Copyright © 2020 International Journal of Cyber Criminology – ISSN: 0974–2891
January – June 2020. Vol. 14(1): 157–174. DOI: 10.5281/zenodo.3749468
Publisher & Editor-in-Chief – K. Jaishankar / Open Access (Authors / Readers No Pay Journal).

Examining the Effect of Victimization Experience on Fear of Cybercrime: University Students' Experience of Credit/Debit Card Fraud

Mohammed A. Abdulai[1]
University of Saskatchewan, Canada

Abstract

Fear of crime research tends to focus disproportionately on physical or place-based crimes while cybercrimes, which have been increasing over the past two decades, are relatively excluded. Drawing on Beck's theory of a risk society, this paper examines the impact of previous victimization experiences on fear of future encounters with cybercrime. A total of 462 students at the University of Saskatchewan participated in an online survey that collected demographic information and asked if they had ever felt fearful about being the victim of credit/debit card fraud. Binary logistic regression was used to predict fear of cybercrime victimization. Prior experience of victimization was positively associated with students' fear of becoming victims of credit/debit card fraud. Socio-demographic factors and knowledge of cybercrime were not significant predictors of students' fear of becoming victims of credit/debit card fraud. This study highlights the need to reconsider risks and examine reflexivity further as it relates to how people modify their behaviors when faced with the threat of cybercriminal victimization. This study also highlights the need for fear of crime research, and victimology in general, to consider the unique differences between the different crime forms – conventional and cyber-based crimes.

Keywords: Cybercrime, Fear of crime, Risk, Victimization.

Introduction

Prior experience of victimization remains a much-studied correlate of fear of crime, eliciting two contrasting explanations. The dominant view is that a positive association exists between victimization and fear of crime, as former victims of crime express more worry and perceive more risks (Alshalan, 2006; Friedman, Bischoff, Davis, & Person, 1982; Maguire & Corbett, 1987; Mawby & Gill, 1987; Smith & Torstensson, 1997; Virtanen, 2017). The other view is that prior experience of victimization is not a straightforward predictor of fear of crime and, with regards to cybercrimes, is more variable (Yu, 2014). The significance of victimization experience depends on interaction with low social status and low confidence (Virtanen, 2017); it also depends on the type of

[1] Ph.D. Candidate and Sessional Lecturer, Department of Sociology, University of Saskatchewan, Arts 1019, 9 Campus Drive, Saskatoon, SK S7N 5A5, Canada.
Email: mohammed.abdulai@usask.ca

cybercrime, where the experience of victimization significantly predicts both fear of cyber bullying and of being infected with computer viruses but is an insignificant predictor of fear of online scam and digital piracy (Yu, 2014).

Current studies on fear of crime have several weaknesses. First, the overarching emphasis is on "'ordinary' street crime rather than corporate or white-collar crime" and, consequently, research into fear of crime has followed a similar path (Hale, 1996, p. 84). Second, researchers rely on "a global measure (so called because the question makes no reference to a specific crime)" to measure fear of crime (Hale, 1996, p. 85). However, cybercrimes, including credit/debit card fraud, have increased drastically in recent years in many countries (Adler & Adler, 2006; Internet Crime Complaint Centre, 2007, 2008, 2009, 2010, 2011, 2012, 2013, 2014, 2015, 2016, 2017, 2018; Marcum, Higgins, & Ricketts, 2010; Pratt, Holtfreter, & Reisig, 2010; Van der Meer, 2015; Van Wilsem, 2011). Such an increment means cybercrimes must receive increased academic scrutiny if they are to be correctly understood and if effective interventions are to be developed.

Using the framework of Beck's (1992) risk society theory, this paper attempts to explain the fear of credit/debit card fraud victimization among students. At the core of the risk society theory is that risk and hazards have become a permanent feature of the modern time due to the various unintended consequences of numerous techno-scientific innovations. This suggests that students' fear of credit/debit card fraud victimization might be an unintended consequence of advances in digital finance, despite claims of safer and more efficient ways of pursuing commerce. Risks and the associated fear are also likely to be a feature of future societies. Using Beck's theory, findings from an increased scholarly investigation will allow testing, refinement, expansion, or elaboration of existing theoretical models. Furthermore, technological advancements of the 21st century have increasingly made cybercrimes unintended consequences, which makes it imperative that fear of crime research begins to focus on cybercrimes as well. The empirical examination of this issue is therefore intended to contribute to filling the void in the criminological literature and mapping a trajectory for future research.

