimization experience, persons victimized in the past year had higher odds of resorting to defensive behavior than those not, although this association was not statistically significant at the 5 % confidence interval (OR = 1.22; 95 % CI: 0.67, 2.23). Similarly, not being

sure about victimization status encouraged defensive behavior use because the odds associated with this group were higher (by twice) than persons not victimized, although this association was not statistically significant at the 5 % confidence interval (OR = 2.05; 95 % CI: 0.88, 4.76). Overall, victimization experience was a statistically significant predictor of defensive behavior in the univariable analysis. The two victimization experience groups, relative to the reference group, both encouraged defensive internet use behavior.

Regarding cybercrime incident reporting, persons who were very likely to report an incident had higher (almost thrice) odds of resorting to defensive behavior than persons who were very unlikely to report, although this association was not statistically significant at the 5 % confidence interval (OR = 2.81; 95 % CI: 0.83, 9.48). Also, the odds of resorting to defensive behavior associated with persons who were likely to report an incident of cybercrime were higher than persons who were very unlikely to report, although this association was not statistically significant at the 5 % confidence interval (OR = 2.38; 95 % CI: 0.72, 7.89). Similarly, persons who were unlikely to report a cybercrime incident also had higher odds of turning to defensive behavior than persons who were very unlikely to report, although this association was not statistically significant at the 5 % confidence interval (OR = 2.92; 95 % CI: 0.79, 10.81). Overall, cybercrime incident reporting was not a statistically significant predictor of defensive behavior in the univariable analysis, while all the reporting levels, relative to the very unlikely to report, were encouraging defensive internet use behavior.

Regarding knowledge of risk, having an excellent knowledge of risk was encouraging defensive behavior because the odds associated with this awareness were higher than having poor knowledge, although this association was not statistically significant at the 5 % confidence interval (OR = 2.71; 95 % CI: 0.84, 8.76). Persons with a good knowledge of risk had

significantly higher odds of resorting to defensive behavior than those with poor knowledge (OR = 2.32; 95 % CI: 1.05, 5.12). Also, persons with a fair knowledge of risk had higher odds of resorting to defensive behavior than those with poor knowledge, although this association was not statistically significant at the 5 % confidence interval (OR = 1.83; 95 % CI: 0.86, 3.89). Overall, knowledge of cybercrime risk was a statistically significant predictor of defensive internet use behavior in the univariable analysis. All the levels of risk knowledge, relative to poor knowledge, encouraged defensive internet use behavior.

In terms of internet use frequency, persons who use the internet once daily had higher odds of resorting to defensive behavior than persons who use the internet weekly or more, although this association was not statistically significant at the 5 % confidence interval (OR = 3.09; 95 % CI: 0.65, 14.62). Likewise, using the internet several times a day was encouraging defensive behavior, as the odds associated with this usage were higher than weekly or more use of the internet, although this association was not statistically significant at the 5 % confidence interval (OR = 2.89; 95 % CI: 0.76, 11.03). Overall, the frequency of internet use was not a statistically significant predictor of defensive behavior in the univariable analysis, while both levels of frequency of use, relative to the reference group, encouraged defensive internet use behavior.

5.5 Multivariable Analysis of Outcome Variables by the Predictors

The following sections present the multivariable relationship between predictor and outcome variables. Adjusted odds ratios (together with the corresponding 95 % confidence intervals) were used to describe the strength of the association and to determine statistical significance. A p-value cut-off of 0.05 was used to determine significant predictors of fear and

risk of cybercrime and avoidance and defensive internet use behaviors. The rest of this section is organized as follows: Subsections 5.5.1 and 5.5.2 describe the multivariable relationship between predictor variables and fear and risk of cybercrime victimization, respectively, while 5.5.3 and 5.5.4 describe the relationship between predictor variables and avoidance and defensive internet behaviors, respectively.

5.5.1 Multivariable Analysis of Fear of Cybercrime

In the multivariable analysis shown in Table 5.11, after controlling for other predictors, age, ethnicity, employment status, and victimization experience remained significant predictors for fear of cybercrime. In particular, persons aged 40-46 were associated with significantly lower odds of expressing fear of cybercrime than those aged 18-32 when all the other predictors were held constant in the multivariable model (OR = 0.43, 95 % CI: 0.22, 0.85). For ethnicity, the odd of expressing fear of cybercrime among Whites is almost doubled that of their non-White counterparts when all the other predictors were held constant in the multivariable model (OR = 1.96; 95 % CI: 1.05, 3.68), and that relationship is significant. Regarding employment, employed individuals were associated with almost twice the odds (statistically significant) of expressing fear compared with unemployed individuals in the current study (OR = 1.68; 95 % CI: 1.08, 2.62). Inconsistent with author expectations and the literature (Abdulai, 2020; Brands & Van Wilsem, 2021; Choi et al., 2021; Elhai et al., 2017; Lee et al., 2019; Virtanen, 2017), victimized persons in the past year were associated with significantly lower odds of fear of cybercrime than their counterparts with no such experience (OR = 0.34; 95 % CI: 0.21, 0.54) when all other predictors were held constant in the multivariable model. A similar significantly lower odds of expressing the fear of cybercrime was observed for persons uncertain about being victimized in the past compared to those without victimization experience (OR = 0.49, 95 % CI: 0.27, 0.88).

Table 5.11

Final Multivariable Model Analysis – Associations between Fear of Cybercrime and Predictor Variables

Predictors	Outcome: Fear of Cybercrime		
	β (Standard error)	**Adjusted Odds Ratio (95% CI)**	**Multivariable *p*-value**
Socio-Demographics:			
Age			**0.01**
18-32	Ref		
33-39	0.36 (0.33)	1.43 (0.75, 2.71)	0.28
40-46	-0.84 (0.35)	0.43 (0.22, 0.85)	0.02
47-52	-0.26 (0.34)	0.77 (0.40, 1.49)	0.44
53 and older	-0.43 (0.29)	0.65 (0.37, 1.14)	0.13
Gender			0.52
Male	-0.12 (0.19)	0.89 (0.61, 1.28)	0.52
Female	Ref		
Ethnicity			**0.04**
Non-white	Ref		
White	0.68 (0.32)	1.96 (1.05, 3.68)	0.04
Employment status			**0.02**
Employed	0.52 (0.23)	1.68 (1.08, 2.62)	0.02
Not employed	Ref		
Other Predictors:			
Victimization experience			**<0.001**
Yes	-1.09 (0.25)	0.34 (0.21, 0.54)	<0.001
Not sure	-0.71 (0.30)	0.49 (0.27, 0.88)	0.02
No	Ref		

5.5.2 Multivariable Analysis of Risk of Cybercrime

In the multivariable analysis for the risk of cybercrime, as shown in Table 5.12, after controlling for other predictors, gender, education, marital status, and experience of victimization remained significant predictors for the risk of cybercrime. Notably, male internet users had higher odds of perceiving the risk of cybercrime than female internet users when all the other predictors were held constant (OR = 1.17, 95 % CI: 0.73, 1.89). For education, the odds of

perceiving risk among internet users without a university education were significant and more than twice that of their counterparts with a minimum of university education when all the other predictors were held constant (OR = 2.26, 95 % CI: 1.49, 3.44). As regards marital status, married persons had significantly lower odds of feeling at risk than their single counterparts (OR = 0.42, 95 % CI: 0.25, 0.71). Similarly, separated persons had reduced odds of feeling at risk compared to single persons though not significant (OR = 0.65, 95 % CI: 0.29, 1.48). Also, the odds of feeling at risk for persons in common-law unions were lower than their single counterparts, although it is not significant (OR = 0.79, 95 % CI: 0.43, 1.44). Equally, widowed persons' odds of feeling at risk were lower than single persons, although it is not significant (OR = 0.48, 95 % CI: 0.18, 1.24). For victimization experience, persons with prior experience were associated with a lower odd of feeling at risk of cybercrime than persons with no such experience when all other predictors were held constant in the multivariable model (OR = 0.91, 95 % CI: 0.46, 1.81). On the contrary, a higher odd of feeling at risk was observed among persons who were unsure about their victimization status than those without victimization experience (OR = 1.17, 95 % CI: 0.47, 2.92).

Table 5.12

Final Multivariable Model Analysis – Associations between Risk of Cybercrime and Predictor Variables

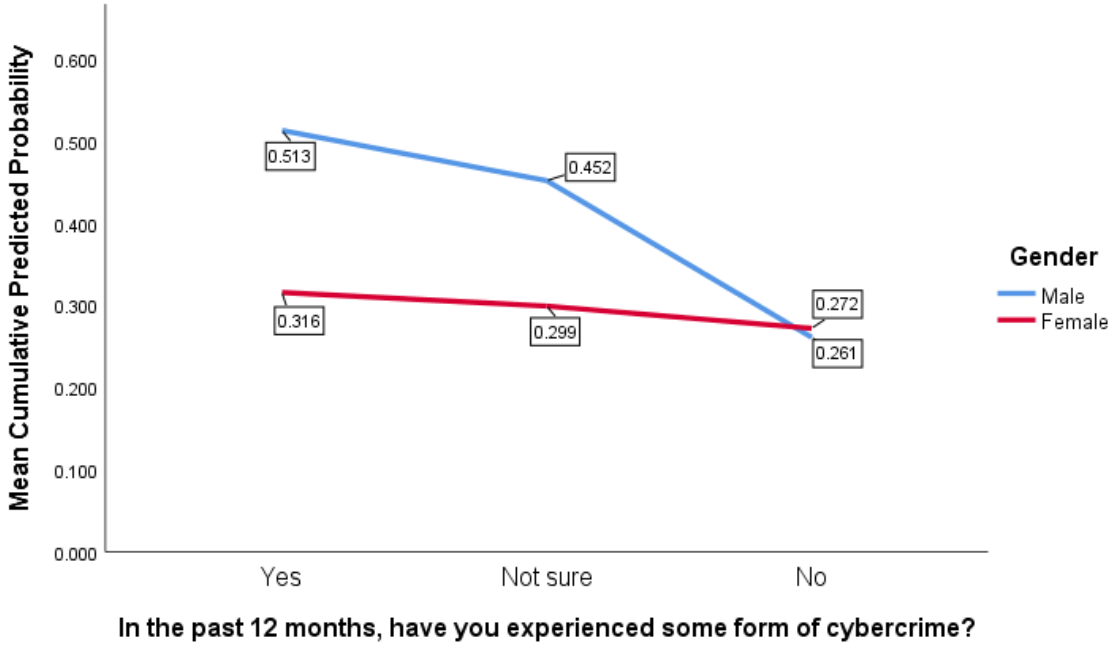
Predictors	Outcome: Risk of Cybercrime		
	β (Standard error)	**Adjusted Odds Ratio (95% CI)**	**Multivariable *p*-value**
Socio-Demographics:			
Age			0.13
18-32	Ref		
33-39	-0.69 (0.34)	0.50 (0.26, 0.98)	0.04
40-46	-0.46 (0.36)	0.63 (0.31, 1.29)	0.21
47-52	-0.60 (0.37)	0.55 (0.27, 1.14)	0.11
53 and older	-0.78 (0.31)	0.46 (0.25, 0.84)	0.01
Gender			**0.02**
Male	0.16 (0.24)	1.17 (0.73, 1.89)	0.51
Female	Ref		
Education			**<0.001**
Less than university	0.82 (0.21)	2.26 (1.49, 3.44)	<0.001
University and above	Ref		
Marital Status			**0.02**
Single	Ref		
Married	-0.87 (0.27)	0.42 (0.25, 0.71)	0.001
Separated	-0.43 (0.42)	0.65 (0.29, 1,48)	0.31
Common-law	-0.24 (0.31)	0.79 (0.43, 1.44)	0.43
Widowed	-0.74 (0.49)	0.48 (0.18, 1.24)	0.13
Other Predictors:			
Victimization experience			**0.04**
Yes	-0.09 (0.35)	0.91 (0.46, 1.81)	0.80
Not sure	0.16 (0.47)	1.17 (0.47, 2.92)	0.73
No	Ref		
Interaction:			**0.03**
Gender*Victimization			
Male * Yes	-0.91 (0.50)	0.40 (0.15, 1.07)	0.07
Male * Not sure	-1.41 (0.63)	0.24 (0.07, 0.84)	0.03
Ref			

Additionally, there was a statistically significant interaction between gender and victimization in feeling at risk of cybercrime. Specifically, victimized male internet users had

lower odds of feeling at risk (OR = 0.40, 95 % CI: 0.15, 1.07). Similarly, a significantly lower odd of feeling at risk of cybercrime was observed among male internet users who were unsure about being victimized (OR = 0.24, 95 % CI: 0.07, 0.84).

The plot in Figure 5.3 represents a schematic visualization of the significant interaction between gender and victimization in the multivariable risk model. In particular, the lack of parallelism in the profile plots indicates the significance between gender and victimization (C.I: 0.15, 1.07; and 0.07, 0.84; $p<0.05$).

Figure 5.3. Average Cumulative Predicted Probability Plot for Interaction between Gender and Victimization on Risk Perception



5.5.3 Multivariable Analysis of Avoidance Internet use Behavior

Table 5.13 shows the final multivariable model analysis results for avoidance internet use behavior. In the multivariable analysis for avoidance behavior, marital status and knowledge of cybercrime risk remained significant predictors of avoidance internet use behavior after controlling for other predictors. Concerning marital status, internet users who were married were associated with significantly higher (almost three times) odds of resorting to avoidance behavior than single users (OR = 2.75; 95 % CI: 1.59, 4.76). Similarly, being separated encouraged or incentivized avoidance behavior as the odds associated with this group was significantly higher than single users (OR = 3.88; 95 % CI: 1.51, 9.95). On the contrary, the odds of resorting to avoidance behavior associated with persons in common-law unions were lower than single persons, although not significant (OR = 0.91; 95 % CI: 0.48, 1.75).

Conversely, widowed internet users' odds of turning to avoidance behavior were significantly higher than single persons when all the other predictors were held constant (OR = 4.51; 95 % CI: 1.23, 16.59). As regards knowledge of risk, internet users with excellent knowledge of risk were associated with significantly lower odds of resorting to avoidance behavior when all the other predictors were held constant in the multivariable model (OR = 0.24; 95 % CI: 0.08, 0.72). Compared to users with poor knowledge of risk, users with good knowledge had lower odds of resorting to avoidance behavior, although the association failed to reach significance (OR = 0.76; 95 % CI: 0.33, 1.78). Equally, internet users with a fair knowledge of risk had lower odds of turning to avoidance behavior than users with poor knowledge, although the association was did reach significance (OR = 0.88; 95 % CI: 0.39, 2.01).

Table 5.13

Final Multivariable Model Analysis – Associations between Avoidance Behavior and Predictor Variables

Predictors	Outcome: Avoidance behavior		
	β (Standard error)	**Adjusted Odds Ratio (95% CI)**	**Multivariable *p*-value**
Socio-Demographics:			
Gender			0.68
Male	0.10 (0.24)	1.10 (0.69, 1.75)	0.68
Female	Ref		
Marital Status			**<0.001**
Single	Ref		
Married	1.01 (0.28)	2.75 (1.59, 4.76)	<0.001
Separated	1.36 (0.48)	3.88 (1.51, 9.95)	0.01
Common-law	-0.09 (0.33)	0.91 (0.48, 1.75)	0.79
Widowed	1.51 (0.66)	4.51 (1.23. 16.59)	0.02
Knowledge of cybercrime risk			**0.02**
Excellent	-1.44 (0.57)	0.24 (0.08, 0.72)	0.01
Good	-0.27 (0.43)	0.76 (0.33, 1.78)	0.53
Fair	-0.13 (0.42)	0.88 (0.39, 2.01)	0.76
Poor	Ref		

5.5.4 Multivariable Analysis of Defensive Internet use Behavior

Table 5.14 shows the final multivariable analysis for defensive internet use behavior. As Table 5.14 shows, in the multivariable analysis for defensive behavior, none of the predictors were significant predictors of defensive internet use behavior after controlling for other predictors. This result was achieved even after using the strongest univariable predictors as a reduced model after none of the hypotheses' related predictor variables qualified for the multivariable analysis (see notes under methodology).

Table 5.14

Final Multivariable Model Analysis - Associations between Defensive Behaviors and Predictor Variables

Predictors	Outcome: Defensive behavior		
	β (Standard error)	**Adjusted Odds Ratio (95% CI)**	**Multivariable *p*-value**
Socio-Demographics:			
Age			0.67
18-32	Ref	Ref	
33-39	-0.44 (0.40)	0.65 (0.30, 1.41)	0.27
40-46	0.06 (0.46)	1.06 (0.43, 2.61)	0.90
47-52	0.06 (0.45)	1.06 (0.44, 2.53)	0.90
53 and older	0.14 (0.39)	1.15 (0.53, 2.48)	0.73
Gender			0.81
Male	-.06 (0.26)	0,94 (0.57. 1.56)	0.81
Female	Ref		
Knowledge of cybercrime risk			0.25
Excellent	1.02 (0.63)	2.78 (0.80, 9.60)	0.12
Good	0.75 (0.42)	2.13 (0.93, 4.87)	0.08
Fair	0.48 (0.40)	1.62 (0.74, 3.57)	0.23
Poor	Ref	Ref	
Employment status			0.75
Employed	-0.10 (0.30)	0.91 (0.51, 1.63)	0.75
Not employed	Ref		
Marital Status			0.12
Single	Ref		
Married	0.44 (0.32)	1.56 (0.83, 2.91)	0.17
Separated	1.36 (0.67)	3.88 (1.05, 14.39)	0.04
Common-law	-0.17 (0.36)	0.84 (0.41, 1.71)	0.64
Widowed	0.83 (0.71)	2.29 (0.57, 9.30)	0.25
Victimization experience			0.45
Yes	0.11 (0.32)	1.11 (0.59, 2.10)	0.74
Not sure	0.56 (0.45)	1.76 (0.73, 4.21)	0.21
No	Ref	Ref	

5.6 Results of Hypotheses testing

The following section presents the results of the hypotheses based on the results from the preceding analysis. For each hypothesis, I make a declaration about the study position (outcome) and justify each using the traditional levels of significance as a threshold (i.e., p-value<0.05). In all cases, the outcome of each hypothesis is based on the results of multivariable modeling in sections 5.5.1 through 5.5.4. The exceptions are hypotheses 4 (a and b), 5, and 6 (a and b). I reference univariable model analysis for these hypotheses because the relevant variables did not qualify for inclusion in the final multivariable logistic regression models.

Table 5.15

Summary of hypotheses testing based on results

	Hypotheses	Study position	Justification
1.	Socio-demographic factors are associated with the risk of cybercrime victimization.	Partially supported	• Gender (*p*-value = 0.02) • Education (*p*-value = <0.001) • Marital status (*p*-value = 0.02) (See Table 5.12)
2.	Prior victims of cybercrime are expected to be more fearful of cybercrime than persons without victimization experience.	Not supported	• The odd for persons with victimization experience to express fear is significantly lower than the odds for those without such experience: (OR = 0.34; 95 % CI: 0.21, 0.54). (See Table 5.11)
3.	Prior victims of cybercrime are expected to perceive more risk of cybercrime than persons without victimization experience.	Not supported	• The odds for persons with victimization experience to perceive risk is lower than the odds for those without such experience: (OR = 0.91; 95 % CI: 0.46, 1.81). (See Table 5.12)
4.	Cybercrime victims are more prone to exhibit internet behavior constrain:		
	a) Cybercrime victims are more prone to resort to avoidance internet behaviors than non-victims of cybercrime.	Not Supported/ inconclusive	• In the univariable modeling, *Victimization* has 1.25 times higher odds of resorting to avoidance behaviors than non-victims, although this association was not significant: (OR = 1.25; 95% CI: 0.72, 2.16) (See Table 5.9) • *Victimization* did not qualify to be included in the final multivariable logistic regression model for *Avoidance behaviors* (i.e., the hypothesized relationship could not be assessed). (See Table 5.13)
	b) Cybercrime victims are more prone to adopt defensive	Not Supported/ inconclusive	• In the univariable modeling, *Victimization* has 1.22 times higher odds of engaging in

	Hypotheses	Study position	Justification
	internet behaviors than non-victims of cybercrime.		defensive behaviors than non-victims, although this association was not significant: (OR = 1.22; 95% CI: 0.67, 2.23) (See Table 5.10) • *Victimization* did not qualify to be included in the final multivariable logistic regression model for *Defensive behaviors* (i.e., the hypothesized relationship could not be assessed*).* (See Table 5.14)
5.	Cybercrime incident reporting is associated with fear of cybercrime.	Not Supported/ inconclusive	• Across all levels, incident reporting was associated with more than two times higher odd of expressing fear as compared to the reference category, although only the likely to report (OR=3.03; 95 % CI: 1.01, 9.06) category was statistically significant in the univariable relationship (See Table 5.7). The fear-incident reporting relationship could not be explored in the multivariable modeling stage since cybercrime incident reporting was not a candidate in the multivariable analysis stage.
6.	Frequent users of the internet are more inclined to exhibit internet behavior constrain:		
	a) Frequent internet users are more inclined to engage in avoidance internet behaviors than less- frequent users.	Not Supported/ inconclusive	• In the univariable modeling, frequent internet users (several times in a day usage) have higher odds (more than twice) of resorting to avoidance behaviors than less frequent users, although this association was not significant: (OR = 2.19; 95% CI: 0.54, 8.90) (See Table 5.9) • *Internet use frequency* did not qualify to be included in the final multivariable logistic regression model for *Avoidance behaviors* (i.e., the hypothesized

	Hypotheses	Study position	Justification
			relationship could not be assessed at the multivariable level*).* (See Table 5.13)
	b) Frequent internet users are more inclined to adopt defensive internet behaviors than less- frequent users.	Not Supported/ inconclusive	• In the univariable modeling, frequent internet users (several times in a day usage) had higher odds (more than twice) of resorting to defensive behaviors than less frequent users, although this relationship was not statistically significant at 5 %: (OR = 2.89; 95 % CI: 0.76, 11.03) (See Table 5.10) • *Internet use frequency* did not qualify to be included in the final multivariable logistic regression model for *Defensive behaviors* (i.e., the hypothesized relationship could not be assessed at the multivariable level*).* (See Table 5.14)

5.7 Analyzed Conceptual Framework

In this section, I present the outcome of the conceptual framework following the multivariable analysis. Table 5.16 presents the summary of the results of the conceptual framework from the multivariable analysis and shows outcomes in terms of significant and non-significant associations. Figure 5.4 shows the analyzed conceptual framework. The study variables are enclosed in oval shapes and occupy the framework's middle block in the analyzed framework. The solid thick blue line arrows indicate the paths of significant associations between variables, while the broken solid thick blue line arrows indicate partial associations. In

this way, the arrow connecting victimization experience (VExp.) to the risk of victimization (RCV) shows a significant association between the two variables.