1. Background

1.1. Trends and Costs of Cybercrimes

While academics have yet to fully grasp the extent and theoretical implications of cybercriminal victimization (see Jaishankar, 2007), cybercrimes have been getting much recent attention from the government, media and security organizations. The Pew Internet and American Life Project Report, for example, showed that the vast majority of all Americans (92 % and 87 %) are concerned about online child pornography and online credit card theft respectively, with 69 % being "very concerned" about credit card theft online (Fox & Lewis, 2001, pp. 7-8). Also, the Crime Survey for England and Wales for year ending December 2018 revealed over 3.6 million incidents of fraud reported by adults aged 16 years and over, a 12 % increase from the previous year (Office for National Statistics, December 2018, p. 56). Significantly, more than half (56% and 54%) of the total fraud incidents for survey year endings September and December 2018 were both deemed to be "cyber-related", that is cybercrimes (Office for National Statistics, September 2018, p. 56; December 2018, p. 56). Additionally, the British Crime Survey of 2005/06 also revealed that more than half (57%) of respondents owning credit cards reported being 'fairly worried' or 'very worried' about being a victim of card fraud (Roberts, Indermaur,

& Spiranovic, 2013, p. 10). On the other hand, the Canadian Council of Better Business Bureaus reports that identity theft is the fastest-growing type of fraud in North America, with losses in the billions of dollars each year (Smyth, 2010). Against this backdrop, more than 12,000 cases of identity theft complaints were reported in Canada by PhoneBusters — the Canadian central agency for collecting telemarketing, fraud, and identity theft information — with losses amounting to over $9 million (Smyth, 2010, p. 45). From all indications, this is likely to continue growing as internet usage increases, and more transactions are performed online (Arango, Huynh, Fung, & Stuber, 2012).

The growth in the volume and value of online transactions over the past two decades also warrant concerns over the risks of cyber fraud. A 2016 Pew Research Center study found that roughly eight-in-ten (79%) Americans are online shoppers with 15 % making weekly online purchases, compared with 22 % of Americans who reported ever doing online shopping back in the year 2000 (Smith & Anderson, 2016). The study also revealed that 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." (2016, p. 5). Among the 28 European Union (EU) member region, almost three quarters (72%) of all persons aged 16 to 74 accessed the internet daily, with 80% of all persons in the same age range within the EU-28 accessing the internet once a week (but not every day) (Eurostat, 2017). This growth creates immense opportunities for cyber fraud, including identity theft and hacking customers' credit/debit card details from retail sales or their devices. Grau (2008) notes that concern over the security of credit card payments holds some Canadians back from buying more online.

Concern about cybercrimes is not only a personal issue but often also affects the business community and government. Businesses are forced to incur considerable costs to upgrade their Information Communication Technology (ICT) security as well as to ensure against cybercrimes. For example, global estimates show that organizations spent more than $81 billion in 2016 on information security, an increase of over 7 % from 2015 (CloudMask, 2016). These concerns have already compelled national agencies and the Canadian government to devise strategies aimed at curtailing the threat. For example, coming up with a "whole-of-government approach to cybersecurity" was identified as a strategic priority by Public Safety and Emergency Preparedness Canada in its 2009-2010 report (Ministry of Public Safety, 2009, p. 10). A practical response to the cybercrime problem in Canada was the launch of the PhoneBusters initiative by the Ontario Provincial Police to counter telemarketing fraud (Smyth, 2010, p. 55). Similar and increasingly innovative approaches are needed to counteract the potential risks posed by the growth in cyber transactions.