In contrast, the broken line arrow linking socio-demographic factors (SDF) to fear of cybercrime victimization (FCV) demonstrates a significant partial association between the two variables. Also, the solid thick blue double line arrows indicate an interaction between variables. Accordingly, the solid thick double line arrow between SDF and VExp shows an interaction between social demographic factors and victimization experience. The two rectangles with rounded corners at the extremes of the framework represent the building blocks of the current study. That is, internet use and its consequences manifested as cybercrime. Finally, the study variables in the middle of the framework all relate to the targets of the study, internet users, who can either be victims or potential victims of cybercrime or both.

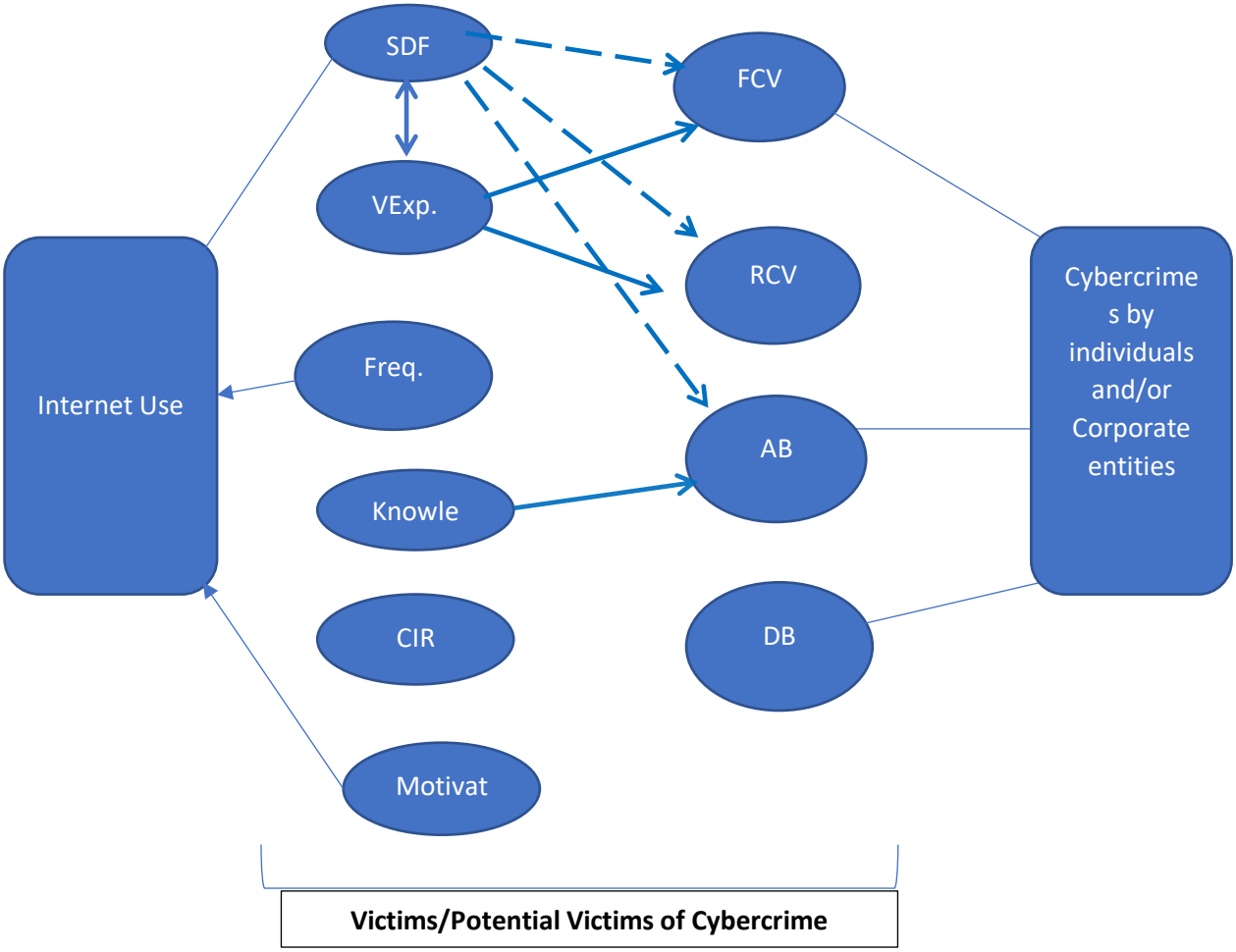
Table 5.16

Summary of Analyzed Conceptual Framework based on Results of Multivariable Analysis

Predictors	Outcomes			
	Fear	**Risk**	**Avoidance Behavior**	**Defensive Behavior**
Socio-demographic				
Age	**S***	NS	NS	NS
Gender	NS**	**S**	NS	NS
Education	NS	**S**	NS	NS
Ethnicity	S	NS	NS	NS
Marriage	NS	S	**S**	NS
Family income	NS	NS	NS	NS
Employment	**S**	NS	NS	NS
Other predictors				
Victimization Experience	**S**	**S**	NS	NS
Cybercrime Incident Reporting	NS	NS	NS	NS
Knowledge of Cybercrime Risk	NS	NS	**S**	NS
Frequency of Internet Use	NS	NS	NS	NS

*S = Significant **NS = Not Significant

Figure 5.4. Analyzed Conceptual Framework



Chapter Six: Qualitative Data Analysis of Motivations of Internet Use

6.0 Introduction

The following sections present a qualitative analysis of data about people's motivations for using the internet, and it is pertinent to the research question: what are the motivations for internet use among Canadian adults? In the first section, I describe the socio-demographic profile of the participants who answered the question about internet use motivation. Next, I describe the complete coding and theme development process and present a table of the thematic network of codes and organizing themes. I follow this in the next section by offering a thematic analysis of the qualitative data from participants' responses. The main themes include education and knowledge acquisition, entertainment and fun, communication and social media access, commercial purposes, work and personal-related use, and news and information access. I present the summary and conclusion in the final part, which prepares the reader for the subsequent chapter.

6.1 Socio-demographic profile of study participants

A total of 309 participants responded to the question about motivation for internet use. As shown in Table 6.1, more than half (158) were female, and the majority (125) were aged 53 and over. Also, more than half (162) of the participants had less than a university education, and an overwhelming majority (277 and 138 participants) identified as White and married, respectively.

Responses were number P1-P309, each row of response considered as a single participant. Of this number, 12 responses were deemed invalid since they did not make any

meaning, bringing the total number of valid participant responses to 297. See Appendix C for the extracted raw qualitative data wherein invalid responses have been highlighted in red.

Table 6.1

Summary of Socio-demographic profile of qualitative responses

Socio-demographic	Category	Frequency	Total
Gender	Male	146	304
	Female	158	
Age	18-32	57	307
	33-39	47	
	40-46	38	
	47-52	40	
	53 and over	125	
Education	Less than university	162	308
	University and higher	146	
Ethnicity	White	277	309
	Non-white	32	
Marital status	Single	72	308
	Married	138	
	Separated	31	
	Common-law	48	
	Widowed	19	

Source: Field Data, 2022

6.2 Coding and theme development process

A systematic and orderly coding framework and theming process were used in the thematic analysis. The specific ordered steps which were carried out are presented in the following bullet points:

- The qualitative data from SPSS was extracted.

- A preliminary scanning of participant responses about their motivations for internet use occurred.
- Responses were numbered P1 – P309, each response row representing a participant.
- Responses in French were translated into English using Google Translate.
- Keywords and phrases were identified – this was done after re-reading participant responses.
- Keywords and phrases were used to generate initial codes.
- Codes were grouped into categories and organized into themes to reflect the overarching motivations of Canadian internet users.

Table 6.2 shows the thematic network, revealing the basic codes, the accompanying issues discussed under each, and the associated organizing themes generated after the stepwise coding and theming process. It demonstrates the flow of the theming process (thematic analysis) from the basic codes to the organizing themes.

Table 6.2

Thematic Network of Codes and Themes

Basic codes	Issues discussed within codes	Organizing theme
- Research - For teaching - Online schooling - Online classes - Education - Learning new languages - Reading articles - Writing - Surveys - Searching for information - E-books etc.	• Internet use for research • Internet use for teaching • Internet use for studies • Language acquisition	Education and knowledge
- Netflix - YouTube - Videos - Music - For fun - Personal amusement - Play games - Podcasts - For pleasure - Sports - Watching concerts - Leisure etc.	• Internet use to watch films • Internet use to listen to music • Internet use for pleasure • Internet use to watch sporting activities	Entertainment and fun
- Communication - Social relations - Social networking - Social connections - Social media - Facebook - Twitter - Keeping connected with families, friends, relatives, co-workers - Family contacts	• Internet use for communication with family, friends, co-workers • Internet use for social networking • Internet use for social media • Internet use to maintain social and professional contacts	Communication and social media access

- Skype for correspondence - Microsoft Teams etc.		
- Banking - Business - Financial transactions - Online shopping - Buying groceries - Checking adverts - Credit card statements - Commerce - E-commerce - Stock markets - Paying bills	• Internet use to complete financial transactions • Internet use for stock trading • Internet use for shopping • Internet use for bill payments	Commercial purposes
-Work - Work from home - Personal work - Meetings - Social distancing - Covid-19 - Job search - Job application - Plan or book vacations	• Internet use for work • Internet use for meetings • Internet use for job search and application • Internet use to plan and book vacations	Work and personal use
- News - Newspapers - TV news - TV streaming - Google maps - Checking the weather - Searching for recipes	• Internet use to access news • Internet use for weather updates • Internet use for googling maps and driving directions	News and information access
- Easy to use - Accessibility - Easy access - Convenience - Convenient - Cheap - Effective - Quick to use - Free - Opinion polls etc.	• Internet use for general and overlapping purposes.	Other uses

6.3 Thematic Analysis of Qualitative data

The main qualitative themes developed from this data set are shown in Figure 6.1 and discussed in sections 6.3.1 through 6.3.7. Note that content analysis was not employed because a participant could have mentioned several uses of the internet that belong to one content category, thereby preventing a simple frequency count. Such a situation would have resulted in incomprehensible frequency tables/graphs. For example, participant P248 stated that they use the internet "To do personal business, to keep in touch with friends and family, to watch shows, to listen to music, to play games." With this response, activities such as *watching shows, listening to music,* and *playing games* will all fall under the theme of Entertainment and having fun. This illustration shows that having a frequency table where Entertainment, Education, Communication, Commercial, etc., are the main frequency categories would not provide an accurate picture of the various internet uses among participants. Additionally, thematic analysis was used to elicit broader themes that captures a broader variety of responses. Hence, the following themes emerged as being informative:

Figure 6.1. Analyzed Motivations for Internet Use

6.3.1 Theme 1 - Education and knowledge acquisition

The theme of education and knowledge acquisition explicate how people use the internet for research purposes, including for conducting surveys, accessing journal articles for reading and writing in their research, or engaging with specific software. Respondents in this study also used the internet to learn new languages, for online teaching and classes, to keep informed on current events and trends, or to access and read e-books. Hence, the theme of education and

knowledge acquisition summarizes how the internet provides a platform for exploration and innovation and affirms why some people are drawn to it. This theme appears consistent with the realities of the current technological era, where the traditional medium of teaching and learning in the classroom and hard copy prints has given way to a hybrid form. Some examples of words and phrases from respondents in the study that denote education and knowledge acquisition use of the internet are outlined below. Specific words and phrases that exemplify the themes are underlined [my emphasis].

- "I am doing genealogy research for a genealogy site" (*Participant P159*)
- "Stay connected to international things like friends and news, Computer research, Teaching and getting council online" (*Participant P231*)
- "Streaming Netflix, YouTube, e-mails, learning languages" (*Participant P234*)
- "To communicate with friends, e-books, online banking Purchases from known companies and e-mail" (*Participant P246*)
- "Why do you post your surveys for responses on the internet instead of randomly accosting strangers on the street corner for input?" (*Participant P273*)

The wide variety of educational and knowledge acquisition uses that respondents offered are closely inextricable from the pervasiveness of technology and the increasing role it plays in structuring daily lives. Given the speed and frequency at which trends and processes that are critical to daily change, it is vital to have research skills and to acquire new knowledge. The internet connects individuals to knowledge sources, culture, trends and emerging processes which are essential for navigating current lives. Connected with the education and knowledge acquisition is motivation, which has intrinsic and extrinsic sources: the intrinsic dimension links to internet users' curiosity or desire to acquire knowledge and the extrinsic dimension relates to

actors' studies and work needs. Both dimensions are external to actors. The theme also has structure and agency dimensions, as shown in Figure 6.1. Actors' need for exploration and innovation underlines their active agency to utilize technology to desired ends. The influence of structure is equally manifest: the demands of school, work (as depicted by research purposes), conducting surveys, and online teaching represents structure and its determining role or effect on the choices and actions of actors. Crucially, respondents quote imply that the activities are required and unavoidable for people; hence, people are motivated or required to use the internet for these purposes in spite of perceived risks and fear of cybercrime. In other words, the perceived risk of victimization associated with the internet relative to the "need" to use the internet means people are not deterred from the latter. Additionally, because people use the internet for required and unavoidable activities, it means less regard for avoidance and defensive internet use behaviors. Therefore, this motivational theme of internet use is in sync with the theoretical and conceptual discussion in the current study, which recognizes a significant role of structure and agency in the construction of socio-technological actions. Future studies can explore the possibility of correlating these responses with the perception of risk, fear of cybercrime, avoidance internet use, and defensive internet use.

6.3.2 Theme 2 - For entertainment and having fun

The internet is a significant source of entertainment for most of the study's participants (internet users). Respondents indicated that Netflix and YouTube were most frequently accessed to watch videos, movies, concerts, and play music. Some respondents used the internet for personal amusement or enjoyment, including watching adult content videos, sports, and playing games. Other participants indicated that they use the internet for leisure, among other activities. Reflecting on the varying perspectives given by respondents, this motivational theme for internet

use reflects the various dimensions of entertainment, each motivating an individual's decision to use the internet. Some selected words and phrases from respondents that convey the motivational theme of entertainment and having fun are underlined [my emphasis] in the following extracts.

- "Research and leisure" (*Participant P216*)
- "…, to watch videos and listen to music" (*Participant P244*)
- "… to amuse myself [entertainment], to shop" (*Participant P256*)
- "YouTube, Netflix [entertainment], banking …." (*Participant P266*)
- "… for amusement; to take online classes or watch concerts, shows, etc." (*Participant P108*)

The theme of entertainment and having fun emanate from intrinsic and extrinsic sources: actors and society. This is because entertainment and fun correspond with internet users' need for leisure, fun and relief from boredom, facets that lie at the individual or micro and macro levels of social reality. Latently, however, there is also an element of extrinsic source to this motivation. Western societies' socio-cultural and technological landscape foster individualism, unlike in developing societies. Therefore, internet users' motivation to access the internet for entertainment and relief from boredom may be a way of responding to the individualized and, at times, isolating environment they inhabit.

Accordingly, the theme is both agential and structural, as indicated in Figure 6.1: Internet users access the internet and other technology tools at times and places of their choice for essentially utilitarian ends conditioned by society. Entertainment is becoming a basic need in modern social culture; hence individuals might forego the risk of online victimization to satisfy their personal entertainment "need." While foregoing risk to satisfy their need for entertainment,

people may choose from many defensive internet use strategies, such as enhanced anti-virus software and multi-factor authentication, to enhance the satisfaction of their needs. Conversely, people will pay less regard to avoidance internet use actions, such as outright avoidance of certain websites, since that might constrain the realization or maximization of their needs. Accordingly, culture and the constraints of modern social life exemplify a unique interplay between structure and agency. In this way, even as social culture structures what kind and how entertainment is offered, individuals exercise their agency in selecting from the plethora of options, and the kind of defensive strategies (if any) that they adapt to manage perceived risks. Hence, it is consistent with the structure and agency perspective in the structure and agency debate.

6.3.3 Theme 3 - Communication and social media access

The theme of communication and social media access encompasses using the internet to maintain the connection with family, friends, and relatives using Facebook, Twitter, WhatsApp, and or Skype. Other activities connected with this theme included using the internet for social networking, socialization, and correspondence. During the COVID-19 pandemic, most participants used social media apps and platforms to communicate and connect with their social relations. However, a surprising finding is that among the 309 participants who answered this question, none has stated using the internet for online dating, which was a surprise, given the pervasiveness of online dating apps in most developed countries, including Canada (Chen et al., 2021; Qian, 2021; Schwartz & Velotta, 2018). Nonetheless, I acknowledge that participants could have hidden this particular internet usage motivation under the social connections or social networking categories. In addition, without prompts, respondents might just not have thought about it.

A selection of words and phrases from respondents that convey the overarching idea in the theme are underlined [my emphasis] in the following extracts.

- "To communicate with my relatives and friends" (*Participant P198*)
- "Talk to family 4000 km away [social connection] …" (*Participant P237*)
- "It is how we communicate with companies, friends, and the world ..." (*Participant P237*)
- "... To communicate with family and friends as I can see them on my screen" (*Participant P200*)
- "The internet is my primary method to communicate with co-workers, customers, friends, and family" (*Participant P242*)

Viewed in the context of the theoretical discussion, the motivational theme of communication and social media access reflects elements of structure and agency, as reflected in Figure 6.1. Even though individualism has taken hold in the technological era, which has ushered in the risk society, social and familial bonds are still maintained through tools of technology. In a feat of agency, internet users, through social media, used the internet to connect and keep family and social relationships. Meanwhile, family and social institutions represent components of social structure. Thus, structure and agency again patterned internet users' motivations and decisions to access the internet. It is important to note that even in an individualistic culture, the need for social connection remains strong, motivating respondents to intentionally mediate relationships virtually.

This theme implies that people rationalize risk to meet their communication and social media access needs. In other words, the perceived "needs" of communication and social media

access see people justifying the risk of cybercrime to access the internet. People might project the risk of victimization in cyberspace to be nonexistent or minimal if it does exist. Similarly, the strategies of risk rationalization imply people might disregard avoidance internet use activities while considering some defensive internet use activities to meet their communication and social media access needs. Future studies might also consider correlating these responses with perceived risk, fear, avoidance, and defensive internet use.

6.3.4 Theme 4 - Using the internet for commercial purposes

The motivational theme of using the internet for commercial purposes includes using the internet for online banking, shopping, making purchases (e.g., groceries, stocks), and other business transactions. Some participants used the internet to pay bills, access credit card statements, to check store flyers, for investment purposes, or to monitor business advertisements on companies' websites. Other participants used the internet to buy drugs, pharmaceutical products, casino activities, and e-commerce. In other words, this theme suggests that people's need for banking, shopping, and payment of bills, among others, becomes a motivation for them to use the internet. In the reality of the current technological era, characterized by its fast pace, using the internet for these needs is convenient. The internet has evolved into a tool that facilitates people's daily life.

Some examples of words and phrases from respondents that reflect motivational theme 4 include the following quotes with the relevant words, phrases, and sentences underlined [my emphasis].

- "… shopping due to covid-19 [sic], find deals on marketplace" (*Participant P237*)
- "To find information and [pay] online bills" (*Participant P249*)

- "... For online shopping - sometimes items are only available online. To receive and pay the bills because it costs a fee to have them in the paper by mail, so I have no choice" (*Participant P200*)
- "… online banking, purchases from known companies and e-mail" (*Participant P246*)
- "Stock market trading information through Google" (*Participant P232*)

The activities or codes identified under the theme of commercial use motivation suggest a sense of inevitability about using the internet. The activities are so linked with people's everyday lives that they cannot hold back, irrespective of the risk and fear of cybercrime. Equally, the sense of unavoidability of the internet will signify an inclination to some defensive internet use behaviors with less regard for avoidance internet use. Risk rationalization strategies will be a convenient coping strategy for internet users in such a situation.

Banking, shopping, health, and business – that is, commercial – landscapes are structural with a pre-determined or set operational logic. These influence how internet users relate to them; hence, its source is extrinsically motivated. Conversely, internet users' access of the internet platform rather than walking into brick-and-mortar spaces for commercial transactions is an invitation to actor agency. Here too, structure and agency are crucial and intersect at the node of commercial use motivation for internet users' access to the internet, as Figure 6.1 shows; thus, it is consistent with the theoretical discussion.

6.3.5 Theme 5 - Work and personal related use

The ongoing COVID-19 lockdowns and restrictions have made the internet the most active channel for work-from-home purposes. Other internet functions under this motivational theme included checking emails, planning trips and vacations, volunteer activities, job search

and applications, and social/physical distancing due to COVID-19. Under this theme, participants' activities point to the interconnectedness of the internet to professional and work life. The COVID-19 pandemic further increased the salience of the internet for some work-related activities. Selected direct quotes from respondents to the effect of the above theme include the following extracts [underlined to show my emphasis]:

- "Send and receive an e-mail." (*Participant P225*)
- "Work, email, personal communication … " (*Participant P293*)
- "Work, social outreach due to COVID-19 …" (*Participant P305*)
- "I work in computer science, necessary for my job" (*Participant P261*)
- "Working, working remotely, finding information, recipes/cooking, …" (*Participant P264*)

Work and personal use motivation for internet use also suggest intrinsic and extrinsic roots. Whereas work relates to the extrinsic source dimension, personal related-use links to the intrinsic component. The demands of work structures people's use of the internet, especially during the COVID-19 pandemic era while people also resort to the internet for personal uses in a demonstration of agency. Perceived risk and the fear of victimization might impact work and personal use motivation. In the pre-COVID-19 world, where remote work was the exception rather than the rule, perceived risk and fear could have meant people shunned or minimized their internet use for work and personal activities. However, with the advent of the COVID-19 pandemic, internet use for work and personal needs has become unavoidable, a necessity irrespective of perceived risk and the fear of cybercrime. In this new reality, some options available to people include rationalizing risk and or incorporating defensive internet use strategies.

.

6.3.6 Theme 6 - For news and information access

The motivational theme of news and information access, which may intersect with other themes, has functions of the internet to include the following: for reading newspapers, checking weather information and updates, finding driving directions, checking online recipes, perusing Television (TV) news, accessing Google Maps, and searching Wikipedia guides. Many participants used the internet to keep them informed about happenings in the country and around the globe. They needed for example, to keep themselves informed about COVID-19 updates, the economy, the weather, and any news necessary for their daily lives and activities. This theme suggests that the internet's traction in people's lives is linked to one of news, accessing information, or both. In terms of information and news, people no longer have to obtain paper prints of newspapers and magazines, as e-copies of these are readily available on the internet. Beyond newspapers and magazines, the internet is also awash with digital news platforms. Thus, the internet's fluidity motivated some participants' use of the internet in this study.

Some examples of words and phrases from respondents in the data that denote the above theme include the following quotes with the relevant words and phrases underlined [my emphasis].

- "Research on different subjects, information, listening to radio, music, podcast" (*Participant P217*)
- "Reading news and research information," (*Participant P212*)
- "To obtain information …" (*Participant P254*)

- “Free access to media (daily newspapers, TV networks) and other information sources (Wikipedia, Meteor Media, Google Maps)” (*Participant P6*)
- “Because I'm housebound most of the time due to COVID-19, I use the internet for Google searches, online shopping, and news via CBC, CTV, and CNN. Also, Facebook, see what my family and friends are up to ...” (*Participant P21*)

This motivational theme is replete with structure trappings and is extrinsically inspired. The central idea around the theme is information access. Meanwhile, internet users do not control the information nor the outlets and institutions that provide it. As such, news and information access constitute the element of structure that influences or patterns internet users' actions in their desire to access it. Since information and its sources are external to internet users, it implies that this motivation is extrinsically sourced. In effect, structure plays the overriding role under this theme, as Figure 6.1 shows, and thus aligns with the structure perspective of the structure and agency debate.

The underlying logic in this theme is convenience in information access. Even though people do not control the information, the outlets, and institutions, they have a choice in choosing between diverse media – traditional and digital platforms. The risk of victimization and fear of cybercrime may influence people’s choices, most likely in favor of traditional media. However, the situation will likely change when one factors convenience into the picture. People may tend to rationalize risk to take advantage of the convenience offered by the internet. Such rationalization may also mean more defense and less avoidance internet use.

6.3.7 Theme 7 - Other uses of the internet

This theme captures other internet uses that could not readily be categorized under any of the above themes. Thus, according to the participants in this study, other internet uses included ease of access or use, convenience, accessibility, quick and free, and cheap or effective. One participant indicated utilizing the internet for political reasons, that is, monitoring opinion polls. Together, the words and phrases under this category of internet use motivations reflect an interaction between structure and agency and their motivation through intrinsic and extrinsic sources. For some of the responses, it was impossible to delineate agency and structure.

6.4 Summary and Conclusion

In this chapter, I have presented the qualitative thematic analysis of Canadian internet users' motivations for using the internet. The analysis provided a breakdown of the socio-demographic characteristics of participants, including their gender, age, education, ethnicity, and marital status. They also revealed the complete coding and theming process, from data extraction to grouping codes into organizing themes that project the overarching motivations of Canadian internet users.

Crucially, the analysis revealed the underlying motivational themes underscoring Canadians' use of the internet, thus answering the related research question about internet use motivation. These were education and knowledge acquisition, entertainment and fun, communication and social media access, commercial purposes, work and personal-related use, news and information access, and other uses. Each motivational theme embodied elements of either structure, agency, or both, once again revealing the salience and interaction between structure and agency in human social action, including internet use. The analysis also examined

the connections between the motivational themes and perceived risk of victimization, fear of cybercrime, avoidance, and defensive internet use behaviors.

The next chapter will provide an analytical discussion of the results in line with the research questions.

Chapter Seven: Discussion

7.0 Introduction

This section provides a critical analysis of the research findings in relation to the literature. The discussion also examines the implication of the findings in terms of the theoretical and conceptual implications and relevance to policy and practice. In the first section, I discuss the study findings regarding socio-demographic factors and the risk of cybercrime, followed by victimization and fear of cybercrime in the next section. In the subsequent sections, I analyze the results regarding the association between cybercrime victimization experience and the fear of cybercrime, cybercrime victimization experience, and internet use constraint behavior, and between cybercrime incident reporting and fear of cybercrime. Next, I provide an analysis of the results regarding the relationship between internet use frequency and internet use behavior constraints. I follow this in the next section and discuss the results about motivations for internet use. In the final section, I discuss the implications of the results, presenting the theoretical and practical implications.

7.1 Socio-demographic factors and risk of cybercrime victimization

Based on the results from the multivariable analysis in this study, hypothesis one – socio-demographic factors are associated with the risk of cybercrime victimization – is partially supported. Out of seven socio-demographic factors included in this study, only gender (p-value = 0.02), education (p-value <0.001), and marital status (p-value = 0.02) were found to be significant. Regarding gender, male internet users were likelier to perceive (higher odd) the risk of cybercrime than female internet users. For education, internet users without university education had significantly higher odds of perceiving the risk of cybercrime than their

counterparts with a minimum university education. The odds for users without university education were more than twice that of the reference group (OR = 2.26). In terms of marriage, married internet users had significantly lower odds of perceiving the risk of cybercrime than single users (OR = 0.42, 95 % CI: 0.25, 0.71).

The partial support finding for socio-demographic factors' effect on the risk of victimization is consistent with some of the prior literature (Garbarino & Strahilevitz, 2004; Liebermann & Stashevsky, 2002; Reisig et al., 2009). In their study, Reisig et al. (2009) found that race and class association were significantly associated with the risk of cybercrime, while gender and age had no significant effect. They found that minorities and lower SES persons perceived higher levels of risk, whereas women and older persons did not perceive higher risk judgments than men and younger persons, respectively (Reisig et al., 2009, p. 377). On their part, whereas women reported higher levels of the perceived risk of online credit card use than men, there was no difference between older and younger persons' risk perception (Garbarino & Strahilevitz, 2004, p. 771).

In their study of the risk of victimization, Liebermann & Stashevsky (2002) found partial support for the effect of gender, age, marriage, and education on the risk of cybercrime. Women reported significantly higher levels of perceived risk associated with internet use in the elements of "internet credit card stealing," "pornography and violence," and "missing the human side in internet purchases" than men (Liebermann & Stashevsky, 2002, p. 297). In comparison, older people had significantly higher risk perception than their younger counterparts in the aspects of "supplying personal information," "pornography and violence," "missing the human side in internet purchases," and "internet usage addiction" (Liebermann & Stashevsky, 2002, p. 297). Additionally, they found that the married had significantly higher risk perception about the

internet than the unmarried in the elements of "supplying personal information," "pornography and violence," "information reliability," "missing the human side in internet purchases," and "internet usage addiction" (p. 297). Also, respondents with non-academic education had significantly more risk perception about the internet than academically educated persons in the elements "lack of physical contact," "missing the human side in internet purchases," and "internet usage addiction" (Liebermann & Stashevsky, 2002, p. 298). In effect, these studies found that some socio-demographic variables influenced cyber-risk perceptions, thus, in accordance with the current findings.

Despite the consistency in the overall finding of partial support, there is a notable difference between the current study and some prior literature. While gender is significant in the present study and Garbarino's and Strahilevitz's (2004) research, it is non-significant in Reisig et al.'s (2009) and partially significant in Liebermann's and Stashevsky's research (2002). Even with studies that also found a significant effect on gender, there is a difference in the direction. Whereas in this study, male internet users were associated with significantly higher odds of perceiving risk, the opposite – women report heightened levels of the perceived risk of online purchasing – was true in Garbarino's and Strahilevitz's study (2004). Also, whereas in the current study, marriage is significant, with married internet users having significantly lower odds of risk perception than single users, it is partially significant and in the opposite direction in Liebermann and Stashevsky (2002). However, education is significant in this study and partially significant but in the same direction as in Liebermann and Stashevsky (2002). These observed wide variations between the findings of the current study and those of the extant literature may be due to several factors, including the context of the studies, the sample, and methodology.

The finding of education in terms of its significance and direction on internet users' risk perception is noteworthy. All things being equal, better-educated internet users (respondents with a university or academic education) were more informed about the risk of victimization in cyberspace and the protective ways to minimize or guard against such risks. Such risk awareness need not be gained from direct firsthand experience of victimization; it can equally be gleaned vicariously through the experiences of others, either close associates or from reading from the media. In contrast, less educated internet users (those without university or non-academic education) were less likely to be informed about the risk of victimization, protective measures, or both. Conversely, their relatively low education means also that less-educated internet users were more inclined to overestimate the inherent risks of victimization in cyberspace.

Furthermore, the significant finding for education is also consistent with the theoretical and conceptual discussion in this study. Education aligns more closely with knowledge of risks, while the latter comprises the (external) structure of the internet. Recalling the discussion of structuration, structure comprises both rules and resources. Thus, the external structure comprising cyberspace or the internet platform generates rules and resources about the operations of the IT world. Accordingly, these rules and resources socialize and facilitate internet users' acquisition of internet use knowledge and perception of safety risks in cyberspace. Operating with the use knowledge and awareness of the risk profile in cyberspace – both gleaned from structure – through a feat of agency and reflexivity, educated internet users will feel less threatened because they can modify their online behavior accordingly. In sync with the theoretical discussion, an intricate interaction is visible between structure and agency regarding risk in cyberspace and internet users' projection of such based on the influence of education

(knowledge and awareness). Relative to educated internet users, less educated actors have reduced agency, which impedes their risk calculations of cybercrime.

However, the significant gender and marital status findings were surprising and appear at odds with the theoretical discussion. The nature of cyber risk and victimization means that factors such as gender and marriage are not expected to be decisive. Cybercrime occurs in the virtual realm, devoid of the physical meetings of (prospective) victims and their victimizers. People interact virtually, not necessarily knowing the other person from the other side. Socio-demographic identifiers such as gender and marriage are even less critical because cyberspace allows actors to anonymize their identities.

Moreover, the significant gender and marriage results suggest that actor agency is gendered and sensitive to marriage. However, this is further from the theoretical discussion. Actors are accorded agency regarding their roles in the construction of social action, irrespective of their socio-demographic identification.

7.2 Victimization experience and fear of cybercrime victimization

According to the results of the multivariable analysis in this study, the hypothesis that prior victims of cybercrime are expected to be more fearful of cybercrime than persons without victimization experience is not supported (p-value<0.001). That is, there is not enough evidence to support the statement that victims of cybercrime are more fearful of cybercrime than non-victims. On the contrary, according to this study, internet users with prior cybercrime victimization experience were associated with significantly lower odds of expressing fear of cybercrime than users without such experience (OR = 0.34, 95 % CI: 0.21, 0.54). The current finding is in line with Elhai and Hall's (2016) study about data breach anxiety. In their research,

Elhai and Hall (2016) found that none of the prior cybercrime victimization incidents (indicated as previous hacking incidents) experienced by respondents had a significant relation to current data breach anxiety regarding fear of cybercrime (p. 183). In other words, prior hacking victimization was not significantly associated with fear of data breach anxiety. Unlike the current study, however, Elhai and Hall combined different emotional aspects – worry, anxiety, and stress – with various elements or forms of online breaches into a unique outcome measure called data breach anxiety.

Meanwhile, some findings in the prevailing literature are inconsistent with the current results. Some such studies, including Abdulai (2020), Brand and van Wilsem (2021), Choi et al., (2021), Elhai et al., (2017), Lee et al., (2019), and Virtanen (2017) made contrary findings to the effect of there being a significant positive association between victimization and fear of cybercrime. In his study of credit or debit card fraud, Abdulai (2020) found a significant positive relationship ($p<.01$, odds ratio = 3.246) between victimization and fear of cybercrime (p. 166). This implies that respondents with prior victimization experience were more fearful of credit or debit card fraud victimization. In their study of online financial crime, Brands and van Wilsem (2021) found that all victimization experiences – being hacked, being infected by a computer virus, and being defrauded online – were significantly positively related ($p<.001$) to fear of cybercrime (p. 224-225). Also, Choi et al. (2021) found a significant positive relationship between identity theft victimization and fear of identity theft victimization. Persons with prior identity theft victimization experience in the past year had 181 % (almost twice) higher odds of expressing heightened fear of identity theft victimization than persons without such experience (Choi, 2021, p. 418). Additionally, in Lee et al.'s (2019) study, they found that respondents who had experienced victimization on social network sites ($p<.001$) were more likely to fear

victimization on social network sites (p. 12), indicating a significantly positive association. These results tend to support the generally established finding regarding victimization and fear in the sphere of conventional crimes.

In another twist, the current findings also appear inconsistent with another dimension of results in the literature. In opposition to both the present findings and those suggesting a positive association, Henson et al. (2013) found an inconclusive relationship. They found positive, negative, and non-significant associations between victimization and fear (Henson et al., 2013). In their study, prior online victimization experience was statistically significantly related to fear of online interpersonal victimization by close relations, not strangers (p. 488). Specifically, they reported "a significant and positive relationship between direct victimization and fear of online interpersonal victimization by a current/former intimate partner … [and] … a significant but negative relationship between experiencing indirect victimization and fear of online interpersonal victimization by current/former intimate partners and friends/acquaintances" (Henson et al., 2013, p. 488-489). Notably, the study made note-worthy distinctions, distinguishing between the type of victimizations and incorporating victim-offender relationships. Thus, the mixed or inconclusive results are influenced by the victimization type (direct or indirect) and victim-offender relationship.

Studies that report a positive relationship between victimization and fear of cybercrime tend to differ markedly from the current study. For instance, whereas the present study used a nationally representative sample (Canada-wide sample), Abdulai (2020) and Lee et al. (2019) used student samples. In contrast, Elhai et al. (2017) used an internet labor market (Amazon's Mturk system). Also, whereas the current study combined a single emotion (fear) and various unspecified cybercrimes into a single outcome measure, Abdulai (2020), Choi et al. (2021), and

Lee et al. (2019) combined a single emotion (fear) and specific cybercrime (credit/debit card fraud, identity theft, and online victimization, respectively), and Brands and van Wilsem (2021) combined different emotions (fear and worry) with several cybercrimes into a single outcome measure.

Like the distinctions with studies reporting a positive association, the current research is also distinct from the Henson et al.'s (2013), which reported inconclusive results. The present study used a nationally representative sample of internet users in Canada, whereas Henson et al. (2013) used full-time undergraduate students. Also, the current study combined a single emotion (fear) and various unspecified cybercrimes into a single outcome measure. In contrast, as Brands and Van Doorn (2022) points out, Henson et al. (2013) used three single outcome measures by linking distinct cybercrimes with a single sentiment in their work. These nuances are worth pointing out because they can have definite influences on the results, thus leading to differential findings.

The finding of the mixed effect of victimization's impact on fear highlights the complex nature of the interaction between the two variables. However, the reverse result in the current study may appear surprising at face value or from the common-sense expectation. But on reflection, it seems plausible within the context of the present subject matter. First, it means that rather than creating a specter of fear and leaving victims in a constant state of fear, as implied in Ferraro's (1996) "shadow of sexual assault" thesis in support of women's heightened fear of crime, cybercrime victimization makes people resistant, hence, less fearful. Victimization experience may create a sense of awareness among victims whereby a feeling of resistance sets in instead of fear. Victims can feel a sense of familiarity with the criminogenic environment prevalent in cyberspace, thereby dousing their fear of victimization.

The current finding is significant within the context of the conceptual lens adopted for this study. Victimization and fear of cybercrime constitute outcomes and unintended consequences of internet use. Built into victimization are elements of structure, agency, and outcomes. Actors, because they possess agency, demonstrate such by accessing the internet, the latter constituting structure. By interacting with structure in this way, internet users (actors) experience victimization as a consequence (outcome) of interacting with the internet.

People experience fear when they use the internet, directly or indirectly. Accordingly, fear becomes wired into the internet and is experienced as an (unintended) outcome of acting in cyberspace. Similarly, fear is built into the internet structure and comprises an outcome. In this way, victimization and fear both have similar characteristics, thus conceptually significant and plausible that they do not influence or affect each other. However, the results reveal an association in the opposite direction, where victimization experience is associated with reduced fear of cybercrime. The results thus call for theory modification and/or further probing, and the mixed evidence in the existing literature adds credence to such a call.

7.3 Cybercrime Victimization Experience and Risk of Cybercrime Victimization

Results from this study's multivariable analysis do not support the hypothesis that prior victims of cybercrime are expected to perceive more risk of cybercrime than persons without victimization experience (p-value=0.04). In other words, there is not enough evidence to uphold the statement that victims of cybercrime perceive more risk of cybercrime than non-victims. The reverse, according to this study, is true. Holding all other predictors constant, internet users who have been victimized had lower odds of feeling at risk of cybercrime than their counterparts without such experience (OR = 0.91, 95 % CI: 0.47, 2.92). The study also revealed a statistically

significant interaction (p-value = 0.03) between gender and victimization in internet users' perception of cybercrime risk. Specifically, according to this study, male internet users who have been victimized had lower odds of feeling at risk. In other words, the lower odds of perceiving cybercrime risk among internet users with experience of victimization is especially pronounced among males, not females. This means the effect of victimization experience on cybercrime risk perception is not a given or uniform across gender. Instead, such an effect is sensitive to gender because it is observed only among victimized male internet users.

As previously noted in the literature review section, unlike conventional crime, studies about the relationship between cyber victimization and the risk of cybercrime are limited. However, the evidence in the current research results does not support the finding in the literature. In their study of cyber victimization in the EU, Riek et al. (2015) found that cyber victimization is an antecedent to the perceived risk of cybercrime; thus, victimized European internet users perceived a heightened risk of victimization. Also, Abdulai (2016) reported that students who were prior victims of credit or debit card fraud tended to perceive more risk and demonstrated heightened fear of becoming victimized again. Additionally, Alshalan (2006) reported a positive relationship between cybercrime victimization and fear and risk among US households. US households who experienced cybercrime also reported greater fear and risk than non-victims. Like the current results, Alshalan also found a significant interaction between gender and victimization regarding risk and fear. The difference was that the two studies observed the interaction effect in the opposite direction. Whereas in the current study, males with prior victimization experience had lower odds of perceiving risk, women with previous victimization perceived more risk and were more likely to be fearful than others in Alshalan's (2006).

Aside from being at variance with findings in the existing literature, empirically, the current results may also come across as contradictory as it suggests that persons victimized by cybercrime tend to perceive less risk than their counterparts. However, the finding is analytically meaningful and empirically plausible. Persons victimized might perceive less risk because their prior experience makes them numb and not averse. They may perceive otherwise risky situations as less risky because they have lost the feeling of dread, which is associated with the unknown. In other words, people's familiarity with risk due to their victimization may make them contemptuous of risk.

On the other hand, persons who have not experienced firsthand victimization may tend to harbor more fear and perceive more risk. Their heightened sense of risk could result from stories of others' victimization experiences. Thus, their relative lack of experience positions them at a disadvantage, leaving them with feelings of dread and perceiving higher risks.

Conceptually, victimization experience and risk perception are outcomes of the interaction between structure and agency. Internet users demonstrate agency by accessing the internet – structure – and become victimized. Thus, such experience becomes an outcome (unintended consequence) of their agency. Meanwhile, risk is built into structure (note that cyberspace is the internet's virtual structure) and becomes an outcome (unintended consequence) when people use the internet. Given that both variables have similar attributes - outcomes experienced from actor agency interacting with structure - it is expected both will vary in a similar direction, where an increase in one will relate to a similar increase in the other and vice-versa. However, this conceptual expectation is not supported by the results. Like victimization experience and fear of cybercrime, the results suggest a need for theory modification or further investigation.

The findings have implications for cyberspace offending, victimization, and crime control. When persons who have been victimized perceive less risk, it probably means they downplay the extent of the costs of their experience. Doing so has the unintended consequence of exposing people to further and more expensive offenses in cyberspace. Persons with ill motives will be spurred on in their deviant activities and will seize more opportunities to target unsuspecting internet users. Alternatively, the victimized may perceive less risk because they lack an understanding of the nature of risk. Such a dearth of knowledge can cloud victimized persons' anticipation and projection of the risk of victimization. The effect will be repeated and create increasingly severe victimizations because the inadequate understanding will provide an opportunity for deviants lurking in cyberspace. In both cases, education about the nature of risk and the dangers of downplaying risks and victimizations in cyberspace for internet users will be a helpful crime control strategy. Advocacy and sensitization campaigns across virtual and physical platforms will be needed.

7.4 Victimization Experience and Internet Behavior Constraint:

7.4.1 Victimization Experience and Avoidance Internet Use Behavior

Results from the multivariable analysis in this study do not support the hypothesis that victims of cybercrime are more likely to resort to avoidance internet use behaviors than non-victims. In the univariable modeling, victims of cybercrime had 1.25 times higher odds of resorting to avoidance behavior than non-victims, although the association did not reach significance (OR = 1.25; 95 % CI: 0.72, 2.16; see Table 5.9). In other words, cybercrime victims are not any more prone to avoidance internet use behaviors than non-victims. V*ictimization* as a variable did not qualify for inclusion in the final multivariable logistic regression model for

Avoidance behavior. As a result, this study concludes that the hypothesized relationship between victimization and avoidance behavior could not be ascertained or is inconclusive (see Table 5.13).

The current finding is inconsistent with Böhme and Moore's (2012) similar study in the EU. Their study found that cybercrime victimization experience, concern about cybercrime, and media exposure lead to online service avoidance among consumers (Böhme & Moore, 2012). Through online service avoidance, persons with cybercrime experience resorted to avoidance internet use behaviors. Similarly, Saban et al. (2002) found that consumer experience of cybercrime negatively affected internet use, irrespective of gender, including reducing "repeat online purchases . . . [and] the overall value of the internet as a viable marketing channel" (p. 34). Here also, Saban et al.'s (2002) study refers to avoidance internet use as a response to people's victimization experiences. In both studies, internet users experience behavioral constraint in the sense of having to avoid certain online activities owing to their victimization experiences. In contrast, internet users who experienced victimization in the current study did not experience constraint in their subsequent internet use activities.