Apart from the direct costs of cybercrimes, particularly credit and debit card fraud, are the indirect costs (Anderson et al., 2013; Smyth, 2010). Anderson et al. (2013) argue that "indirect loss is the monetary equivalent of the losses and opportunity costs imposed on society by the fact that a particular cybercrime is carried out, successfully or not and independent of a specific instance of that cybercrime" (p. 271). These costs include the loss of trust in online banking and its resulting impact on reduced revenues from electronic transaction fees (Anderson et al., 2013; Smyth, 2010), which can have far-reaching consequences. An additional aspect of indirect costs is the expense businesses and institutions incur in their resolve to protect the cyber landscape. This cost is captured differently in other literature as defence costs and includes spam filters, antivirus software, and browser extensions, among others (Anderson et al., 2013). Though indirect, the real value of losses from indirect costs is substantive. For example, "the botnet behind a third of the spam sent in 2010 earned its owners around $2.7 million while worldwide expenditures on spam prevention probably exceeded a billion dollars" (Anderson et al., 2013, p. 266). Finally, a significant social cost of increased cybercrimes is the rising concern and fear of victimization, which is well documented in countries such as Canada, the USA, and England and Wales (Grau, 2008; Office for National Statistics, December 2018; Fox & Lewis, 2001). The internet has opened new avenues for criminal behaviours, which has created opportunities to explore how fears are experienced among (potential) cybercrime victims. Consequently, this study aims to contribute to the scholarship on cybercrime through an empirical analysis of how university students experience cybercrime fear/victimization, and the determinants of such fears. Like Kohm, Waid-Lindberg, Weinrath, Shelly, and Dobbs (2012), the present study has the unique strength of using offence-specific questions to measure fear of cybercrime.

1.2. Prior Experiences and Fear of Cybercrimes

The rational expectation of a direct relationship between victimization and fear of crime have resulted in varying outcomes (Hale, 1996; Kohm, Waid-Lindberg, Weinrath, Shelley, & Dobbs, 2012). In their Australian study, Mawby and Gill (1987) found that fear was the most typical emotional response experienced by victims of crime. This is in line with the concept of the real-world thesis – the view that a direct first-hand experience of crime affects fear (Weinrath, Clarke, & Forde, 2007). Significant, though, is if the experience of victimization influence fear of cybercriminal victimization, on which researchers disagree. On the one hand, prior experiences are believed to enhance fear of crime (Callanan & Rosenberger, 2015, p. 324; Virtanen, 2017), a view that supports the rational expectation of a direct relationship. However, Rosini (in Carcach, Frampton, Thomas, & Cranich, 1995), for example, argues that past victimization tends to motivate people into taking precautionary measures (and lessens their fear of crime) rather than increase fear of crime. This argument is, however, contentious. Importantly, the idea of taking precautions could as well suggest harbouring fear. This perspective is relevant because the relationship between the two (adopting precautionary measures and fear reduction) is not linear or causal. Preventive actions in this regard can be interpreted as a risk-mitigating step.

On the other hand, others argue that fear is unrelated to patterns of victimization or actual victimization. Instead, fear of crime is the result of "perceived vulnerability based on subjective judgments of personal risk" (Whitrod & Maxfield, in Carcach et al., 1995, p. 273). This perspective resonates with the perception of disorder argument, i.e., when people perceive disorder, they tend to modify their behaviours accordingly. Disorder, as observed here, could be associated with violence, insecurity, or any number of adverse outcomes. As a result, when disorder is perceived, be it real or imaginary, fear becomes one of the immediate behavioral responses.

Consequently, a disturbance in the neighborhood (i.e., environment) is an essential precursor to environmental or conventional crimes. The perception of disorder or disorderly neighborhood argument is potentially applicable to cybercrimes as there is a cyber equivalent of disruptive social environments. Easy examples are the intrusive trolling, proliferation of pop-ups without apparent reason, and spamming (particularly for unsavory sites) in cyberspace (internet platform). This evidence of intrusion substantially raises doubts and fears about, for example, the safety of financial information. Thus, disorderly digital neighborhoods could also be a precursor to cybercrimes.

In a further twist to the argument, some scholars have found mixed outcomes of victimization experience on fear within the same study. In their comparative study of fear of crime among American and Canadian students, Kohm et al. (2012) found a differential impact of previous victimization experience on fear in the general sample and the sub-sample. In the general sample, the traditional predictors of fear, including previous victimization experience, were found to be significantly related to students' fear, with previous victimization related to lower levels of fear (2012, p.83). In the sub-sample, however, previous victimization experience was found not to be a significant predictor of fear for Canadian students while it was associated with lower levels of fear for their American counterparts (p.84). While the findings could have been influenced by some factors, including possible unique context effects, it remains useful within the broader fear of crime debate, as well as in the specific case of victimization experience.