The finding of victimization experiences' non-association with avoidance internet use behaviors also appears inconsistent with common-sense expectations. Conceptually and in an ideal world situation, one would expect a discernible relationship in the positive direction between cybercrime victimization and avoidance behavior. The conceptual and common-sense view is especially tenable as the literature suggests further that victimization has a significantly positive effect on fear of cybercrime (Abdulai, 2020; Brands & Van Wilsem, 2021; Choi et al., 2021). By having a positive effect on fear, it implies that victimization indirectly influences avoidance behavior through the mediating effect of fear. Accordingly, it is expected that

cybercrime victims would constantly live with a shadow of their 'negative' experience, one they would want to avoid encountering again. Consequently, a way to escape future victimizations would be to avoid certain online activities, thus avoiding internet use.

Also, the study's finding challenges the theoretical stance of the study. Victimization experience arises from an interaction between structure and agency, wherein users, accorded with an agency, access the internet, which is the element of structure. Victimization then results as an outcome or unintended consequence of the interaction. On the other hand, avoidance behavior is a behavioral response to risk, fear, and actual victimization from accessing the internet, and it represents actor agency and reflexivity. Theoretically, it is expected that victimization will trigger a reflexive response from internet users – avoidance internet use behaviors – to ward off such threat of victimization. This plausible expectation, however, is not supported by the results.

However, the finding at face value may seem counter to common sense and can be accounted for in several ways. First, like with every quantitative study, this finding may have been impacted by the sample size. Second, this study's findings could also reveal the nature of the internet rather than the behavior of internet users. The ubiquity of the internet suggests internet users have little opportunity or incentive to scale back on their use or minimize some of their internet use activities, notwithstanding their unpleasant experiences online. For some internet users, avoiding certain kinds of internet use behaviors may appear to diminish or reduce the use-value of the internet. In this way, the defining role of structures (the internet) in people's daily lives (agents or internet users) comes to the fore. In other words, cybercrime victims having a decreased odds of avoiding internet use behaviors may be a consequence of limited agency in

the face of the determining role of structure, a perspective consistent with the structure strand of the structure versus agency debate (see Chapter 3).

The results have some implications for theory and policy. Theoretically, the findings suggest a call to redefine actor agency and reflect on actor agency vis-à-vis ideas of control and rationality. Actor agency need not always be about actors asserting their agency actively and rationally. As seen from the results, actor agency is equally about being passive, losing or giving up control, and being vulnerable to structure dictates. Policy-wise, cyber-security stakeholders need to scale up efforts at developing friendly and affordable but robust security patches and protocols to securitize cyberspace for internet users. Internet users will need this “big brother-esque" support from the state and private sector to ensure they are not overly exploited. This can be achieved by increasing research and development allocations for cheap but effective software programs.

7.4.2 Victimization Experience and Defensive Internet Use Behavior

Like victimization and avoidance behavior, the current study results do not support the hypothesis that cybercrime victims are more likely to adopt defensive internet use behaviors than non-victims. In other words, cybercrime victims are no more prone to defensive internet use behaviors than non-victims. Even though in the univariable modeling, cybercrime victims had 1.22 times higher odds of engaging in defensive behaviors than non-victims, such univariable association was not significant (OR = 1.22; 95 % CI: 0.67, 2.23; see Table 5.10). In this study, *victimization* as a variable did not qualify for inclusion in the final multivariable logistic regression model for *Defensive behavior*. As such, this study's hypothesized relationship between victimization and defensive behavior is inconclusive as it could not be assessed (see Table 5.14).

The results here may at first appear to contradict common-sense expectations. In an ideal situation, internet users who have suffered cybercrime victimization would be expected to protect themselves against further victimizations in the future. This is because victimization has a significantly positive effect on the fear of victimization (Abdulai, 2020; Brands & Van Wilsem, 2021; Choi et al., 2021). Indeed, a way to protect oneself from potential (or actual) cybercrime victimization is to incorporate defensive techniques in subsequent internet use. Accordingly, conceptually it is consistent to present that the victims of cybercrime might be expected to strive to integrate defensive internet use behaviors to ward off repeat victimization. Utilizing these defensive techniques would ensure an internet user can access the internet safely and securely.

Moreover, the results also appear contrary to and challenge the theoretical posture of the study. Defensive internet use behaviors are behavioral responses to risk and outcome of actions from using the internet, be it fear or actual victimization. These defensive behaviors imply actor agency and reflexivity. Thus, theoretically, the expectation is that victimization experience will result in an almost automatic response from internet users, defensive internet use techniques or precautions, given actors' active and reflexive nature. But the results do not seem to support such theoretical expectations.

However, the study's results could be explained from several lenses. First, the results may imply that defensive internet behavior is utilized by all internet users, irrespective of their prior victimization experiences. Defensive internet behavior use in this way could also be a result of people's realization of the riskiness of activity in the cybersphere, a sphere devoid of the physical meeting of persons and yet fraught with opportunities for deviance and crime. Consequently, as active agents who play a role in the construction of their lived experiences, internet users demonstrate control (agency) by choosing to utilize defensive internet behaviors in

their internet use while staying free from cybercrime victimization. In this way, we see an interplay between structure (the internet and its attendant risk) and agency (internet users turning to defensive internet behaviors).

Unlike victimization and avoidance of internet behavior, the results here may also reveal the nature of internet users rather than the internet. Victimized persons may lack a resolve towards defensive internet use techniques merely because they lack knowledge and awareness of these strategies. Precautionary internet use actions such as a passcode or fingerprint on smartphones and laptops, multi-factor authentication, a virtual private network (VPN), use of firewall and encrypted computers, among others, though effective, may not be accessible to most internet users owing to a knowledge gap, affordability, stigma or a combination of any of such related factors. Consequently, knowledge and awareness gaps may inhibit the agency of internet users. Thus, despite having experienced victimization, the opportunity to assert actor agency and reflexivity by subscribing to defensive internet use strategies may be constrained.

Reflectively, this finding has implications for theory and policy. Theoretically, the results indicate a need for closer examination of actor agency in light of the structure and agency nexus in social action. Contrary to the prevailing opinion, this study reveals that actor agency is not a given. Agency can be given impetus or constrained by social structural factors, ranging from knowledge, awareness, resource, and cost. Thus, agency also means not acting. Also, the results imply that victimization need not always elicit a thoughtful behavioral response from internet users. Empirically and in the realm of policy, policy interventions need to target social structural factors which can inhibit internet users' use of defensive behaviors. Information about preventive internet use techniques needs to be made easily accessible through advocacy programs. These

targeted policy interventions will additionally serve as confidence-building measures to encourage users to access the internet safely and confidently.

Imperatively, the study's findings throw a wrinkle into the literature about victimization and constrained behavior. As previously noted in the literature review section, the prevalent literature has tended to focus on or limit constrained behavior only to avoidance behaviors. For example, Böhme and Moore's (2012) study focused on only online service avoidance as a response to victimization, neglecting online defensive services or actions. Also, Saban et al. (2002) found that cybercrime victimization reduced consumer internet behavior, indicating an impact in the direction of service avoidance. However, I argue in this study that such a focus blurs reality and impacts theory and policy. As revealed in Rader et al. (2007) and Rader (2004), constrained behavior is a two-way street comprising avoidance and defensive behaviors. In contrast to Böhme and Moore (2012) and Saban et al. (2002), and in line with Rader et al. (2007) and Rader (2004), the current study provides a broader focus in terms of projecting how victimization impacts not just avoidance, but equally defensive behavior.

7.5 Incident Reporting and Fear of Cybercrime Victimization

Based on results from the multivariable analysis in this study, hypothesis 5 – cybercrime incident reporting is associated with fear of cybercrime – is not supported. In other words, there was not enough evidence to sustain the statement that cybercrime incident reporting is related to fear of cybercrime. Across all levels, incident reporting was associated with more than two times higher odds of expressing fear as compared to the reference category, although only the likely to report category (OR = 3.03; 95 % CI: 1.01, 9.06) was statistically significant in the univariable relationship (see Table 5.7). As such, the fear-incident reporting relationship could not be

explored in the multivariable modeling stage since cybercrime incident reporting was not a candidate in the multivariable analysis stage. In other words, this study found no conclusive relationship between fear of cybercrime and incident reporting.

The current results partially support van de Weijer et al.'s (2020) study, which looked into the interaction between cybercrime fear and willingness to report cybercrime victimization to the authorities. Following their work, van de Weijer et al. (2020) found that fear of cybercrime victimization was significantly and positively associated (OR=1.19, $p<.05$) with willingness to report cybercrime incidents (p. 26). In other words, respondents were more inclined to report cybercrime if they were fearful of being a victim. While the latter finding is consistent and supported by the result at the univariable level of analysis in the current study, where incident reporting is associated with much higher odds of expressing fear (OR=3.03), it is not replicated at the multivariable level of analysis. Nonetheless, the univariable results is significant. Moreover, van de Weijer et al.'s (2020) research is comparable to the current study across several metrics. Both studies have been conducted at the national level – Netherlands and Canada - with nationally generalizable (but not necessarily representative) samples; both used online research panel samples and had similar sample sizes – 595 and 483.

Given the constraint of limited sample size and small sub-sample size (n) in the study, the univariable finding of significant positive association appears to be indicative of the relationship between incident reporting and fear, though not definite. Such indication means that there may be potential association between the two variables that can be clarified by further research. The possible impact of an interaction with a confounding variable is not ruled out. Also, the sample size could be an issue, as with most quantitative studies. Despite this, the multivariable finding of inconclusiveness is equally relevant. Imperatively, it gives room for additional research, as

surmised in the univariable result. For instance, though unexplored in this study, the intensity or seriousness of the cybercrime can have a possible mediation in the relationship between fear of victimization and internet users' decision to report cybercrime. This reasoning is plausible because offense seriousness has been found to predict cybercrime reporting behavior (van de Weijer et al., 2020; Wall, 2008; Yar, 2013). In this way, internet users' projection or evaluation of the seriousness of cybercrime – in terms of financial, emotional, or social cost – will be instrumental in whether they entertain fear and subsequently impact their reporting decisions.

Within the context of the conceptual lens adopted for this study, the current finding is significant though not consistent. Cybercrime incident reporting constitutes agency (active agency), whereas fear of cybercrime constitutes structure and outcomes (unintended consequences) of internet use. Incident reporting manifests as internet users consciously inform the police or other responsible outfit about their encounter with cybercrime. Exercising the choice of communicating their experience indicate internet users' active role in the socio-technological action of reporting cybercrime incidents. Conversely, fear is built into the internet structure and comprises an outcome. People experience fear either when they use the internet, directly or indirectly, or when they reflect on their victimization experiences (also directly or indirectly). Accordingly, fear becomes wired into the internet and is experienced as an outcome (unintended) of acting in cyberspace. In this way, incident reporting and fear are distinct and disparate constituents, as the results show. Theoretically and conceptually, the absence of a definite association between incident reporting and fear means it is inconsistent with the theoretical discussion in the study – that is, the perspective that social action results from an intricate interaction between structure and agency which does not accord priority to either structure or agency.

Notwithstanding the lack of clarity or decisiveness regarding the association between fear of cybercrime and cybercrime incident reporting in this study, the results provide a valuable niche for further research and probing. The generally low incidence of cybercrime incident reporting is unmistakable and fairly established in the literature (CBS, 2018; Cross et al., 2016; Goucher, 2010; van de Weijer et al., 2020; Wall, 2008; Yar, 2013). However, the link between fear of cybercrime and incident reporting behavior is palpably missing in the literature. Therefore, demonstrating a link between incident reporting behavior and fear of cybercrime victimization will contribute significantly to better understanding the nuances involved in the generally low incidence of cybercrime incident reporting among internet users. Additionally, clarifying this relationship will also help to compare whether a similar association applies to the fear of victimization and reporting behavior of conventional crimes. Accordingly, in cybercrime prevention and policy making, the police and other responsible institutions can develop targeted policies to motivate people to report their victimization. Additionally, establishing an evidence-based relationship, or otherwise, between these two key variables will also be essential for cyber-security policy-making among security agencies and others involved in policy discourse.

7.6 Internet Use Frequency and Internet Behavior Constraint

7.6.1 Frequent Internet Users and Avoidance Behavior

Results from the multivariable analysis in this study do not support the hypothesis that frequent users of the internet are more inclined than less frequent users to engage in avoidance internet use behavior. In the univariable modeling, frequent internet users (several times in a day usage) had higher odds (more than twice) of resorting to avoidance behavior than less frequent users, although the association did not reach significance (OR = 2.19; 95 % CI: 0.54, 8.90; see

Table 5.9). In other words, frequent internet users are not more given to avoidance internet use behaviors than less frequent users. As a variable, internet use frequency did not qualify for inclusion in the final multivariable logistic regression model for *Avoidance behavior*. Thus, in this study, the hypothesized relationship between internet use frequency and avoidance behavior is inconclusive as it could not be assessed at the multivariable level (see Table 5.13).

The inconclusive result means categorical statements cannot be made about the relationship between the two variables. However, the literature on internet use frequency and fear of victimization may offer insights into the current results. According to Holt and Bossler (2009), internet use frequency alone (measured as the number of hours users spend online in chat rooms, internet relay chat, and instant messages) does not have a significant impact on victimization risk (p. 13). Accordingly, neither spending more time on the computer nor interactive websites places internet users at more risk of victimization (Holt & Bossler, 2009, p. 13). However, Henson et al.'s (2013) study showed that hours spent online in a day did not significantly affect on fear of online interpersonal victimization, Lee et al. (2019) also found that usage time on social networking sites had no statistically meaningful impact on fear of victimization or sense of enhanced exposure leading to heightened risk. Instead, Holt and Bossler (2009) argue that such exposure time with others needs to happen in the context of online deviant acts (p. 13). The latter argument suggests the presence of a condition or an interaction with other elements. These non-significant findings imply that internet users will be less motivated to incorporate avoidance behaviors, given that online exposure does not affect their victimization. Yet internet use frequency is also positively associated with fear of cybercrime (Maddison & Jeske, 2014; Roberts et al., 2013). This means that increased online exposure increases the

vulnerability of users to victimization, hence increased fear of cybercrime. Meanwhile, increased fear of victimization will presuppose an urge to avoid certain internet use behaviors.

Some studies have demonstrated that internet use frequency or online exposure does affect victimization. In Virtanen (2017), only one out of three models revealed a significantly negative association ($p<.01$) between internet usage (respondents' frequency of accessing the Internet at work, home, or in public) and cybercrime fear (p. 336). For Brands and van Wilsem (2021), "rather than being an indicator of exposure to risk, device possession may indicate confidence in online skills and a low perceived risk of victimization" (p. 225). Device possession, referenced in the latter study, is also used to correlate online exposure. By extension, the reverse implication is also plausible; lower scores on device possession and other metrics of online exposure imply a shortage of computer skills and a perceived heightened risk of victimization.

The current results appear instructive when one juxtaposes these disparate results about the relationship between these variables (internet use frequency and fear of cybercrime). Avoidance of internet use behavior is internet users' active agency and reflective response to perceived risk, fear, and actual victimization. Meanwhile, internet use frequency (online exposure) correlates with heightened risk, fear, and victimization. So, in the circumstances of a lack of clarity and decisiveness in terms of the effects of internet exposure time and fear, an inconclusive outcome between internet use frequency and avoidance of internet use behavior is tenable and increasingly justified.

Nonetheless, the current finding is theoretically and conceptually refreshing. Internet use frequency is a measure of actors' active agency in their interaction with the internet (the component of structure); more frequency implies heightened agency and, consequently,

increased exposure. Avoidance of internet use, on the other hand, is a measure of actors' behavioral responses (reflectivity) to (perceived) consequences of their agency in cyberspace (internet use). That is, avoidance internet use is an action in furtherance of agency. Conceptually, the expectation is that heightened agency in cyberspace will mean enhanced exposure to risk, which will then set off a reflective response – avoidance behavior in this situation. However, this conceptual expectation is neither supported nor refuted by the empirical results, as the finding is inconclusive. The results mean that actors have yet to perceive that their increased internet exposure activity has placed them at increased risk of victimization, thus the urge not to incorporate avoidance measures. Also, à la Brands and van Wilsem (2021) on device possession and risk, increased frequency of use may also indicate actors' increased confidence in their internet use skill set, including their ability to maneuver themselves out of risky or vulnerable situations online.

7.6.2 Frequent Internet Users and Defensive Behavior

Like with internet use frequency and avoidance behavior, results from this study do not support the hypothesis that frequent users of the internet are more inclined than less frequent users to adopt defensive internet use behaviors. That is, frequent internet users are not any more likely to adopt defensive internet use behaviors than their less frequent user counterparts. Even though in the univariable modeling frequent internet users (several times in a day usage) had higher odds (more than twice) of engaging in defensive behaviors than less frequent users, such a univariable relationship did not reach statistical significance at 5 % (OR = 2.89; 95 % CI: 0.76, 11.03; see Table 5.10). As a variable, internet use frequency did not qualify for inclusion in the final multivariable logistic regression model for *Defensive behavior*. As such, in this study, the

hypothesized relationship between frequency of internet use and defensive behavior could not be assessed at the multivariable level as it is inconclusive (see Table 5.14).

Reflecting on this finding, it appears to border on the contrary with everyday expectations. Frequent internet access means people spend considerably more time online than the average user. Doing so implies also that actors are exposed not only to the opportunities but, crucially, to the risks fostered by the internet. Cyberspace, as a sphere of interaction, constitutes a criminogenic environment that facilitates the virtual meeting of offenders and victims. Logically, an increased exposure will presuppose greater possibilities to reap the benefits or opportunities while also placing users at the threshold of increased probability of risk of victimization. Deductively, then, internet users – as active and 'rational' operators - will be expected to adopt strategies that will ensure they continue to maximize the opportunities of their increased internet activity while minimizing the associated risks.

Like with internet use frequency and avoidance behavior, the literature on constrained internet behavior use (defensive internet use techniques) and fear of victimization may also offer some insights into the current finding. Using multiple regression analysis, Elhai and Hall (2016) found a less than substantive (not significant) association between electronic security precaution use (defensive behavior) and data breach anxiety. In other words, respondents who reported using electronic security precautions (including passcode/fingerprint, anti-virus software, and VPN, among others) did not experience significant changes in their anxiety about data breaches. By frequency count, only a few respondents (8 persons or 2.7 %) and the majority (122 persons or 40.5 %) felt the use of security precautions reduced their data breach anxiety "very much" and "a little bit" respectively (Elhai & Hall, 2016, p. 183). Accordingly, respondents did not perceive electronic security precautions to reduce or impact their fear of cybercrime. Going by

this finding, then, the current results become meaningful. If internet users do not feel their use of defensive internet behaviors douses their fear of victimization, using the internet frequently would not have a discernible effect on their incorporation of defensive internet use techniques. The reverse is true: internet users will be expected to move towards incorporating more defensive internet use precautions if they perceive such preventive actions to reduce their risk of victimization.

From the above, the current results appear to be in sync with the theoretical focus of the study. Internet users are active agents who play an active role in constructing their social and lived experiences. They do so by not giving in to the dictates of structure (the internet) but by interacting with structure in decisive ways. Defensive internet use behavior is an exercise in actor active agency and reflectivity to the operations of structure (cyberspace or the internet). As reflective operators who think, reflect, and calculate the consequences of their actions in cyberspace, internet users will not be expected to continue to deploy more defensive internet use techniques if they lack trust or conviction about the efficacy of these measures to reduce the calculus of their risk of victimization. Thus, the finding of inconclusiveness between internet use frequency and defensive behavior is a plausible and theoretically consistent conclusion.

7.7 Motivations for Internet Use

Six main motivational themes were developed from the thematic analysis of participants' responses that reflected the varying motivations for internet users' utilization of the internet and other CMCs. These thematic components include education and knowledge acquisition, entertainment and fun, communication and social media access, commercial purposes, work and personal-related use, and news and information access. Additionally, an 'other' motivational

thematic component was developed to reflect the other uses of the internet that could not readily be categorized under any of the six main thematic components. For this research, the analysis of internet user motivation was focused or reduced to the presence and primacy or latency of structure and agency in each motivational thematic component and the connections between each theme and risk o victimization, fear of cybercrime, avoidance internet, and defensive internet use. Even though this approach may be criticized as reductionist, such apparent reductionism is necessary and consistent with research.

The thematic analysis revealed that an intricate interaction between structure and agency straddles all but one of the thematic motivational components. Structure is salient in the "News and Information access" motivational theme. Overall, each dimension of structure and agency is prevalent in the various motivations underpinning internet users' access to the internet. Even in the thematic component where primacy is accorded to structure, there is not a total absence of agency. The difference is that each dimension appears to have latent effects, which leads to their relegation to secondary but not insignificant roles. Regarding the existing literature, some motivation literature relates to agents' role in cyber security. For example, LeFebvre's (2012) study examined students' motivation to protect themselves online. This kind of study is not focused on general determinants for internet use per se (one of the foci of the current study). However, some studies relate to and corroborate the present findings.

The analysis also revealed connections between the thematic motivational categories and perceived risk, fear, avoidance, and defensive internet use. The activities and codes under the themes suggest an inevitability about them to the extent they are seen as required. Some themes and activities also lie at the node of culture and the constraints of modern social life. Accordingly, people are motivated to use the internet for these activities irrespective of perceived

risks and the fear of cybercrime. They do this by either rationalizing risk, denying its existence, or minimalizing risk as a coping strategy. Furthermore, people will tend to incorporate defensive internet use strategies while disregarding avoidance internet use to maximize their internet use.

Some extant literature about the motivation for cyber victims or internet users' access to the internet is focused on specific internet communication activity – Social Network Site (SNS) (Barker, 2009). In his study of older adolescents' motives for SNS use, it was found that communication was the main determinant or motivation for SNS (Barker, 2009, p. 209). In other words, SNS use was used as a decoy for internet use, and it emerged that communication with peer group was the foremost determinant. Additionally, the study also found an interaction between collective self-esteem (group identification), SNS use (communication), and gender (Barker, 2009, p. 209). Thus, participants who scored high in positive collective self-esteem had a stronger motivation to use to communicate with peer groups. Additionally, female participants reported higher overall use, higher collective self-esteem, and more SNS communication with peers (Barker, 2009). Imperatively, the significant determinant of adolescent internet use intersects and supports the current study's results. Communication and social media access is one of the thematic components of internet use motivation among Canadian internet users. Furthermore, consistent with the theoretical and conceptual discussion, the theme of communication and social media access embodies elements of both structure and agency.

The findings by Papacharissi and Rubin (2000) also support the current results. Unlike in LeFebvre (2012), this study had a similar focus to the present study. Using factorial analysis in their quantitative study, Papacharissi and Rubin (2000) found five main motives that undergird computer users' access to the internet. The motives included "interpersonal utility, pass time, information seeking, convenience, and entertainment" (Papacharissi & Rubin, p. 185). These

correspond to the motivational themes developed in the current study. For example, the interpersonal utility motive maps to work and personal use, pass time maps to entertainment and fun, information seeking maps to news and information access, convenience maps to commercial purposes, and entertainment maps to entertainment and fun. As revealed in the analysis, the motives and determinants of internet access are arrived at through an interface between structure and agency, hence, in line with the theoretical and conceptual discussion in the current study.

In a related study about the correlates of internet use, Joiner et al. (2005, p. 371) found that "gender, internet anxiety, and internet identification" predicted internet use among undergraduate students. The gendered difference hints at the role of actors (males and females) in engendering internet use. Similarly, internet identification and internet anxiety also relate to factors at the individual or micro-level, thus indicative of actors' agency. Generally, Joiner et al.'s study focused specifically on the role of agency as conveyed by all the correlates measured in their work.

The current study is unique and differs markedly from the literature cited above. First, the present study (specifically about motivation) is qualitative, while the cited extant literature is quantitative. In other words, unlike in the cited literature, the current study did not limit respondents to given or specified motivational factors. Instead, the motivations for internet use emerged organically by allowing respondents to self-report the specific elements they perceived to motivate their use of the internet. The collated responses were then synchronized and analyzed, and the respective motivational components developed. Second, the current study focused on witting down respondents' self-reported motivations to the role of structure and agency and their connections with perceived risk, fear, avoidance, and defensive internet use.

Imperatively, the current finding is consistent with and underscores the theoretical and conceptual discussion in the present study. Like any socio-technological activity, internet use is an embodiment of active agents interacting with the internet on various platforms. The internet and the multiple media that host it, such as laptop computers, desktop computers, tablets, and mobile phones, constitute structural elements. Also, the various institutions of work, education, business, and commerce, as well as social media, all comprise structure. Meanwhile, agency refers to the active roles of internet users.

Theoretically, the mutually reinforcing structure agency relationship, as revealed across the motivational themes, imply a need to rethink the structure agency dichotomous discourse. The mutual interaction between structure and agency suggests that the binary argument is no longer tenable or useful. It is better to examine nuances in the structure-agency dynamic better.

Practically, these findings imply that utilizing the internet is a function of both individual choice and factors or forces external to the individual. This further means that structures need to entice and encourage people to engender more internet use. For example, educational institutions can encourage students to use the internet by increasing the availability of computers and laptops in libraries and other vantage points on campus. Equally important is to improve internet access and connectivity across campus. Similarly, employers can encourage employees to use the internet by providing computers and laptops and improving internet connectivity at workplaces. Employers can also transition some activities online to encourage employees to use the internet. Local authorities and governments will also need to stock public libraries with computers and improve internet access and connectivity in libraries. Importantly, these structures, including educational and work institutions and governments, will also need to ensure computers and

laptops are signed to efficient anti-virus software to guarantee users a sense of safety. Additionally, alongside the role of structures, individual actors also need to be actively involved.

7.8 Implications

The research findings in the current study provide some theoretical and practical implications for researchers, practitioners, and internet users in general. The rest of the section is organized as follows: in subsection 7.8.1, I present the study findings' implications for theory, while in section 7.8.2, I present the practical implications.

7.8.1 Theoretical Implications

Several theoretical implications are gleaned from the study.

First, cybercrime risk perception is strongly associated with education, gender, and marriage and implies that the risk of cybercrime is sensitive to these socio-demographic variables. Further, this means that less educated, male, and unmarried internet users have limited agency. On the contrary, the current theoretical discussion about the individual agency is totalizing; it suggests that agency is available and is manifested equally or freely by individuals. In hindsight, this is a limitation of the current theoretical discussions of agency and indicates that arguments about individual agency need to be reimagined and reformulated. Agency is limited and not experienced or manifested equally across the board.

Secondly, victimization experience, fear of cybercrime, and risk of cybercrime all share similar ethos and attributes as they fall under the same theoretical concept of outcome and un/intended consequences. Characterizing these variables as belonging to the same theoretical

category implies that each can be isolated for closer scrutiny, and findings may apply to the others.

Additionally, structures have a deterministic effect on agents in certain realms of social experience. This is demonstrated by cybercrime victims having decreased odds of resorting to avoidance internet use behaviors. Avoiding certain kinds of internet activities is tantamount to diminishing the use-value of the internet. And it suggests limited agency in the face of the overarching role of structure. Accordingly, a limitation in the current theoretical discussion is that there is too much emphasis on the individual agency regarding cybercrime. In most instances, as demonstrated in this study, however, people lack the capacity to protect themselves or even perceive the extent of the damage.

A related theoretical implication is that actor agency does not necessarily equate to action/ing; it can be given impetus or constrained, and it also means being passive and giving up control. These implications have been demonstrated in the association between victimization experience and internet behavior constraint (avoidance and defensive internet use). This suggests that the current theoretical formulation of actor agency is potentially limited and needs to be broadened. Discussions of actor agency need to capture its dual nature, and imperatively, the non-acting dimension needs to be given equal prominence in these discussions.

Moreover, the mutually reinforcing structure agency relationship, as revealed across the motivational themes, imply a need to rethink the structure agency dichotomous discourse. The mutual interaction between structure and agency suggests that the binary argument is no longer tenable or useful. It is better to examine nuances in the structure-agency dynamic better

Furthermore, the claim that internet use frequency or enhanced exposure (resulting from a heightened agency) will elicit a reflective response (avoidance behavior) needs further probing as the current study failed to reach a decisive conclusion.

Lastly, actor reflexivity is salient in internet users' interactions with the internet and other computer-mediated communications. The significance of reflexivity is demonstrated by the finding that frequent internet users are not more likely to adopt defensive internet behavior than less frequent users.

7.8.2 Practical Implications

Several practical implications emerge for practitioners and internet users upon reflecting on the study findings.

First, the significance of education indicates that better-educated internet users are more informed about the inherent risk in cyberspace and the protective measures. They also have increased agency while their counterparts - less educated internet users have less or limited agency. This further suggests that education enhances actor agency and positions actors' to better interact and engage with the internet as it relates to the risk of cybercrime. Accordingly, to strengthen the agency of internet users, education needs to be given a significant place. Educational programs and interventions to better inform and raise the awareness of internet users will have practical utility in improving the overall agency of internet users. In this respect, the Canadian National Cyber Security Strategy (2018) and the National Cyber Security Action Plan (2019-2024) would be enhanced by incorporating education, advocacy, and sensitization about risk.

Second, cybercrime victimization embodies both positive and negative aspects. Through victimization, victims learn firsthand the pain and cost of cybercrime while equipping themselves with the knowledge of victimization risk. The victimization experience may alternatively breed familiarity and numb victims, thus ushering in contempt for the risk of cybercrime victimization.

Also, the ubiquity of the internet means that it is almost impossible to scale back from its usage. Accordingly, individuals are powerless to avoid internet use and sometimes cannot protect themselves, even when informed about its inherent vulnerabilities. Moreover, in Canada's networked and technologically driven society, avoiding certain internet activities diminishes the use-value of the internet for people. This suggests that internet users need help. Accordingly, there needs to be increased research and development for affordable but robust security patches made available to all Canadian internet users.

Finally, internet use is the outcome of internet users' choices and the demands and inducements of structures. People decide about accessing the internet and other computer-mediated communications. However, such a decision is motivated and constrained by structural factors. In the end, it is not one but a synchronous and, at times, dependent interaction between internet users and various structures. Here also, the Canadian National Cyber Security Strategy (2018) and the National Cyber Security Action Plan (2019-2024) can be strengthened by incorporating on-going consultations with everyday Canadian internet users (not only experts) to understand their concerns and experiences of risk and victimization.

Chapter Eight: Summary Conclusions

8.0 Introduction

The study sought to determine whether people's internet use in Canada has been impacted by fear, risk perceptions, and victimization from cybercrime. The study is framed within the disciplinary lens of socio-criminological research. In this chapter, I present the summary and concluding remarks on the study.

The research explored the apparent paradox in the relationship between internet use, cybercrime risk, victimization experience, and motivations for internet use. Following a review and inferences from the existing literature on cyber-victimology and internet use themes, the conceptual framework was developed. Afterward, a series of hypotheses about the relationships among the concepts were proposed.

The rest of the chapter proceeds: first, I restate the study's aim and objectives and summarize the research design in the following section. Next, I give an overview of the findings. I then follow this with a presentation of the theoretical, practical, and policy contributions. In the subsequent section, I examine the study's limitations and offer suggestions for future research before closing this study with concluding statements.

8.1 Restatement of Aims and Objectives

This research aimed to understand why Canadians continue to use the internet, notwithstanding the fear and persistent or inherent risk of victimization in cyberspace. The goal was to project this paradox within the limelight of Sociology's structure and agency discourse. After reviewing the pertinent literature, the constructs of interest in the study included fear of cybercrime victimization, risk of cybercrime, constrained internet use behavior, and cybercrime

victimization experience. The rest were cybercrime incident reporting, knowledge of cybercrime risk, frequency of internet use, and motivation for internet use. Socio-demographic factors were included as control constructs. Subsequently, seven secondary research questions were explored: to examine the ways socio-demographic characteristics affect the risk of cybercriminal victimization, to determine how prior cybercrime victimization experience affects the fear of future cybercrime victimization, to determine how cybercrime victimization experience affects the perceived risk of cybercrime, to investigate how victimization experience constrains internet use behavior, to examine the way cybercrime incident reporting affect fear of cybercrimes, to explore how internet use frequency constrains internet use behavior, and to understand the motivations for internet use among Canadian adults.

8.2 Summary of the Research Design

Technological developments have spurred massive transformations in society. Consequently, internet penetration is on the increase. It has become commonplace to the extent that internet use feels like an act of compulsive behavior, though such a conclusion equates internet use to addiction (Baumeister & Nadal, 2017). However, technological improvements have also created an opportunity for persons with deviant intentions to target unsuspecting internet users (Jaishankar, 2008). Online victimization is increasing with increasing self-reported incidents of victimization (Anderson, 2007; Internet Crime Control Centre, 2006; RCMP, 2014). At the same time, internet and computer use continue to grow (Arango et al., 2012). The above situation raises a profound paradox and warrants attention within a technologically driven society like Canada.

The study utilized a quasi-mixed method design comprising quantitative and qualitative questions deployed in an online survey. The research questions and associated hypotheses were

tested by analyzing results from the survey administered nationally in Canada. Ekos – a professional research vendor who supplies samples and interfaces with participants – recruited the sample by curating a subset of eligible participants from their existing panel assembled through random digit dialing. From this, Ekos procured a representative sample of Canadian respondents using random sampling. The survey questionnaire comprised 43 questions and was organized into ten sections (see Appendix A). The first section was about knowledge and perceptions of cybercrime risk, followed by sections on attitudes to cyber security, concerns about online transactions, and the impact of concerns on behavior. The next sections focused on cybercrime fear and its impact on behavior. The following sections examined victimization, reporting, and implications for behavior, followed by the place of internet use/access. Next followed questions about the frequency of internet use and its impact on behavior and motivations for internet use. The final section reviewed socio-demographic information. A total of 403 completed responses were recorded from the survey.

Descriptive analysis, consisting of frequency distribution and bivariate analysis, was used to analyze and present the descriptive information. Statistical modeling analysis, including logistic regression, was used to develop models for the outcome variables and analyze the statistical data. Finally, thematic (qualitative) analysis was used to analyze the qualitative data.

8.3 Summary of Findings

Four hundred and three (403) internet-using Canadian adults, consisting of about 80 % Anglophone speakers, participated in the study. A third of the participants were below age 40, and one-in-two (53 %) were males, while less than half had at least a university education. A tenth of the participants were non-White, while more than two-in-ten were single. Less than half of respondents earned less than $75,000 and were unemployed, respectively. Of the socio-

demographic factors, only gender, education, and marriage were significantly associated with cybercrime risk.

Contrary to the literature, victimization experience has a significantly negative association with fear, with prior victims expressing significantly lower odds of fear. The risk of cybercrime is also not significantly correlated with victimization experience. On the contrary, previously victimized internet users have a lower perception of cybercrime risk. With victimization, fear, and risk representing outcomes from actor agency interacting with structure, the findings suggest a call for theory modification and further probing. Also, although the univariable results indicate a positive association, the effect of victimization experience on internet behavior constraints (avoidance and defensive) is inconclusive. Moreover, the fear-incident reporting relationship could not be explored in the multivariable modeling stage since cybercrime incident reporting was not a candidate in the multivariable analysis stage. There is no conclusive link between incident reporting and fear of cybercrime.

Nonetheless, across all levels in the univariable analysis, incident reporting was associated with more than two times higher odds of fear as compared to the reference category, although only the likely to report category (OR = 3.03; 95 % CI: 1.01, 9.06) was statistically significant (see Table 5.7). Additionally, it is unclear whether internet use frequency constrains the behavior of internet users, even though the univariable results suggest frequent internet users have increased odds of adopting avoidance and defensive internet use actions. Finally, the motivations (developed as thematic components) of internet use among Canadian adults include education and knowledge acquisition, entertainment and fun, communication and social media access, commercial purposes, work, and personal-related use, news and information access, and others.

8.4 Theoretical Contributions of the Study

The goal of projecting the apparent paradox in internet use, fear, and inherent risk of victimization in cyberspace and outcomes in the sociological discourse of structure and agency has been achieved. The study confirms that an incipient interaction between structure and agency is prevalent in internet usage, its attendant outcomes of risk and fear, and behavioral responses regarding constrained internet use behavior. Furthermore, the study demonstrates that elements of structure and agency straddle Canadian adults' varying motivations for internet use while there also exist connections between motivation and risk, fear of cybercrime, avoidance internet, and defensive internet use. The study also reveals that gender, education, and marriage affect internet users' agency regarding cybercrime risk perception.

The broadening of constrained behaviour to encompass avoidance and defensive internet use within the context of internet use is one of the study's major contributions. One of the significant contributions of the current study is the expansion of constrained behavior to include both avoidance and defensive internet use within the context of internet use. To my knowledge, this is the first socio-criminological study to incorporate both aspects of constrained behavior within a single research study, thus filling a gap in the literature. As previously noted in the literature review section, the prevalent literature has tended to limit constrained behavior only to avoidance behaviors. For example, Böhme and Moore's (2012) study focused on only online service avoidance as a response to victimization, neglecting online defensive services or actions. Also, Saban et al. (2002) found that cybercrime victimization reduced consumer internet behavior, though not explicit, indicating an impact in the direction of service avoidance. However, I argued in this study that such a focus blurs reality and impacts theory and policy. As revealed by Rader et al. (2007) and Rader (2004), constrained behavior is a two-way street

comprising avoidance and defensive behaviors. In contrast to Böhme and Moore (2012) and Saban et al. (2002), and in line with Rader et al. (2007) and Rader (2004), the current study provides a broader focus in terms of projecting how victimization impacts not just avoidance, but equally defensive behavior.

In accordance with proponents of structural determinism, the study reveals that structures exert a deterministic effect, including internet use, as demonstrated by cybercrime victims having decreased odds of resorting to avoidance internet use behaviors. Avoiding certain kinds of internet activities is tantamount to diminishing the use-value of the internet. And this implies limited agency in the face of the overarching role of structure.

The study also adds to the literature by pointing to another dimension of agency: agency does not necessarily equate to action/ing; it can be spurred or constrained and means being passive and giving up control. The association between victimization experience and internet constraint behavior (avoidance and defensive) unearths the contributions.

Also, the current study, through the thematic analysis of internet use motivations, reinforces the argument about the need to rethink the structure-agency dichotomous discourse. The themes revealed the mutually reinforcing nature of structure and agency and suggested that the binary argument is no longer tenable. Instead, it is better to examine the nuances in the structure-agency dynamic.

And in sync with agency proponents, this study demonstrates that actor reflexivity is salient in internet users' intercourse with structure. The finding that frequent internet users are less likely to adopt defensive internet behavior than less frequent users is a highlight of reflexivity.

8.5 Practical and Policy Contributions of the Study

The results of this study can be applicable to other industrialized nations because the findings are representative of the Canadian population. Also, the results can be applied to developing countries where there are efforts to digitalize almost everything to follow the path of advanced societies. There is a more significant and profound dependency on the internet for virtually all activities in developed societies and increasingly in developing societies. As previously indicated, internet use is so widespread to such an extent that its use has become nearly an act of compulsive behavior.

The finding that victimized internet users have lower cybercrime risk perception has implications for cyberspace offending, victimization, and crime control. When the victimized perceive low risk, it potentially means they downplay their victimization, exposing people to further offenses in cyberspace. Conversely, the victimized may perceive less risk because they do not understand the nature of risk. Such a dearth of knowledge can cloud their anticipation and projection of cybercrime risk. In both scenarios, education about the nature of risk and the dangers of downplaying risks and victimization in cyberspace for internet users will be a helpful crime control strategy. Advocacy and sensitization campaigns across virtual and physical platforms will be needed.

The lack of support (inconclusive results) for the relationship between victimization and avoidance behavior has implications for practice and policy. Policy-wise, cyber-security stakeholders need to scale up efforts at developing friendly, affordable, but robust security patches and protocols to securitize cyberspace for internet users. Internet users will need this ‘big brother-esque' support from the state and private sector to ensure they are not overly exploited.

Such support can be achieved by increasing research and development allocations for cheap but effective software programs.

Also, the lack of support for the hypothesis that cybercrime victims are more likely to adopt defensive internet use activities has telling implications for policy. Empirically and in the realm of policy, policy interventions need to target social structural factors which can inhibit internet users' use of defensive behaviors. Information about preventive internet use techniques needs to be made easily accessible through advocacy programs. These targeted policy interventions will additionally serve as confidence-building measures to encourage users to access the internet safely and confidently.

The intricate interaction between agency and structural elements in internet users' varying thematic motivational components means that accessing the internet is a function of individual choice and factors or forces external to the individual. Additionally, it means that structures need to entice and encourage people to engender more internet use. Concurrent with the role of structures; however, individual actors also need to buy into the push, for example, by getting involved actively. More specifically, the Canadian National Cyber Security Strategy (2018) and the Action Plan (2019-2024) towards its realization will be better enhanced and more responsive if it incorporates the above findings. Education, advocacy, and sensitization about risk will be crucial. These need to be implemented alongside ongoing consultations with everyday Canadian internet users about their concerns and experiences of risk and victimization.

8.6 Limitations of the study

Several limitations must be considered in interpreting and drawing conclusions from this study. First, although the study sample is representative and statistically significantly suitable for this study (because of the rigorous probability-based sampling methods used to constitute the

sample pool), it is not necessarily generalizable to the Canadian population. Ekos' reach may still be limited. Nonetheless, the rigorous probability-based sampling methods used to curate the sample means inferences can be confidently made about the Canadian population.

Another potential limitation is the unequal number of Anglophone and Francophone responses. The study generated 321 Anglophone Canadian responses compared to 82 Francophone Canadian responses. The unequal responses make it difficult to compare the two language groups across relevant statistical metrics in the analysis. However, in hindsight, the unequal distribution of responses between Anglophone and Francophone Canadian respondents is not a significant limitation because there is an unequal distribution between the two official language groups across Canada, with the Anglophone group outnumbering their Francophone counterparts.

Moreover, the low number of responses generated by the qualitative question (309 answers) means extra caution must be exercised in interpreting the results, specifically about motivations for internet use. Besides the low number of responses, the qualitative results also lack quality and depth (richness). Some participant responses were too brief to elicit significant meaning and aid any meaningful (in-depth) analysis. The lack of depth in the responses was probably because the qualitative responses were collected with the quantitative data using a survey questionnaire. Nonetheless, the qualitative responses provide useful exploratory information about internet-using Canadians' underlying motivations for internet use.

A further methodological limitation related to the qualitative data was the challenge of conducting detailed disaggregated pattern and trend analysis within and between groups about Canadians' internet use motivations from the qualitative thematic analysis. This challenge was further heightened by the nature of the qualitative responses (brief, single words, phrases, and

sentence responses) and the manual analysis utilized. However, unlike quantitative research, qualitative thematic analysis is not intended to provide disaggregated patterns with statistical implications.

Finally, because the original study was developed purely as quantitative, it is possible that all the principles of mixed method research design have not been followed or applied in comprehensive terms. Nonetheless, the qualitative aspect was not a significant focus of the study, hence would not constitute a major methodological limitation.

8.7 Suggestions for Future Research

The mixed evidence in the extant literature and the negative association in the current study about the relationship between victimization and fear means further research is needed. Future research can explore this relationship by applying different theoretical standpoints.

Similarly, the lack of support for the victimization and cybercrime risk relationship also calls for further research. Alternatively, different theoretical frameworks can be applied to clarify the relationship further. This research can confirm whether the calls for theory modification are warranted.

Victimization experience and constrained internet behavior activities need to be replicated in further research, focusing on both aspects of constrained behavior – avoidance and defensive. Unlike Böhme and Moore (2012) and Saban et al. (2002), the current research took a giant step forward by incorporating defensive behavior. The inconclusive result of the study puts the limelight on the variables and presents opportunities for future research. For starters, the operationalization and measurement of these variables are worth a more thorough look. Also, deploying the study in a much larger sample size and in a different geographical setting could clarify the relationship between victimization and internet use behavior constraints.

Likewise, frequency and constrained internet use behavior also need to be explored further, focusing on both aspects of constrained behavior - avoidance and defensive. While the current study added to the literature by incorporating defensive internet use, unlike Böhme and Moore (2012) and Saban et al. (2002), the inconclusive results present opportunities for further research. For starters, the operationalization and measurement of these variables may be worth a thorough look. Also, deploying the study in a much larger sample size and a different geographical setting could be useful for understanding the relationship between internet use frequency and internet use behavior constrain.