2. Theoretical Foundation

The risk society theory (Beck, 1992) is a critical late modernist theory that espouses a critique of scientific knowledge and advancement. A principal argument in this theory is the centrality of ideas of risk, given the various scientific developments in the world. Beck asserts 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). Consequently, for Beck, the dangers of techno-industrial developments are not limited in time and space, and none can be held accountable for such hazards. Cybercrimes, perpetrated with computers as a tool or object, defy boundary and time limitations and can be committed simultaneously across multiple locations. Considering these risks, however, Beck is optimistic. He argues that the effects of the hazards can be managed through radicalized rationality, which holds reflexivity as an essential element in the evolution of societies. Radicalised rationality describes a situation in which 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 implies a radical shift in the overall social and technological context in which individuals, as active agents, have been positioned in late modernity. The risk society is a distinct social formation operating on radically different axial principles; the axial tenets of risk society are the distribution of "bads or dangers" and the society is structured through individualism (Beck, 1992, p. 3).

Notably, people experience crime, either directly or indirectly, through the experiences of friends, family, or significant others. Even though a victimization experience may result in a person becoming more cautious (Carcach et al., 1995), it is yet unclear whether such caution makes a person more fearful (Hale, 1996). Curiously, studies support all three possible outcomes between victimization and fear; a robust direct relationship, a weak link, and a non-existent relationship have all been observed (Box, Hale, & Andrews, 1988; Braungart, Braungart, & Hoyer, 1980; Ferraro, 1995; Kohm et al., 2012; Liska et al., & Wanne & Caputo in Hale, 1996, p. 104; Virtanen, 2017; Weinrath & Gartrell, 1996). The argument that the experience of crime makes people more cautious and hence less fearful of crime appears challenging to support; the same case could as well suggest such a person is harbouring fear, resulting in cautious steps.

In the realm of traditional crime, studies have also investigated the association of indirect victimization with fear, and has revealed mixed findings (Arnold, 1991; Box et al., 1988; Callanan et al., 2015; Kohm et al., 2012; Weinrath et al., 2007). In one breath, it was found that indirect victimization through salience of specific media consumption predicted fear, while overall media consumption did not (Kohm et al., 2012, pp. 82-83). On the other hand, Arnold (1991) found indirect victimization to significantly predict fear in his comparative study of data on fear from three surveys (p.118). Such mixed findings regarding the effect of indirect victimization on fear reveal a dynamic layer to the argument – a dynamic centred on how such an outcome is accomplished. On their part, Callanan et al. (2015) explored further the effect of indirect victimization on fear. They argued that such an effect is mediated by other factors, notably the media and, specifically, television. The conclusion to be drawn here is that the indirect victimization and fear relationship, like the direct victimization and fear relationship, is inconsistent.

Consequently, some explanations have been given to account for such contradictory findings. In these explanatory attempts, however, Hale (1996) argues that the use of global measures, rather than crime-specific measures, is a likely reason for such findings. Suffice to say at this point that the theme of indirect victimization on fear of cybercrime will be explored in a future study.

The question then becomes how to explore these issues in the context of credit/debit card fraud victimization, as their application is notwithstanding the mixed findings of the relationship between the prior experience of cybercrime victimization and fear of cybercrime victimization (Alshalan, 2006). It is reasonable for one to expect that a person who has had experience of cybercrime victimization, either a direct first-hand experience or vicariously through a friend or significant other, may be much more fearful of subsequent victimization. Reasoning this way offers greater possibilities given that cybercrime, and specifically credit/debit card fraud, is unaffected by physical proximity and the perpetrators enjoy an almost perfect anonymity. The resultant uncertainty about when and how a person may become victimized could likely make individuals with victimization experience (direct or indirect) much more fearful of the risk of subsequent victimization. So, rather than the experience of victimization motivating people to become more cautious as Carcach et al. (1995) argue, the experience could make such people more uncertain and hence fearful of subsequent victimizations.

Following from Hale's (1996) view that the inconsistencies in the victimization and fear relationship are caused by using global rather than crime-specific measures, this paper focuses on cybercrimes, and specifically credit/debit card fraud, and intends to make a scholarly contribution toward clarifying the debate. Specifically, this paper seeks to determine i) how students' perception/knowledge of cybercrime impacts how fearful they are of becoming victims of credit/debit card fraud, ii) if/how students fear of victimization is affected by socio-demographic factors, and iii) how experience of credit/debit card fraud victimization affects fear of future credit/debit card fraud victimization.

3. Methods

Data were collected by an online survey. The study, which was designed in collaboration with the Social Science Research Laboratories (SSRL) at the University of Saskatchewan, was anonymously administered online using Qualtrics® software. The study was advertised on various campus media, including the university's intranet (PAWS), which is available to all students, as well as posters and word of mouth. Student participation in the survey was voluntary without any reward. Sampling was based on convenience. The exploratory nature of the study made a student population suitable as a source of data. Also, digital literacy has become an essential part of student life (Prensky, 2001); as such, students represent potential victims of cybercrime.