Furthermore, the lack of clarity in the current study's fear of cybercrime and incident reporting relationship identifies a valuable niche for future research. While the low incidence of cybercrime reporting is unmistakable and fairly established in the literature, studies assessing the relationship between cybercrime fear and incident reporting are palpably missing. The current study added to the extant literature by examining the association between the fear of cybercrime and cybercrime incident reporting.

Finally, future research should consider testing the thematic motivational components as constructs of internet use motivation. Quantitatively, this can be done by employing factor analysis and confirmatory factor analysis, among other techniques. Relatedly, future research can also explore correlating the thematic internet use motivations with risk of victimization, fear of cybercrime, avoidance internet use, and defensive internet use behaviors.

8.8 Conclusion

This was a national study (i.e., Canada-wide). It was exploratory in terms of both the research problem and the themes addressed. The research problem explored whether the perception of cybercrime changed how Canadians use the internet. The themes included fear of

cybercrime victimization, risk of cybercrime, constrained internet use behavior, and cybercrime victimization experience. Additional themes were cybercrime incident reporting, knowledge of cybercrime risk, frequency of internet use, and motivation for internet use. The findings highlighted some note-worthy paradoxes in cybercrime risk, victimization, and internet use behavioral actions. The results serve to identify a critical gap that requires further studies and invites more detailed examinations of the significance of the issues revealed in the current study.

References

Abbott, J., & McGrath, S. A. (2017). The effect of victimization severity on perceived risk of victimization: Analyses using an international sample. *Victims & Offenders, 12*(4), 587-609. https://doi.org/10.1080/15564886.2016.1208130

Abdulai, M. A. (2020). Examining the effect of victimization experience on fear of cybercrime: University students' experience of credit/debit card fraud. *International Journal of Cyber Criminology*, *14*(1), 157-174. DOI: 10.5281/zenodo.3749468

Abdulai, M. (2016). *Determinants of fear of cybercrime victimization: A study of credit/debit card fraud among students of the University of Saskatchewan* (Masters thesis, University of Saskatchewan).

Accenture. (2017). *Accenture Canada cybercrime survey 2017.* Accessed September 13, 2019, from https://www.accenture.com/ca-en/company-news-release-canada-cybercrime-survey-2017

Accenture Security. (March 6, 2019). Ninth annual cost of cybercrime study. Accessed September 13, 2019, from https://www.accenture.com/_acnmedia/accenture/redesignassets/dotcom/documents/local/1/accenture-ninth-annual-cost-cybercrime-canadai-nfographic-v2.pdf#zoom=50

Adams, J., & Trinitapoli, J. (2009). The Malawi religion project: Data collection and selected analyses. *Demographic Research*, *21*(10), 255-288. DOI: 10.4054/DemRes.2009.21.10

Adler, P. A., & Adler, P. (2006). The Deviance society. *Deviant Behavior, 27*(2), 129-148. https://doi.org/10.1080/15330150500468444

Adom, D., Hussein, E. K., & Agyem, J. A. (2018). Theoretical and conceptual framework: Mandatory ingredients of a quality research. *International Journal of Scientific Research*, *7*(1), 438-441.

Alshalan, A. (2006). *Cyber-crime fear and victimization: An analysis of a national survey*. ProQuest.

Anderson, J. (1987). Structural equation models in the social and behavioral sciences: Model building. *Child Development*, 58(1), 49-64. Doi: 10.2307/1130291

Anderson, K. B. (2007). *Consumer fraud in the United States: The second FTC survey*. Washington: Federal Trade Commission.

Andrews, K. T. (2001). Social movements and policy implementation: The Mississippi civil rights movement and the war on poverty, 1965 to 1971. *American Sociological Review*, 71-95. DOI: 10.2307/2657394

Arango, C., Huynh, K. P., Fung, B., & Stuber, G. (2012). The changing landscape for retail payments in Canada and the Implications for the demand for cash. *Bank of Canada Review, 2012* (Autumn), 31-40.

Archer, M. S., & Archer, M. S. (1996). *Culture and agency: The place of culture in social theory*. Cambridge University Press.

Australian Bureau of Statistics. (2008). *Personal fraud 2007*. Author

Axinn, W. G., & Pearce, L. D. (2006). *Mixed method data collection strategies*. New York: Cambridge University Press.

Barker, V. (2009). Older adolescents' motivations for social network site use: The influence of gender, group identity, and collective self-esteem. *Cyberpsychology & behavior*, *12*(2), 209-213. https://doi.org/10.1089/cpb.2008.0228

Bauman, Z. (2000). *Liquid Modernity*. Polity Press.

Bauman, Z. (2006). *Liquid fear*. Polity Press.

Baumeister, R. F., & Nadal, A. C. (2017). Addiction: Motivation, action control, and habits of pleasure. *Motivation Science*, *3*(3), 179.

Beck, U. (1992). *Risk society: Towards a new modernity* (R. Mark Trans.). Sage Publications.

Becker, H. S., Geer, B., Hughes, E. C., & Strauss, A. L. (1961). *Boys in white*. University of Chicago Press.

Bhatnagar, A., Misra, S., & Rao, H. R. (2000). *On risk, convenience, and internet shopping behavior: Why some Consumers are online shoppers while others are not*. Communications of the Association for Computing Machinery 33:98-105.

Bidgoli, M. (2015). *A Mixed Methods approach to understanding undergraduate Students' victimization, perceptions, and reporting of cybercrimes*. University of California.

Bidgoli, & Grossklags, J. (2016). End user cybercrime reporting: What we know and what we can do to improve it. *2016 IEEE International Conference on Cybercrime and Computer Forensic, ICCCF 2016*. (pp. 1-6). https://doi.org/10.1109/ICCCF.2016.7740424

Bilodeau, H., Lari, M., & Uhrbach, M. (2019). Cyber security and cybercrime challenges of Canadian businesses, 2017. *Juristat: Canadian Centre for Justice Statistics*, 1-18.

Böhme, R., & Moore, T. (2012, October). How do consumers react to cybercrime? In *2012 eCrime Researchers Summit* (pp. 1-12). IEEE.

Bourdieu, P. (2004). *Science of science and reflexivity*. Stanford University Press.

Boyatzis, R. E. (1998). *Transforming qualitative information: Thematic analysis and code development*. Sage.

Brands, J., & Van Doorn, J. (2022). The measurement, intensity and determinants of fear of cybercrime: A systematic review. *Computers in Human Behavior*, *127*, 107082. https://doi.org/10.1016/j.chb.2021.107082

Brands, J., & van Wilsem, J. (2021). Connected and fearful? Exploring fear of online financial crime, Internet behaviour and their relationship. *European Journal of Criminology*, *18*(2), 213-234. DOI: 10.1177/1477370819839619

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*(2), 77-101. https://doi.org/10.1191/1478088706qp063oa

Bryman, A., Bell, E., & Teevan, J. J. (2012). *Social research methods: Third Canadian edition*. Oxford University Press.

Burgard, A., & Schlembach, C. (2013). Frames of fraud: A qualitative analysis of the structure and process of victimization on the internet. *International Journal of Cyber Criminology*, *7*(2).

Canada Revenue Agency. (September 17, 2020). *Cyber incidents*. Accessed August 2, 2022, from https://www.canada.ca/en/revenue-agency/news/2020/09/cyber-incidents.html

Calhoun, C., J. Gerteis, J. Moody, S. Pfaff, and I. Virk. (Eds). (2012). *Contemporary Sociological Theory* (3rd Ed.) Wiley-Blackwell.

CBS (2018). Veiligheidsmonitor 2017. Den Haag/Heerlen/Bonaire, Den Haag: Centraal Bureau voor deStatistiek.

Cao, J. (2012). *A structural equation model of customers' behavioural intentions in the Chinese restaurant sector* (Publication No. 10049261) [Doctoral dissertation, Newcastle University]. ProQuest Dissertations & Theses Global.

Centre for Forensic Behavioral Science and Justice Studies. (2014). *Saskatchewan Crime Survey*. University of Saskatchewan. Retrieved https://cfbsjs.usask.ca/project-articles/current-project-articles/saskatchewan-crime-survey.php

Chadee, D., Ng Ying, N. K., Chadee, M., & Heath, L. (2019). Fear of crime: The influence of general fear, risk, and time perspective. *Journal of Interpersonal Violence*, *34*(6), 1224-1246. https://doi.org/10.1177%2F0886260516650970

Chawki, M., Darwish, A., Khan, M. A., & Tyagi, S. (2015). *Cybercrime, digital forensics and jurisdiction* (Vol. 593). Springer.

Chen, Q., Yuan, Y., Feng, Y. & Archer, N. (2021). A decision paradox: benefit vs risk and trust vs distrust for online dating adoption vs non-adoption. *Internet Research*, *31*(1), 341-375. https://doi.org/10.1108/INTR-07-2019-0304

Cherlin, A. J., Burton, L. M., Hurt, T. R., & Purvin, D. M. (2004). The influence of physical and sexual abuse on marriage and cohabitation. *American Sociological Review, 69*(6), 768-789. DOI: 10.1177/000312240406900602

Choi, J., Kruis, N. E., & Choo, K. S. (2021). Explaining fear of identity theft victimization using a routine activity approach. *Journal of Contemporary Criminal Justice*, *37*(3), 406-426. DOI: 10.1177/10439862211001627

Clement, J. (February, 2019). *Internet usage in Canada – statistics & facts*. Statista. Retrieved October 15, 2019, from https://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_423_en.pdf

Clement, J. (July, 2019). *Most popular online activities among internet users in Canada as of March 2019*. Statista. Retrieved October 15, 2019, from https://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_423_en.pdf

Clement, J. (January, 2019). *Average weekly time spent online in Canada from 2015 to 2018 (in hours)*. Statista. Retrieved October 15, 2019, from https://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_423_en.pdf

Coleman, J. S. (1990). *Foundations of Social Theory*. Belknap Press of Harvard University Press.

Collins, R. E. (2016). Addressing the inconsistencies in fear of crime research: A meta-analytic review. *Journal of Criminal Justice*, *47*, 21-31. https://doi.org/10.1016/j.jcrimjus.2016.06.004

Costello, A. B., & Osborne, J. (2005). Best practices in exploratory factor analysis: Four recommendations for getting the most from your analysis. *Practical Assessment, Research & Evaluation, 10*, 7. http://cyber.usask.ca/login?url=https://www.proquest.com/docview/2366831151?accountid=14739

Creative Research Systems, (2012). *Sample size calculator*. Retrieved from http://www.surveysystem.com/sscalc.htm

Creswell, J. W. (2003). *Research design: Quantitative, qualitative, and mixed methods approaches*. Sage.

Cross, C., Richards, K., & Smith, R. G. (2016). The reporting experiences and support needs of victims of online fraud. *Trends and Issues in Crime and Criminal Justice*, (518), 1-14. https://doi.org/10.3316/informit.300566903591621

DataReportal. (January 26, 2022). *Digital 2022: Global overview report*. Accessed July 14, 2022, from https://datareportal.com/reports/digital-2022-global-overview-report?utm_source=DataReportal&utm_medium=Country_Article_Hyperlink&utm_campaign=Digital_2022&utm_term=Canada&utm_content=Global_Promo_Block

DataReportal. (February 9, 2022). *Digital 2022: Canada*. Accessed July 14, 2022, from https://datareportal.com/reports/digital-2022-canada

Durkheim, E. (1938). The rules of sociological method, trans. *G. Catlin (Glencoe, Illinois: Free Press, 1938), 18.*

Elhai, J. D., Levine, J. C., & Hall, B. J. (2017). Anxiety about electronic data hacking: Predictors and relations with digital privacy protection behavior. *Internet Research*. *27*(3), 631-649. DOI 10.1108/IntR-03-2016-0070

Eurostat. (2017). *Digital economy and society statistics - households and individuals*. Accessed on April 03, 2019 from https://ec.europa.eu/eurostat/statistics-

explained/index.php?title=Digital_economy_and_society_statistics_-_households_and_individuals#Internet_access

Farrall, S. D., Jackson, J., & Gray, E. (2009). *Social order and the fear of crime in contemporary times*. Oxford University Press.

Ferraro, K. F. (1995). *Fear of Crime: Interpreting Victimization Risk*. State University of New York Press.

Ferraro, K. F., & LaGrange, R. (1987). The measurement of fear of crime. *Sociological Inquiry*, *57*(1), 70–101. https://doi.org/10.1111/j.1475-682X.1987.tb01181.x

Fletcher, N. (2007). Challenges for regulating financial fraud in cyberspace. *Journal of Financial Crime, 14*(2), 190-207.

Fox, S., & Lewis, O. (2001). Fear of online crime: Americans support FBI interception of criminal suspects' email and news laws to protect online privacy. *Pew Internet Tracking Report.*

Fulton, S. & Krainovich-Miller, B. (2010). Gathering and Appraising the Literature. In LoBiondo-Wood, G. & Haber, J. (Eds). *Nursing Research: Methods and Critical Appraisal for Evidence-Based Practice* (7th Edition). Mosby Elsevier.

Gainey, R., Alper, M., & Chappell, A. T. (2011). Fear of crime revisited: Examining the direct and indirect effects of disorder, risk perception, and social capital. *American Journal of Criminal Justice, 36*(2), 120-137. DOI 10.1007/s12103-010-9089-8

Garbarino, E., & Strahilevitz, M. (2004). Gender differences in the perceived risk of buying online and the effects of receiving a site recommendation. *Journal of Business Research*, *57*(7), 768-775. DOI:10.1016/S0148-2963(02)00363-6

Garofalo, J. (1981). The fear of crime: Causes and consequences. The *Journal of Criminal Law & Criminology*, *72*(2), 839-857. https://doi.org/10.2307/1143018

Gau, J. (2010). Basic principles and practices of structural equation modeling in criminal justice and criminology research. *Journal of Criminal Justice Education*, *21*(2), 136-151 DOI: 10.1080/10511251003693660

Giddens, A. (1984). *The constitution of Society: Outline of the theory of structuration.* University of California Press.

Goodman, M. D., & Brenner, S. W. (2002). The emerging consensus on criminal conduct in cyberspace. *International Journal of Law and Information Technology*, *10*(2), 139-223.

Gordon, S., & Ford, R. (2006). On the definition and classification of cybercrime. *Journal in Computer Virology*, *2*(1), 13-20.

Goucher, W. (2010). Being a cybercrime victim. *Computer Fraud & Security*, *2010*(10), 16-18. https://doi.org/10.1016/S1361-3723(10)70134-2

Goudriaan, H., Lynch, J. P., & Nieuwbeerta, P. (2004). Reporting to the police in western nations: A theoretical analysis of the effects of social context. *Justice Quarterly*, *21*(4), 933-969. https://doi.org/10.1080/07418820400096041

Grabosky, P. (2004). The global dimension of cybercrime. *Global Crime*, *6*(1), 146-157.

Grant, C., & Osanloo, A. (2014). Understanding, selecting, and integrating a theoretical framework in dissertation research: Creating the blueprint for your "House". *Administrative Issues Journal: Education, Practice, and Research, 4*(2), 12-26. DOI: 10.5929/2014.4.2.9

Grau, J. (2008). *CanadaB2C E-Commerce: A work in progress*. eMarketer.

Hair, J. F., Black, W. C., Babin, B. J., Anderson, R. E., & Tatham, R. L. (2006). *Multivariate data analysis* 6th Edition. Pearson Prentice Hall.

Hale, C. (1996). Fear of crime: A review of the literature. *International Review of Victimology, 4*(2), 79-150. https://doi.org/10.1177/026975809600400201

Hanson, B. (2008). Wither qualitative/quantitative? Grounds for methodological convergence. *Quality & Quantity*, *42*(1), 97-111. DOI 10.1007/s11135-006-9041-7

Henson, B., Reyns, B. W., & Fisher, B. S. (2013). Fear of crime online? Examining the effect of risk, previous victimization, and exposure on fear of online interpersonal victimization. *Journal of Contemporary Criminal Justice, 29*(4), 475-497.

Hinkle, J. C. (2015). Emotional fear of crime vs. Perceived safety and risk: Implications for measuring “fear” and testing the Broken Windows Thesis. *American Journal of Criminal Justice, 40*(1), 147-168. https://doi.org/10.1007/s12103-014-9243-9

Holloway, I., & Todres, L. (2003). The status of method: flexibility, consistency and coherence. *Qualitative Research, 3*(3), 345-357. https://doi.org/10.1177/1468794103033004

Holt, T. J., & Bossler, A. M. (2008). Examining the applicability of lifestyle-routine activities theory for cybercrime victimization. *Deviant Behavior, 30*(1), 1-25.

Horrigan, J. B. (2008). *Online shopping*. Washington: Pew Internet and American Life Project.

Hosmer, D.W., Lemeshow, S., Sturdivant, R.X. (2013). Model-building strategies and methods for logistic regression. In *Applied Logistic Regression* (3rd Ed) (pp. 89-144). John Wiley & Sons Inc.

Ibrahim, S. (2016). Social and contextual taxonomy of cybercrime: Socioeconomic theory of Nigerian cybercriminals. *International Journal of Law, Crime and Justice*, *47*, 44-57.

Imenda, S. (2014). Is there a conceptual difference between theoretical and conceptual frameworks? *Journal of Social Sciences*, *38*(2), 185-195. DOI: 10.1080/09718923.2014.11893249

Internet Crime Complaint Center. (2006). *Internet crime report*. Washington, DC: The National White Collar Crime Center and the Federal Bureau of Investigation.

Jahankhani, H., & Al-Nemrat, A. (2011). Cybercrime profiling and trend analysis. In *Intelligence Management* (pp. 181-197). Springer, London.

Jaishankar, K. (2008). Space transition theory of cyber crimes. *Crimes of the Internet*, 283-301.

Joas, H., & Knöbl, W. (2009). *Social theory: Twenty introductory lectures*. Cambridge University Press.

Joiner, R., Gavin, J., Duffield, J., Brosnan, M., Crook, C., Durndell, A., Maras, P., Miller, J., Scott, A. J., & Lovatt, P. (2005). Gender, Internet Identification, and Internet Anxiety: Correlates of internet use. *Cyberpsychology & Behavior*, *8*(4), 371–378. https://doi.org/10.1089/cpb.2005.8.371

Kelly, L. M., & Cordeiro, M. (2020). Three principles of pragmatism for research on organizational processes. *Methodological Innovations*, *13*(2), 1-10. https://doi.org/10.1177/2059799120937242

King, N. (2004). Using templates in the thematic analysis of text. In C. Cassell & G. Symon (Eds.), *Essential guide to qualitative methods in organizational research* (pp. 257–270). Sage.

Kraemer-Mbula, E., Tang, P., & Rush, H. (2013). The cybercrime ecosystem: Online innovation in the shadows? *Technological Forecasting and Social Change*, *80*(3), 541-555.

Kshetri, N. (2010). *The global cybercrime industry: economic, institutional and strategic perspectives*. Springer Science & Business Media.

Kuhn, Thomas. S. (1970). *Structure of Scientific Revolutions*. University of Chicago Press.

Lee, S. S., Choi, K. S., Choi, S., & Englander, E. (2019). A test of structural model for fear of crime in social networking sites. *International Journal of Cybersecurity Intelligence & Cybercrime*, *2*(2), 5-22. https://www.doi.org/10.52306/02020219SVZL9707

Lee, M., & Mythen, G. (Eds.). (2017). *The Routledge international handbook on fear of crime*. Routledge.

LeFebvre, R. (2012). The human element in cyber security: A study on student motivation to act. In *Proceedings of the 2012 Information Security Curriculum Development Conference*, 1–8. https://doi.org/10.1145/2390317.2390318

Liebermann, Y., & Stashevsky, S. (2002). Perceived risks as barriers to Internet and e-commerce usage. *Qualitative Market Research: An International Journal*, *5*(4), 291-300. DOI: 10.1108/13522750210443245

Liehr, P., & Smith, M. J. (1999). Middle range theory: Spinning research and practice to create knowledge for the new millennium. *Advances in Nursing Science*, *21*(4), 81-91. DOI: 10.1097/00012272-199906000-00011

Li, X. (2017). A review of motivations of illegal cyber activities. *Kriminologija & socijalna integracija: časopis za kriminologiju, penologiju i poremećaje u ponašanju*, *25*(1), 110-126.

Lieberson, S. (1992). Einstein, Renoir, and Greeley: Some thoughts about evidence in sociology. *American Sociological Review, 57*(1), 1-15. https://doi.org/10.2307/2096141

Liska, A. E., Sanchirico, A., & Reed, M. D. (1988). Fear of crime and constrained behavior specifying and estimating a reciprocal effects model. *Social Forces*, *66*(3), 827-837.

Lipset, S. M., Trow, M., & Coleman, J. S. (1956). *Union democracy: The internal politics of the International Typographical Union.* New York: New York Free Press.

Logan, T. K., & Walker, R. (2017). The gender safety gap: Examining the impact of victimization history, perceived risk, and personal control. *Journal of interpersonal violence*, https://doi.org/10.1177%2F0886260517729405

Marcum, C., Higgins, G., & Ricketts, M. (2010). Potential factors of online victimization of youth: An examination of adolescent online behaviors utilizing Routine Activity Theory. *Deviant Behavior*, *31*(5), 381-410.

Mazzocchi, M. (2008). *Statistics for marketing and consumer research*. Sage.

McAnulla, S. (2002). Structure and agency. *Theory and methods in political science*, *2*, 271-91

McGarrell, E. F., Giacomazzi, A. L., & Thurman, Q. C. (1997). Neighborhood disorder, integration, and the fear of crime. *Justice Quarterly*, *14*(3), 479-500. DOI: 10.1080/07418829700093441

Miles, M. B., & Huberman, A. M. (1994). *Qualitative data analysis: An expanded sourcebook.* Newbury Park, CA: Sage.

Mitchell, K. J., Finkelhor, D., & Wolak, J. (2003). The exposure of youth to unwanted sexual material on the internet: A national survey of risk, impact, and prevention. *Youth & Society, 34*(3), 330-58.

Morgan, D. L. (2007). Paradigms lost and pragmatism regained: Methodological implications of combining qualitative and quantitative methods. *Journal of Mixed Methods Research, 1*(1), 48-76. DOI: 10.1177/2345678906292462

Ngafeeson, M. (2010). Cybercrime classification: a motivational model. *College of Business Administration, The University of Texas-Pan American*, *1201*.