From a total student population of 20,998 (University of Saskatchewan, 2015), a total of 462 students participated in the study, with 405 completing the entire survey. Data analysis was done using the Statistical Package for Social Sciences (SPSS) version 19. Missing data were treated as missing completely at random and were not excluded.

The study has a single dependent variable - fear of credit/debit card fraud victimization. Respondents indicated yes (y=1) or no (y=0) when asked if, during the past month, they had ever felt fearful about being the victim of credit/debit card fraud. Independent indicators were socio-demographic factors; knowledge/perception of cybercrime (cybercrime is only cyber-enabled, y=1; cybercrime is only cyber-dependent, y=2; cybercrime is both cyber-enabled and cyber-dependent, y=3); and experience of victimization (victimization experience, y=1; no victimization experience, y=2). Knowledge is operationalised based on the two broad conceptualisations of cybercrime as either cyber-enabled or cyber-dependent (Holt & Bossler, 2014; McGuire & Dowling, 2013). Cyber-dependent crimes are offences targeted at information technology (IT) and committed using only tools of ICT (e.g., hacking and viruses), whilst cyber-enabled crimes are not targeted at IT but committed using ICT (e.g., cyberbullying and cyber fraud). Some variables (age, annual family income, marital status, place of residence, level of studies, and study mode) were recoded to reduce the number of categories (see Appendix A), allow for comparability with other studies, and allow for meaningful analysis in some other cases (see also Alshalan, 2006; Anderson, 2006; Braungart et al., 1980; Parker, 1988; Yu, 2014).

Table 1 displays the basic descriptive statistics (sample frequencies) of the variables used in the analysis. Table 1 indicates that the base rate of fear of cybercrime among students is about 36 %, that is, more than three-in-ten students reported being afraid of cybercrime. Table 1 also indicates that more than eight-in-ten students (83.7%) believed that cybercrime includes both cyber-enabled and cyber-dependent crimes. Table 1 further reveals that only ten % of students reported having victimization experience with almost nine-in-ten (89.8 %) students having had no experience of victimization. The rest of Table 1 indicates sample frequencies for the demographic variables.

Table 2, on the other hand, displays the results of combined binary logistic regression analysis of the variables used in the study. The value of the odds ratios (Exp(B)) ranged between 0 and ∞, where values of 1 indicate no difference and values > or <1 indicate a difference between the groups compared with respect to the dependent variable.

Table 1. Sample frequencies for demographic and key variables (N = 462)

Variable	Frequency	%	Valid %
Fear of crime (n=413)			
Yes	147	31.8	35.6
No	266	57.6	64.4
Knowledge (n = 418)			
Cyber-enabled	49	10.6	11.7
Cyber-dependent	19	4.1	4.5
Both	350	75.8	83.7
Victimization experience (n = 412)			
Yes	42	9.1	10.2
No	370	80.1	89.8
Demographics			
Gender (n = 399)			
Male	152	32.9	10.2
Female	247	53.5	89.8
Age (n = 405)			
23 or less	281	60.8	69.4
24 – 30	90	19.5	22.2
31 or more	34	7.4	8.4
Level of studies (n = 405)			
Undergraduate	329	71.2	81.2
Graduate	71	15.4	17.5
Other	5	1.1	1.2
Study Mode (n = 395)			
Full-time	377	81.6	95.4
Part-time	18	3.9	4.6
Residency (n = 404)			
Domestic	340	73.6	84.2
International	64	13.9	15.8
Ethnicity (n = 403)			
Aboriginal	14	3	3.5
White/Caucasian	259	56.1	64.3
Asian	56	12.1	13.9
Other	24	5.2	6.0
Marriage (n = 402)			
Single	345	74.7	85.8
Married	57	12.3	14.2
Annual family income (n = 297)			
49,000 or less	176	38.1	59..3
50,000 to 99,000	72	15.6	24.2
100,000 or more	49	10.6	16.5
Place of Residence (n = 403)			
Campus	99	214	24.6
Employment (n = 404)			
Part-time	192	41.6	47.5
Full-time	33	7.1	8.2
Not working	179	38.7	44.3

Table 2. Odds ratios from a logistic regression model predicting fear of credit/debit card fraud victimization (N = 462)

				95% Confidence Interval for Exp(B)	
Predictor Variables	Exp(B)	Std. Error	Sig.	Lower Bound	Upper Bound
Intercept		2.960	.531		
Knowledge of Cybercrime					
Cyber-enabled	1.405	.387	.384	.616	2.808
Cyber-dependent	.593	.739	.476	.132	2.390
Cyber-enabled and Cyber-dependent	.	.	.	.	.
Victimization Experience:					
Yes	3.246	.431	.006*	1.396	7.550
No	.	.	.	.	.
Gender:					
Male	.991	.290	.976	.561	1.751
Female	.	.	.	.	.
Age:					
Age ≤ 23	.753	.607	.640	.229	2.476
24 ≤ Age ≤ 30	.995	.536	.993	.348	2.847
Age ≥ 31	.	.	.	.	.
Level of Studies:					
Undergraduate	.412	1.521	.560	.021	8.120
Graduate	.467	1.578	.629	.021	10.284
Other	.	.	.	.	.
Study Mode:					
Full-time study	.765	.707	.705	.191	3.058
Part-time study	.	.	.	.	.
Domestic Student	.529	.532	.232	.186	1.502
International Student	.	.	.	.	.
Ethnicity:					
Aboriginal	1.558	.746	.553	.361	6.727
White/Caucasian	.518	.523	.208	.186	1.4449
African	.938	.452	.886	.873	2.272
Asian	1.337	.524	.579	.479	3.738
Other (specify)	.	.	.	.	.
Marriage:					
Single	.749	1.589	.856	.033	16.873
Married	.	.	.	.	.
Family Income ≤ 49,000	1.216	.417	.639	.537	2.751
49,000 < Income <100,000	1.704	.448	.234	.709	4.098
Family Income ≥ 100,000	.	.	.	.	.
University Residence	1.127	.362	.742	.554	2.289
Off-campus Residence	.	.	.	.	.
Employment:					
Working Part-time	1.569	.290	.120	.890	2.768
Working Full-time	1.411	.542	.525	.488	4.084
Not Working	.	.	.	.	.

* p < .05

4. Findings

The results in Table 2 indicate knowledge of cybercrime is not significantly associated with fear of credit/debit card fraud victimization, irrespective of the level of the variable. When cyber-enabled is compared with the reference category (both cyber-enabled and cyber-dependent), the p-value is .384, which corresponds to an odds ratio of 1.405. When cyber-dependent is compared with the reference group, a p-value of .476 that corresponds to an odds ratio of .593 is observed. While the odds ratios suggest more fear when a student believes cybercrime is only cyber-enabled and less fear when the student believes cybercrime is only cyber-dependent, the insignificant p-values indicate no significant relationship between knowledge of cybercrime and fear of credit/debit card fraud victimization.

The socio-demographic variables related to gender, age, marital status, ethnicity, and family income all have p-values >.05 and hence are not significant with respect to student fear of credit/debit card fraud victimization.

The predictor variable victimization experience is significant ($p<0.01$), corresponding to an odds ratio of 3.246. The odds ratio implies that the probability of fear occurring with a unit increase in victimization experience is higher than at the original level of victimization experience. This means that students with victimization experience are more fearful of credit/debit card fraud victimization than students with no experience of victimization. In other words, the chances of a student being fearful of credit/debit card fraud victimization increases with experience of victimization. Thus, controlling for other variables in the model, prior experience of victimization is significantly related to fear of future credit/debit card fraud victimization.

5. Discussion

The findings reveal that student perception/knowledge of cybercrime and socio-demographic factors do not affect fear of future credit/debit card fraud victimization. In other words, females, older students, single, non-whites, and those with higher income have no more fear of credit/debit card fraud compared to males, younger, non-single, white students, and those with less income. However, students with an experience of cybercrime victimization report heightened fear compared to those without victimization experience.

The literature on the predictive significance of victimization experience remains contentious. Even though some authors have established that victimization experience can predict fear of cybercrime (Alshalan, 2006), others argue that the predictive influence of victimization experience is not straightforward. Instead, they argue that it depends on the type of cybercrime (Yu, 2014). The latter position is in line with the present study because a view that underpins the current research is that lumping predictors of fear of crime into overarching or broad categories is not helpful. Instead, this study holds the view that there are different predictors for various crimes, including different forms of place-based and cybercrimes. To this extent, it is notable that this study found that victimization experience is a significant predictor of fear of credit/debit card fraud. By doing so, the present study is making a case for specificity of predictors of fear for specific crimes, a position different from the generalized predictors' approach.