Nielsen Online. (2008). *Nielsen Online Reports Topline U.S. data for March 2008*. Nielsen Company.

Nowell, L. S., Norris, J. M., White, D. E., & Moules, N. J. (2017). Thematic analysis: Striving to meet the trustworthiness criteria. *International Journal of Qualitative Methods*, *16*(1), DOI: 10.1177/1609406917733847

Office for National Statistics. (December 2018). *Crime in England and Wales: Year ending December 2018*. Statistical Bulletin. Accessed May 1, 2018, at https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingdecember2018

Office for National Statistics. (September 2018). *Crime in England and Wales: Year ending September 2018*. Statistical Bulletin. Accessed April 30, 2019, at https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingseptember2018#computer-misuse-offences-show-a-decrease-in-computer-viruses

Okonkwo, A. D. (2013). Generational perspectives of unprotected sex and sustainable behavior change in Nigeria. *Sage Open*, *3*(1), 2158244012472346.

Papacharissi, Z., & Rubin, A. M. (2000). Predictors of Internet Use. *Journal of Broadcasting & Electronic Media*, *44*(2), 175–196. https://doi.org/10.1207/s15506878jobem4402_2

Parrado, E. A., McQuiston, C., & Flippen, C. A. (2005). Participatory survey research: Integrating community collaboration and quantitative methods for the study of gender and HIV risks among Hispanic migrants. *Sociological Methods and Research, 34*(2), 204-239. DOI: 10.1177/0049124105280202

Parsons, T. (1954). *Essays in sociological theory* (Rev. ed.). Free Press.

Pearce, L. D. (2012). Mixed methods inquiry in Sociology. *American Behavioral Scientist*, *56*(6), 829-848. DOI: 10.1177/0002764211433798

Perry, G. K. (2009). Exploring occupational stereotyping in the new economy: The intersectional tradition meets mixed methods research. In M. T. Berger & K. Guidroz (Eds.), *The Intersectional Approach: Transforming the Academy Through Race, Class, and Gender* (pp. 229-245). University of North Carolina Press.

Pereira, F., Spitzberg, B. H., & Matos, M. (2016). Cyber-harassment victimization in Portugal: Prevalence, fear and help-seeking among adolescents. *Computers in Human Behavior*, *62*, 136-146. doi.org/10.1016/j.chb.2016.03.039

Pfluke, C. (2019). A history of the five eyes alliance: possibility for reform and additions: a history of the five eyes alliance: possibility for reform and additions. *Comparative Strategy*, *38*(4), 302-315. https://doi.org/10.1080/01495933.2019.1633186

Poushter, J., Bishop, C., & Chwe, H. (2018). Social media use continues to rise in developing countries but plateaus across developed ones. *Pew Research Center*, *22*.

Pratt, T., Holtfreter, K., & Reisig, M. (2010). Routine online activity and internet fraud targeting: Extending the generality of Routine Activity Theory. *The Journal of Research in Crime and Delinquency*, *47*(3), 267-296.

Public Safety Canada. (2019). *National cyber security action plan (2019-2024).* Accessed September 1, 2022, from https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg-2019/ntnl-cbr-scrt-strtg-2019-en.pdf

Public Safety Canada. (2018). *National cyber security strategy: Canada's vision for security and prosperity in the digital age*. Accessed September 1, 2022, from https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/ntnl-cbr-scrt-strtg-en.pdf

Qian, Y. (2021). Disruption or reproduction? Nativity, gender and online dating in Canada. *Internet Research*, *32*(4), 1264-1287. https://doi.org/10.1108/INTR-10-2020-0547

Rader, N. E., May, D. C., & Goodrum, S. (2007). An empirical assessment of the "threat of victimization:" Considering fear of crime, perceived risk, avoidance, and defensive behaviors. *Sociological Spectrum*, *27*(5), 475-505. DOI: 10.1080/02732170701434591

Rader, N. E. (2004). The threat of victimization: A theoretical reconceptualization of fear of crime. *Sociological Spectrum*, *24*(6), 689-704. DOI: 10.1080/02732170490467936

Reisig, M. D., Pratt, T. C., & Holtfreter, K. (2009). Perceived risk of internet theft victimization: Examining the effects of social vulnerability and financial impulsivity. *Criminal Justice and Behavior*, *36*(4), 369-384. DOI: 10.1177/0093854808329405

Riek, M., Böhme, R., & Moore, T. (2015). Measuring the influence of perceived cybercrime risk on online service avoidance. *IEEE Transactions on Dependable and Secure Computing, 13*(2), 261-273.

Roberts, L. D., Indermaur, D., & Spiranovic, C. (2013). Fear of cyber-identity theft and related fraudulent activity. *Psychiatry, Psychology and Law, 20*(3), 315-328.

Royal Canadian Mounted Police. (2014). *Cybercrime: An overview of incidents and issues in Canada*. Accessed September 12, 2019, from http://www.rcmp-grc.gc.ca/wam/media/1090/original/ea3c6b40418cad578c40d403b24cda43.pdf

Royal Canadian Mounted Police. (2015). *Royal Canadian Mounted Police cybercrime strategy*. Accessed October 8, 2019, from http://www.rcmp-grc.gc.ca/wam/media/1088/original/30534bf0b95ec362a454c35f154da496.pdf

Russo, S., & Roccato, M. (2010). How long does victimization foster fear of crime? A longitudinal study. *Journal of Community Psychology*, *38*(8), 960-974. DOI: 10.1002/jcop.20408

Saban, K. A., McGivern, E., & Saykiewicz, J. N. (2002). A critical look at the impact of cybercrime on consumer internet behavior. *Journal of Marketing Theory and Practice*, *10*(2), 29-37. DOI: 10.1080/10696679.2002.11501914

Sanger, D., Long, A., Ritzman, M., Stofer, K., & Davis, C. (2004). Opinions of female juvenile delinquents about their interactions in chat rooms. *Journal of Correctional Education, 55*(2), 120-131.

Schwartz, P., & Velotta, N. (2018). Online dating: changing intimacy one swipe at a time? In Van Hook, J., McHale, S.M. & King, V. (Eds), *Families and Technology*, Springer, Cham, pp. 57-88.

Sinclair, Marlene. (2007). A guide to understanding theoretical and conceptual frameworks. *Evidence-Based Midwifery (Royal College of Midwives)*, *5*(2), 39.

Skogan, W. G. (1987). The impact of victimization on fear. *Crime & Delinquency*, *33*(1), 135-154.

Small, M. L. (2009). "How many cases do I need?" On science and the logic of case selection in field-based research. *Ethnography*, *10*(1), 5-38. DOI: 10.1177/1466138108099586

Smith, A., & Anderson, M. (2016). Online shopping and e-commerce. *Pew Research Center.*

Smyth, S. M. (2010). *Cybercrime in Canadian criminal law*. Toronto: Carswell.

Social Science Research Laboratories. (n.d.). SSRL Saskatchewan community panel. Retrieved from http://ssrl.usask.ca/sask_panel.php#WhatistheSaskatchewanCommunityPanel

Statistics Canada. (October 14, 2020). *Canadians spend more money and time online during pandemic and over two-fifths report a cyber incident*. The Daily. Accessed on July 14, 2022, at https://www150.statcan.gc.ca/n1/daily-quotidien/201014/dq201014a-eng.pdf

Statistics Canada. (2019). Annual demographic estimates: Canada, provinces and territories, 2019. (Catalogue number: 11-627-M). Retrieved October 2, 2019, from https://www150.statcan.gc.ca/n1/en/pub/11-627-m/11-627-m2019061-eng.pdf?st=qhMrGHbE

Statistics Canada. (December 2019). *Just the facts: Cybercrime in Canada*. Accessed July 15, 2022, from https://www150.statcan.gc.ca/n1/pub/89-28-0001/2018001/article/00015-eng.htm

Statistics Canada. (May 2017a). Table 27-10-0018-01 Internet use by frequency of use, age group and sex DOI**:** https://doi.org/10.25318/2710001801-eng Accessed July 14, 2022, at https://www150.statcan.gc.ca/t1/tbl1/en/tv.action?pid=2710001801

Statistics Canada. (May 2017b). Table 22-10-0026-01 Internet use, by location and frequency of use DOI**:** https://doi.org/10.25318/2210002601-eng Accessed July 14, 2022, at https://www150.statcan.gc.ca/t1/tbl1/en/cv.action?pid=2210002601

StatsCan. (2009). *Internet shopping in Canada: An examination of data, trends and patterns* (Publication no. 88F0006X). Retrieved from Statistics Canada website: http://www.statcan.gc.ca/pub/88f0006x/2009005/part-partie1-eng.htm.

Stones, R. (2005). *Structuration theory*. Macmillan International Higher Education.

Sukhai, N. B. (2004, October). Hacking and cybercrime. In *Proceedings of the 1st annual conference on Information security curriculum development* (pp. 128-132). ACM.

Symantec Corporation. (2018). *2017 Norton Cyber Security Insights Reports: Global results*. Retrieved from 2017 Norton Cyber Security Insights Report | NortonLifeLock

TNS Opinion & Social. (2015). *Special Eurobarometer 423. Cyber security report*. Retrieved October 15, 2019, from https://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_423_en.pdf

Trinitapoli, J. (2007). "I Know this isn't PC, but...": Religious exclusivism among US adolescents. *Sociological Quarterly*, *48*(3), 451-483. Doi: 10.1111/j.1533-8525.2007.00085.x

Turner, J. H. (2014). *Theoretical Sociology: A Concise Introduction to Twelve Sociological Theories*. Sage.

Tyler, T. R. (1984). Assessing the risk of crime victimization: The integration of personal victimization experience and socially transmitted information. *Journal of Social Issues, 40*(1), 27-38.

U.S. Census Bureau. (2008). *Projected online retail sales*. Washington, DC: U.S. Census Bureau, Housing and Household Economic Statistics Division.

U.S. Department of Commerce. (2008). *U.S. Census Bureau news: Quarterly retail e-commerce sales, 4th quarter 2007*. Washington, DC: U.S. Department of Commerce.

Van Der Meer, S. (2015). Enhancing international cyber security: A key role for diplomacy. *Security and Human Rights, 26*(2-4), 193-205.

van de Weijer, S., Leukfeldt, R., & Van der Zee, S. (2020). Reporting cybercrime victimization: determinants, motives, and previous experiences. *Policing: An International Journal*. 43(1), 17-34. Doi: 10.1108/PIJPSM-07-2019-0122

Van De Weijer, S. G., & Leukfeldt, E. R. (2017). Big five personality traits of cybercrime victims. *Cyberpsychology, Behavior, and Social Networking, 20*(7), 407-412. DOI: 10.1089/cyber.2017.0028

Van Wilsem, J. (2011). Bought it, but never got it: Assessing risk factors for online consumer fraud victimization. *European Sociological Review, 29*(2), 168-178.

Virtanen, S. M. (2017). Fear of cybercrime in Europe: Examining the effects of victimization and vulnerabilities. *Psychiatry, Psychology and Law, 24*(3), 323-338. DOI:10.1080/13218719.2017.1315785

Visser, M., Scholte, M., & Scheepers, P. (2013). Fear of crime and feelings of unsafety in European countries: Macro and micro explanations in cross-national perspective. *The Sociological Quarterly, 54*(2), 278-301.

Wall, D. S. (2008). Cybercrime, media and insecurity: The shaping of public perceptions of cybercrime. *International Review of Law, Computers & Technology, 22*(1-2), 45-63. DOI: 10.1080/13600860801924907

Weber, M. (1978). *Economy and society: An outline of interpretive sociology* (Vol. 2). University of California press.

Weinrath, M., & Gartrell, J. (1996). Victimization and fear of crime. *Violence and Victims, 11*(3), 187.

Wolf, E., Harrington, K., Clark, S., & Miller, M. (2013). Sample size requirements for structural equation models: An Evaluation of Power, Bias, and Solution Propriety. *Educational and Psychological Measurement, 76*(6), 913-934. https://doi-org.cyber.usask.ca/10.1177%2F0013164413495237

Yang, S., & Wyckoff, L. A. (2010). Perceptions of safety and victimization: Does survey construction affect perceptions? *Journal of Experimental Criminology, 6*, 293-323. doi:10.1007/s11292-010-9100-x

Yar, M. (2013). *Cybercrime and the Internet, 2nd ed*. Sage.

Yazdanifard, R., Oyegoke, T., & Seyedi, A. P. (2011). Cyber-crimes: Challenges of the millennium age. In *Advances in Electrical Engineering and Electrical Machines* (pp. 527-534). Springer, Berlin, Heidelberg.

Ybarra, M., Mitchell, K., Finkelhor, D., & Wolak, J. (2007). Internet prevention messages: Targeting the right online behaviors. *Archives of Pediatrics & Adolescent Medicine, 161*(2), 138-45.

Yu, S. (2014). Fear of cyber crime among college students in the United States: An exploratory study. *International Journal of Cyber Criminology*, *8*(1).

Appendix A: Questionnaire

Questionnaire

A Study into the Paradox of Cybercrime Risk and Internet Use

For this study, cybercrime is defined as any "criminal activity in which computers or computer networks are the principal means of committing an offense or violating laws, rules, or regulations" (Kshetri, 2010, p. 3).

Awareness and Experience of Cybercrime:

Knowledge/Perception of Cybercrime Risk: for all respondents

1. How do you rate your current knowledge about the risk of cybercrime?
    a. Excellent
    b. Good
    c. Fair
    d. Poor
    e. Very poor
2. In your view over the last couple of years, do you think cybercrime is …
    a. Increasing
    b. Decreasing
    c. Stable
    d. Do not know
3. What is your source of cybercrime information? (Please select all that apply)
    a. Media (television, radio, newspaper)
    b. Internet
    c. Friends/colleagues
    d. Other (please specify) …
4. To what extent have you experienced violent crimes (e.g., physical assault, burglary etc.) in the past 12 months?
    a. Never
    b. Seldom
    c. Sometimes
    d. Often

e. Always

5. Indicate your agreement with this statement: Compared to violent crimes, I feel more at risk of cybercrime (e.g., bank fraud, cyber pornography etc.).?
   a. Strongly agree
   b. Agree
   c. Neutral
   d. Disagree
   e. Strongly disagree

Attitudes to Cyber/Internet security:

6. Please indicate the extent of your agreement with each of the following statements:

	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
a. You are concerned that your personal information is not kept secure by websites	□	□	□	□	□
b. You are concerned that your online personal information is not kept secure by public authorities	□	□	□	□	□
c. You avoid disclosing personal information online	□	□	□	□	□
d. You can protect yourself sufficiently against cybercrime, e.g., by taking precautions or by using antivirus software	□	□	□	□	□

Concerns about Online/Internet transactions:

7. What concerns do you have, if any, about using the internet for things like online banking or buying things online or social media or checking and sending email etc.?
   a. You prefer conducting transactions in person e.g., so you can inspect the product yourself or ask a real person about them
   b. You are concerned about the security of online payments
   c. You are concerned about someone misusing your personal data

d. You are concerned about not receiving the goods or services that you buy online
e. Other (specify) …
f. None/no concern

Impact of Concern on Behavior – Avoidance and Defensive:

8. On a scale from "not at all" to "extremely", to what extent has concern about internet security prevented you from doing things you would like to do on the internet?
   a. Not at all
   b. A little
   c. Moderately
   d. Very much
   e. Extremely
9. [If b - e in 8] State any activities that your concern about internet security has prevented you from doing in the past 12 months?
   …
10. On a scale from "not at all" to "extremely", to what extent has concern about internet security caused you to take specific action(s) to minimize your risk of cybercrime on the internet?
    a. Not at all
    b. A little
    c. Moderately
    d. Very much
    e. Extremely
11. [If b – e in 10] Please indicate whether your concern about internet security has caused you to take any of the following actions in the past 12 months?
    a. You have changed your security settings (e.g., your browser, online social media, search engine, etc.)
    b. You use different passwords for different sites
    c. You regularly change your passwords
    d. You do not open emails from people you don't know
    e. You have installed anti-virus software

f. You only use your own computer
g. You only visit websites you know and trust
h. Other (specify) …

Fear of Cybercrime:

12. How fearful have you felt about being the victim of cybercrime during the past month?
    a. Not at all
    b. A little
    c. Moderately
    d. Very much
    e. Extremely
13. Cybercrimes include many different types of criminal activity. Please indicate the extent to which you agree or disagree that you are MOST fearful of becoming a victim of the following cybercrimes:

	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
a. Cyber pornography (receiving unsolicited pornographic or obscene content on the internet)	☐	☐	☐	☐	☐
b. Bank/e-commerce fraud (online fraud where goods purchased were not delivered, counterfeit, or not as advertised)	☐	☐	☐	☐	☐
c. ID theft (somebody stealing your personal data and impersonating you e.g., shopping under your name)	☐	☐	☐	☐	☐
d. Harassment (being stalked or harassed online)	☐	☐	☐	☐	☐
e. Cyber-bullying (receiving intimidating or threatening messages from the internet)	☐	☐	☐	☐	☐
f. Malware/virus attack (discovering malicious software (virus) on your device)	☐	☐	☐	☐	☐

g. Hacking (your bank, social media or email account being hacked)

□ □ □ □ □

14. Consider a time in the past month you felt **MOST fearful** about being the victim of cybercrime. On a scale from "not at all fearful" to "extremely fearful", how fearful were you?
    a. Not at all fearful
    b. Slightly fearful
    c. Somewhat fearful
    d. Very much fearful
    e. Extremely fearful

Impact of Fear on Behavior – Avoidance and Defensive

15. On a scale from "not at all" to "extremely", to what extent has the fear of cybercrime prevented you from doing things you would like to do on the internet?
    a. Not at all
    b. A little
    c. Moderately
    d. Very much
    e. Extremely
16. [If b – e in 15] State any activities that the fear of cybercrime has prevented you from doing in the past 12 months? …
17. On a scale from "not at all" to "extremely", to what extent has the fear of cybercrime caused you to take specific action(s) to minimize your risk of cybercrime on the internet?
    a. Not at all
    b. A little
    c. Moderately
    d. Very much
    e. Extremely
18. [If b – e in 17] Please indicate whether fear of cybercrime has caused you to take any of the following actions in the past 12 months?

a. You have changed your security settings (e.g., your browser, online social media, search engine, etc.)
b. You use different passwords for different sites
c. You regularly change your passwords
d. You do not open emails from people you don't know
e. You have installed anti-virus software
f. You only use your own computer
g. You only visit websites you know and trust
h. Other

Victimization, Reporting and Impact on Behavior:

19. How likely are you to report a cybercrime incident to the police?
    a. Very likely
    b. Likely
    c. Somewhat likely
    d. Unlikely
    e. Very unlikely
20. [If c - d in 19], what would be your main reason for not wanting to report a cybercrime incident to the police (multiple responses allowed)?
    a. Would not want to get involved with the police or the courts
    b. Do not believe the police would be able to do anything about the incident
    c. Belief that the police would not be willing to help
    d. Incident was dealt with in another way
    e. Did not want anyone to find out about the incident
    f. Fear of publicity or media coverage
    g. Reported incident to a bank/credit card company instead
    h. Other (please specify) …
21. In the past 12 months, have you experienced some form of cybercrime? **(if no or not sure, skip to Question 29**)
    a. Yes
    b. No

c. Not sure

22. Have you reported your cybercrime experience to the police?
    a. Yes
    b. Sometimes (I reported some experiences not all)
    c. Not at all

23. Which cybercrime type did you experience? (Select all that apply)
    a. Cyber pornography (receiving unsolicited pornographic or obscene content on the internet
    b. Bank/e-commerce fraud (online fraud where goods purchased were not delivered, counterfeit, or not as advertised)
    c. ID theft (somebody stealing your personal data and impersonating you e.g., shopping under your name)
    d. Harassment (being stalked or harassed online)
    e. Cyber-bullying (receiving intimidating or threatening messages from the internet)
    f. Malware/virus attack (discovering malicious software (virus) on your device)
    g. Hacking (your bank, social media or email account being hacked)
    h. Other

24. On which device did you experience the cybercrime? (Select all that apply)
    a. Cell phone
    b. Tablet
    c. Laptop computer
    d. Desktop computer
    e. Other (specify) …
    f. Don't know

25. On a scale from "not at all" to "extremely", to what extent has your experience of cybercrime prevented you from doing things you would like to do on the internet?
    a. Not at all
    b. Slightly
    c. Somewhat
    d. Very much

e. Extremely

26. [If b – e in 25] State any activities that your cybercrime experience has prevented you from doing in the past 12 months? …

27. On a scale from "not at all" to "extremely", to what extent has your experience of cybercrime caused you to take specific action(s) to minimize your risk of cybercrime on the internet?
    a. Not at all
    b. A little
    c. Moderately
    d. Very much
    e. Extremely
28. [If b – e in 27] Please indicate whether your cybercrime experience has caused you to take any of the following actions in the past 12 months?
    a. You have changed your security settings (e.g., your browser, online social media, search engine, etc.)
    b. You use different passwords for different sites
    c. You regularly change your passwords
    d. You do not open emails from people you don't know
    e. You have installed anti-virus software
    f. You only use your own computer
    g. You only visit websites you know and trust
    h. Other (specify) …

Place of internet use/access:

29. From where do you mostly access internet from?
    a. Home
    b. Work
    c. School
    d. Public computer (e.g., library, cyber café etc.)
    e. Other (please specify)

30. On which device(s) do you access the internet? [Please select all that apply]
    a. Cell phone
    b. Tablet
    c. Laptop computer
    d. Desktop computer
    e. Other (specify) …

Frequency of internet use and impact on Behavior:

31. How frequently do you use the internet or other computer-mediated communication?
    a. Once daily
    b. Several times in a day
    c. Weekly
    d. Monthly
32. On a scale from "not at all" to "extremely", to what extent has the frequency of your internet use caused you to take specific action(s) to minimize your risk of victimization on the internet?
    a. Not at all
    b. A little
    c. Moderately
    d. Very much
    e. Extremely
33. On a scale from "not at all" to "extremely", to what extent has the frequency of your internet use prevented you from doing things you would like to do on the internet?
    a. Not at all
    b. A little
    c. Moderately
    d. Very much
    e. Extremely
34. [If b – e in 33] State any activities that the level of frequency of your internet use has prevented you from doing in the past 12 months? …

35. On average, how much time do you spend on the internet each time you go online?
    a. Less than 30 minutes
    b. More than 30 minutes but less than 1 hour
    c. Between 1 and 2 hours
    d. Over 2 hours

Motivation for Internet use:

36. Why do you use the internet and other forms of computer-mediated communications? Please indicate …

Socio-demographic information:

37. Please indicate your gender.
    a. Male
    b. Female
    c. Other (specify) …
    d. Prefer not to say
38. Please indicate your age range.
    a. 18 – 25 years
    b. 26 – 32 years
    c. 33 – 39 years
    d. 40 – 46 years
    e. 47 – 53 years
    f. 54 and over
39. Please indicate your educational level
    a. Less than high school
    b. High school or equivalent (e.g., GED)
    c. Some University but no degree
    d. University degree
40. Please indicate your ethnicity.
    a. Aboriginal
    b. White/Caucasian

c. African
d. Asian
e. Other (specify) …

41. Please indicate your marital status.
    a. Single (never legally married)
    b. Legally married (and not separated)
    c. Separated, but still legally married
    d. Living with a common-law partner
    e. Divorced
    f. Widowed
42. What category best describes your annual total family income, from all sources before taxes?
    a. Less than $25,000
    b. $25,000 to less than $50,000
    c. $50,000 to less than $75,000
    d. $75,000 to less than $100,000
    e. $100,000 to less than $125,000
    f. $125,000 or more
43. What best describes your current employment status?
    a. Employed, working 1 to 39 hours per week
    b. Employed, working 40 or more hours per week
    c. Not employed, looking for work
    d. Not employed, not looking for work
    e. Retired
    f. Disabled, not able to work
    g. Not working

Appendix B: Variables Names and Labels for Quantitative Analysis

Variable		Name used in Analysis
Demographic variables		
Age		Q38_recoded
Gender		Q37_recoded
Education		Q39_recoded
Ethnicity		Q40_recoded
Marital status		MARRIAGE
Family income		Q42_recoded
Employment status		Q43_recoded
Predictors		
Cybercrime victimization experience		Q21
Knowledge of cybercrime risk		Q1_recoded
Incident reporting		Q19_recoded
Frequency of internet use	Fear and risk	Q31
	Avoidance and defensive behaviors	internetFreqUse_avoidance_defensive
Outcome variables		
Avoidance behavior		Avoidance
Defensive		def_binary
Fear of cybercrime victimization		Q12_recoded
Perceived risk of victimization		Q5

Appendix C: Raw Internet use Motivation data for Qualitative analysis

Why do you use the internet?

P1. Work: emails and research - communication with family / friends - entertainment (twitter, fb, Netflix) - to look up information / news / recipes

P2. banking -communicating with friends and family -watching videos for entertainment or education -checking news/weather/driving directions -reading articles

P3. Work -Socialization

P4. work and for personal use (news, social media, occasional shopping)

P5. A stupid question. Why do I use a car? Why do I wear shoes? You talk like the internet is like the phone, or post office, or Sears. It's just there. It's a tool for everyday use. I don't think about having breakfast. Why should I think about using the internet? How old are you, BTW.

P6. Free access to media (daily newspapers, TV networks) and other information sources (Wikipedia, Meteor Media, Google Maps)

P7. access information

P8. Access to information, communication with family, friends, service providers

P9. Access to information. I'll conceived question . Similar to asking "what is the internet?"

P10. Accessibility

P11. Purchases, communication, agenda

P12. In order to read my personal mail, my banking transactions, my Facebook (my knowledge only), recipes on well-known sites, games, to do my groceries a few times, the renewal of drugs from my pharmacy, local advertising.

P13. All the cool kids are doing it

P14. banking and news and info, searches porn

P15. Banking Booking Information

P16. Banking, investing, games, social media like Facebook, all kinds of research, on-line shopping, downloading music, YouTube, etc.

P17. Banking, family contact

P18. Because everyone does.. it is 2020. Why even ask this? You cannot exist in Canada and not use this stuff...

P19. Because I am a normal human living in the current year

P20. Because I am working from home and do not have a phone

P21. Because I'm housebound most of the time due to COVID-19 I use the internet for Google searches, on-line shopping, and news via CBC, CTV, CNN. Also Facebook, see what my family and friends are up to....stay connected to the outside world.

P22. Because it is the 21st century, how else am I supposed to get information and communicate with people and the world?

P23. Because it's everywhere and very useful

P24. Because it's fun and convenient. As well shopping online allows me to minimize contact with crowds while there is a pandemic on.

P25. Because of the need to use a non-roman alphabet software

P26. Because that's the main way people communicate now

P27. Both business because my business is mostly from overseas. Personal because many of my friends are overseas and family

P28. Business is forcing me to do things online such as banking and paying of bills. They have stopped sending paper invoices.

P29. Business (I work remotely), personal (emails with family), and entertainment (YouTube science and documentary videos).

P30. Buying [shopping and] banking

P31. It is generally more convenient than alternatives to the Internet.

P32. It's easier

P33. It's quick and easy to use

P34. casino-email-music-purchase etc. ..

P35. Cheap and effective

P36. check email, job search

P37. Check emails, research products, visit social media sites

P38. checking emails, banking statements, credit card statements, researching products

P39. Communicate with friends overseas, communicate with family, make purchases, plan trips

P40. Communicate with friends, colleagues, organizations. conduct business transactions and financial transactions, research topics, browse goods and services. occasionally purchase goods or services. catch up on news. watch programs on streaming that I missed on TV

P41. Communicate with friends/family, keep up to date on current events, read about my interests

P42. Communication with organizations I am a part of

P43. Communication, Work, Research, Entertainment, Education, Banking, Commerce

P44. Connecting with others. Work and volunteer related activities. Staying informed, research, some shopping.

P45. Convenience

P46. Convenience

P47. Convenience

P48. Convenience and to maintain a record of interactions

P49. Convenience, I never use social-media

P50. Convenience, Social contact, Management of volunteer activity (Board meetings because of Covid-19 restrictions) – [working from home]

P51. Convenience.

P52. Convenient

P53. Convenient

P54. Convenient and safer during the pandemic

P55. Convenient in this day and age

P56. Email, Facebook, games, search

P57. Emails, Social Networks, Information and News, Weather, Stock Quotes, Opinion Polls, Podcasts. Remote surveillance camera, Surveys, SMS, Skype long distance communications, Movie streaming downloads

P58. Covid-19, Entertainment, Correspondence, Habit, Education, many reasons.

P59. Current events, entertainment, communication, research, e-commerce

P60. Another source of information

P61. Entertainment and work

P62. Entertainment, personal hobbies, and online shopping.

P63. Documented way to communicate, source of information

P64. Ease of use

P65. Ease of use, access to most product, entertainment

P66. Ease of use, accessibility, convenience

P67. ease of use, quick communication with family and friends

P68. ease to find information and numerous sources

P69. Easier to communicate with others and I use internet based app for work

P70. Easiest form of communication

P71. Easy

P72. Easy and convenient

P73. Easy way to communicate

P74. easy, convenient, social distancing

P75. Easy, especially when travelling

P76. Easy; fast; inexpensive; also I can take my time to respond

P77. Efficiency

P78. Email, FB [Facebook], games, banking, sometimes shopping.

P79. Email, news, weather, games, store flyers

P80. email, shopping, banking, reading the news, social media, reading blogs

P81. email, social media, banking, shopping, general browsing

P82. Email, social media, shopping

P83. emails, banking, web browsing, entertainment

P84. Emails, research a product, news

P85. Emails, social media, news, banking, streaming services

P86. emails; online purchases; information [& social] media

P87. Entertainment, communication, work

P88. Entertainment, Information, Communication, Financial transactions, Work

P89. Entertainment, research, social media

P90. entertainment, banking, shopping, knowledge [acquisition]

P91. Everything. Shopping, Gaming, News. Social Media, Videos, Research, etc.

P92. Facebook, email, banking

P93. fast and easy

P94. Fast and easy and efficient

P95. For entertainment and services

P96. For everything

P97. For everything! Work, keeping in touch, entertainment, banking.

P98. For fun, work, banking, social media interaction, living modern day life.

P99. For my job and reading news.

P100. For news, shopping, gaining knowledge, personal enjoyment [entertainment]

P101. For research, work, communication, entertainment, information, learning, providing information, selling, buying

P102. For social interaction. And to keep informed

P103. for socializing

P104. For work

P105. For work and for personal use

P106. For work and personal

P107. For work purposes, to shop, to keep in touch.

P108. For work-related research; for information; to keep in touch with people; for amusement; to take on-line classes or watch concerts, shows, etc.

P109. for work, for leisure

P110. For work. Email is main communication form.

P111. For working and communicating with friends

P112. Friends and family members resident outside the area - and when the time-differential may be extreme. I hate to wake anyone up!

P113. Games

P114. Games, social media, research

P115. Gaming, social networking, email, surveys.

P116. Get information from online resources. Email. Gaming

P117. Handy for information

P118. Huge source of information. Have been using since the 90s for work. Lots of interests. Library, music , twitter, news, science etc.

P119. I advertise my business, and schedule from my phone. I use it to be in direct contact with clients. Also to stay in touch with family and friends

P120. I am physically disabled so getting out & into places is difficult so I use the internet & email for my volunteer activities & shopping

P121. I can't afford good housing, what I have is more than twenty minutes from transit, there's nowhere to go any closer than that, and there's constant road noise all around here, so I have little alternative but to stay indoors. I could rely on the telephone, instead, but that's expensive and difficult to use

P122. I don't understand the question. I don't know how I could get along today without using the Internet. If you mean "for what purposes", I'd have to say personal communications, entertainment, shopping, banking, etc.

P123. I enjoy social media

P124. I get access to answers that are related to my likes.

P.125. I guess if I don't understand the question I don't have an answer.

P126. I like browsing sites such as eBay [shopping], and regularly read comics (on an almost nightly basis)

P127. I only use email. I do not use any other form of social media

P128. I use it for many things.. It's an integral part of my life and is has been for decades

P129. I use the internet for comparison shopping, reading the news, banking, general information

P130. I use the internet for e-mail, news, shopping, banking, fact checking, learning.

P131. I use the internet for researching information, shopping, or pre-shopping and for entertainment. I use computer mediated communication for short non-intrusive communications.

P132. I use the internet for work as well as for streaming TV, and accessing social media

P133. I work from a virtual office

P134. I work from home in an Internet based environment

P135. I work from home so quite often.

P136. I'm a self-employed IT Tech; I use the internet from my phone, my home, my office about equally... If I'm awake, I'm probably online one way or another. I primarily use email and phone for communication, although I will also use texting from time to time. I will use Microsoft Teams, but won't use Facebook Messenger or other 'third-party' public use communication methods

P137. Information

P138. Information and entertainment

P139. Information and shopping

P140. Information gathering, Email

P141. Information, entertainment, social networks

P142. Information

P143. Product information and research

P144. Instant communication

P145. Internet is everywhere, it is impossible not to access the internet these days, in many cases it is the only way to connect with a service provider and avoid the frustration of telephone tag/leave a message or interminable waiting queues to connect to a person.

P146. Investment and business for stocks

P147. It is a quick and convenient method that is always available to me

P148. It is a work requirement

P149. It is easy and fast and free

P150. It is how we communicate with companies, friends, and the world. My banking is done online, I order things online, research items online etc. I will not, however, use any smart home applications as I do not think the companies view security on these items as important as they are.

P151. It is the easiest form

P152. IT professional

P153. It's fast, easy, convenient, less likely to transmit COVID, more likely to have the information I'm looking for, and has become the standard way of communicating with the rest of society.

P154. It's for entertainment. TV, movies, podcasts, music etc. I don't use it at all for work

P155. It's impossible to live life without it: use it for work; for communications with almost everyone I know, for shopping...

P156. it’s easy and quick.

P157. Its 2020, so life. Mostly for communications, news, and entertainment.

P158. It’s convenient and now is some of the only ways to connect to people because of covid-19

P159. I am doing genealogy research for a genealogy site.

P160. I do my transactions almost exclusively online and I gamble a lot.

P161. I work in computer science, necessary for my job. Communication with friends / family. Online shopping, banking management.

P162. Keep up with local and national news. Social media. Play online games ... solitaire, etc.

P163. Keeps my mind active [learning]

P164. utility, speed, diversity, knowledge

P165. Lack of cell phone coverage at my house [communication]

P166. Work

P167. Learning information, entertainment, and social interaction.

P168. Leisure and work

P169. Mainly social media

P170. Make online purchases. Read the news. Watch movies and tv shows. Talk to my friends

P171. makes life much easier, entertainment, information

P172. making purchases [shopping]. reading the news, work

P173. Social media, local and international news

P174. Music [entertainment]

P175. My entire life is connected to the internet: entertainment, work, communication, hobbies. Even my outdoor hobbies like golf, fishing, and hunting are supplemented by apps that require internet access.

P176. my job requires it. education, etc.

P177. Need to for school, work. Use for entertainment and shopping.

P178. News, communication, online shopping

P179. News, entertainment, shopping

P180. News, learning, entertainment, memes, digital communication, banking, shopping, searching for information relevant to my life, etc.

P181. News, weather, FB [Facebook],

P182. News, sports news

P183. News (newspapers), weather forecast, bank transaction

P184. Order items online, social media, shop online.

P185. Part of my job to research and be connected by email and social media

P186. payment of invoices, Online orders [shopping], Text message, Searches [for information]

P187. Pay my accounts, check my investments, and write to my friends

P188. Personal and volunteer reasons

P189. Personal communication search engines writing articles

P190. Personal enjoyment, running small businesses and some external family communications.

P191. Pk it's very practical

P192. Pleasure [Convenience]

P193. Full of things; social networks, entertainment, shopping, email, information, banking services.

P194. Faster

P195. Postal service is not a credible provider of up-to-date information. Neither is print media. Internet provides immediate information

P196. To communicate

P197. For Facebook messenger, banking, and email

P198. To do research, inform me, entertain me, and communicate with my relatives and friends

P199. Primarily for work and entertainment. Sometimes to inform me on various subjects.

P200. Everything is computerized for work. To communicate with family and friends as I can see them on my screen. For online shopping sometimes items are only available online. To receive and pay the bills because it costs a fee to have them in paper by mail so I have no choice.

P201. For work, study, leisure, communication with relatives and friends, management of children's activities, etc.

P202. For work. To access sources of information for action, to join friends

P203. To read news, to do research, to access a site of my co-ownership.

P204. To inform [for information], and shopping

P205. To inform me [for information]

P206. To entertain and inform me [for information]

P207. To keep me informed [for information]

P208. For my work (translator, from home), for information on different subjects and for my emails.

P209. Mainly for business and for information

P210. Quick updates on news, sports, etc.

P211. Read CBC and BBC news sights often. Looking up companies, products, phone numbers, etc. Check emails almost daily.

P212. Reading news and research information, both personal and work related

P213. Reading news/updates....checking out merchandise websites [online shopping]

P214. Reading, research

P215. Information search of recipes, opening hours. Payment from my bank account [banking]

P216. Research and leisure

P217. Research on different subjects, information, listening to radio, music, podcast [entertainment]

P218. Looking for information, I do freelance work to keep up with political news in particular

P219. information, news, recipes, etc ...

P220. research for work

P221. Research; entertainment

P222. Social network / banking / purchasing

P223. Social network, miscellaneous purchases, news, Netflix [entertainment]

P224. Right now, working from home

P225. Send and receive e-mail, Research.

P226. Simplicity, speed, ease of work, etc. [convenience]

P227. Social media apps, Email Business purposes

P228. Social media. Netflix, YouTube [entertainment]. email.

P229. Society pressures. Organizations make it necessary to access information or resolution of problems via the internet. It is difficult to conduct business in person or over the telephone, this lack of face to face transactions lean itself to helping the perpetrators commit cybercrime easily. The government of Canada increasing use of the internet without ongoing monitoring makes users vulnerable. I prefer to deal with a real person.

P230. Sometimes it is simpler to text or message someone for a quick answer [communication]. The internet is a great tool, but one that has completely done away with privacy. I don't believe that my information is private in any way. This doesn't foster reluctance to use it, but I accept that my privacy is an illusion. Still, I haven't been a victim of identity theft or fraud yet.

P231. Stay connected to international things like friends and news, Computer research, Teaching and getting council online

P232. Stock market trading information through Google

P234. Streaming Netflix, YouTube, emails, learning languages

P235. Streaming tv [entertainment]

P236. Study, Netflix, communicate with others, research, entertainment, recipes, social media

P237. Talk to family 4000km away [social connection], shopping due to covid-19, find deals on marketplace

P238. Television information

P239. Texts, emails, games [entertainment]

P240. That's where all the info is [information]

P241. The internet is how I do almost all of my financial transactions, it is how I interact with many of my friends and acquaintances, it is how I read the newspaper and most magazines, it is the source of a significant fraction of my book reading.

P242. The internet my primary method to communicate with co-workers, customers, friends, and family.

P243. There are no other options

P244. To access email and social media, to do research, to make online purchases, to watch videos and listen to music

P245. To answer questions and to research items of interest

P246. To communicate with friends, ebooks, online banking, Purchases from known companies and email

P247. To communicate, work related and banking

P248. To do personal business, to keep in touch with friends and family, to watch shows, to listen to music, to play games

P249. To find information and online bills

P250. To gain specific knowledge that's not covered in other media forms.

P251. To keep in contact with friends, to read the news, to send emails at work, to shop, to check Instagram/Twitter

P252. To keep in touch with family and world events. And spiritual teachings.

P253. To look up information or purchase product

P254. To obtain information, research, and communicate with others.

P255. To play games, banking, ordering and check email.

P256. To socialize, to promote my work, to research for my work, to apply for work, to amuse myself [entertainment], to shop

P257. To stay in touch, to get news, to pay bills, to shop, to find the answers to questions I have.

P258. To stay informed, to entertain, to research, to shop.

P259. To watch News that's not owned by George Soros

P260. Everything is there, data, information, information, news, families

P261. All

P262. Work, leisure, information surrounding daily life.

P263. Work and staff

P264. Working, working remotely, finding information, recipes / cooking, knowing how to do things, Shopping, Communicating with people, Remote dinners and online board games (from the covid-19), Online banking services, Google maps, weather, Training, I also have an online sports coach, Gossage, listen to music (you tube) [entertainment]

P265. TV, History, Science, Documentaries.

P266. YouTube, Netflix [entertainment], banking, email, Amazon [online shopping], research.

P267. Watching videos on Facebook and writing my own thoughts

P268. Well, I'm not going to use a carrier pigeon.

P269. What an odd question. That's like asking for why I use electricity... The internet is a utility. It's engrained in daily life--indeed, it's the infrastructure most daily chores and pleasures rely on [entertainment]

P270. What other way is there in a pandemic?

P271. WhatsApp [social media]

P272. Why do anything? It's fun and interesting [entertainment].

P273. Why do you post your surveys for responses on the internet instead of randomly accosting strangers on the street corner for input?

P274. Why not? News is up to the minute vs newspaper, sports etc. Not to mention playing games or watching videos about everything [entertainment].

P275. Work

P276. Work and communication with friends and colleagues

P277. Work and personal

P278. Work and personal use.

P279. Work and socializing - especially in the pandemic

P280. work communication, personal communication, social media, little online banking, little shopping, reading news, reading various topics, vacation planning

P281. Conveinence

P282. Convenience

P283. Convenience

P284. Work mostly

P285. work related, games using social media, transportation scheduling, downloading points for fidelity programs

P286. Work remotely. Used for collaboration

P287. Work

P288. Convenient

P289. convenience

P290. work, banking, shopping, scheduling, news, socialization

P291. Work, commerce, and socializing (email and Facebook)

P292. Work, communicating with friends, entertainment

P293. Work, email, personal communication, entertainment, research/news updates, online shopping

P294. work, entertainment, social media

P295. Work, fun, educational

P296. Work, how I keep in touch with friends

P297. Work, news, entertainment

P298. Convenience.

P299. Work, News, Wikipedia [information], YouTube, Product Reviews [business purposes]

P300. entertainment, shopping, communication with family/friends.

P301. Work, shopping, banking, investing, chatting, socializing, playing games

P302. work, social media (twitter), banking (now with COVID), some minor shopping (still mainly do in person shopping for groceries, etc.)

P303. Convenience

P304. Work, social media, shopping

P305. Work, social outreach due to COVID-19, gather information and access research, etc.

P306. Work, socializing, tracking data (e.g., running, hobby related)

P307. convenient

P308. Work. Convenience, Covid-19

P309. zoom and email and Facebook with out-of-province family and friends - keeping in touch

Appendix D: Ethics Approval Certificate

UNIVERSITY OF SASKATCHEWAN

Behavioural Research Ethics Board (Beh-REB) 29/May/2020

Certificate of Approval

Application ID: 1915

Principal Investigator: Hongming Cheng Department: Department of Sociology

Locations Where Research Activities are Conducted: Online in Canada, Canada

Student(s): Mohammed Abdulai

Funder(s):

Sponsor:

Title: The Paradox of Cybercrime Risk and Internet Use

Approved On: 29/May/2020

Expiry Date: 28/May/2021

Approval Of: Behavioural Research Ethics Application

Consent form

Questionnaire

Survey invitation email

Debrief form

Acknowledgment Of:

Review Type: Delegated Review

CERTIFICATION

The University of Saskatchewan Behavioural Research Ethics Board (Beh-REB) is constituted and operates in accordance with the current version of the Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans (TCPS 2 2014). The University of Saskatchewan Behavioural Research Ethics Board has reviewed the above-named project. The proposal was found to be acceptable on ethical grounds. The principal investigator has the responsibility for any other administrative or regulatory approvals that may pertain to this project, and for ensuring that the authorized project is carried out according to the conditions outlined in the original protocol submitted for ethics review. This Certificate of Approval is valid for the above time period provided there is no change in experimental protocol or consent process or documents.

Any significant changes to your proposed method, or your consent and recruitment procedures should be reported to the Chair for Research Ethics Board consideration in advance of its implementation.

ONGOING REVIEW REQUIREMENTS

In order to receive annual renewal, a status report must be submitted to the REB Chair for Board consideration within one month prior to the current expiry date each year the project remains open, and upon project completion. Please refer to the following website for further instructions: https://vpresearch.usask.ca/researchers/forms.php.

Digitally Approved by Stephanie Martin
Vice-Chair, Behavioural Research Ethics Board
University of Saskatchewan