The current finding challenges the position that fear is unrelated to patterns of victimization or actual victimization, and that it is instead the result of "perceived vulnerability based on subjective judgments of personal risk" (Whitrod & Maxfield in

Carcach et al., 1995, p. 273). This position brings into focus the argument about the perception of disorders, which give rise to feelings of vulnerability and, hence, fear. On the contrary, however, the current findings demonstrate that patterns of victimization or actual victimization does matter, with prior experience of victimization affecting students' fear of future cybercrime victimization. The perception of disorders argument is a difficult one to support, given that risk in the contemporary techno-scientific era is a realistic proposition. This is because the cyber environment is riddled with the prevalence of various kinds of computer viruses and phishing scams, which makes the space inherently risky. In Beck's (1992) risk society, risk is 'system' immanent and inescapable; this means risk is everywhere in the system. The source of uncertainty, and hence fear, results from the constant state of flux that characterizes cyberspace. The lack of physicality to this space also makes it a challenge for people to feel secure, even after they or their financial institution employ safeguards. A further possible explanation for the fear could be that students sometimes only realize they have been victimized by credit/debit card fraud several weeks after the fact, likely after receiving or checking their bank statements. Recognizing one's victimization in this way tends to leave the victim in fear.

This study has several limitations. Notably, the study used a non-probability (convenience) sample, which means generalizations ought to be made with caution. Also related to sampling is the absence of response rate reporting. This is difficult because the survey was not sent to a panel of respondents. Finally, the study is based on a student population, which makes inferences to the general population a challenge.

5.1 Theoretical Implications

The findings have significant implications for criminological theory and victimology, given that risk currently manifests in several ways. Technological advancements of the 21st century have shaped the occurrence of risk by introducing dynamism both to its appearance as well as individuals' experience thereof. Technological advancements have rendered risk a flux phenomenon. Fear and the potential for credit/debit card fraud victimization is a risk situation that arises from activity in the spatio-temporal environment created by techno-scientific advancements. Given that the spatio-temporal environment is not physical, however, suggests a transformation of risk — from the normal physical realm to the non-conventional cyber realm. Therefore, in line with the construction of risk as dynamic, the need to move away from classical theoretical orientations to more contemporary-based conceptualizations becomes imperative. Such a shift might also mean finding an appropriate medium for integrated theoretical frameworks. To this extent, Beck's theory of risk society comes in handy and serves as an excellent starting point to understand contemporary-based risk phenomena.

This paper has established that Beck's risk society theory is a useful framework for explaining and predicting fear of credit/debit card fraud victimization. Risk society espouses that risk affects everyone regardless of socio-demographic background. The unavoidability of risk explains why these factors had no significant impact on fear of credit/debit card fraud victimization. Additionally, the fact that cybercrime (credit/debit card fraud) takes place in cyberspace, devoid of the physical meeting of victim and offender, means this type of crime is 'blind' to physical space. This is contrary to risk generally being conceived as the outcome of instrumental rationality and as mainly occurring in the physical world (Fox, 1999). Not being place-bound also implies the commission of such crime is without recourse to the physical and other value or lifestyle identifications of people, which again aligns with the predictive insignificance of socio-demographic variables in the binary logistic regression model.

Moreover, individualism also explains the non-significance of socio-demographic variables as predictors of the fear of credit/debit card fraud victimization. Individualism is used here in the sense of people being unique actors in their actions despite their membership or identification with groups and cohorts. Individualism is an essential component of the risk society and a significant factor in Beck's view of reflexive modernization. Given the salience of individualism in late modernity, broad categorization of agents and consequent generalizations in respect of these agents are inconsistent. People choose to go online based on their particular needs at any point in time.

The present work also adds a wrinkle to socio-criminological theory as it seeks to challenge the strict dichotomy or duality of structure and agency that has dominated sociological, and by extension, criminological theorizing. Cyber criminality is a typical activity that results from a combination of structural as well as agency influences. Structurally, cyberspace exists as large open spans. Human activity, constituting agency, accounts for developments in cyberspace that make communication and other interactions possible using the internet. Owning and operating credit/debit cards is an aspect of human agency, especially when we consider behavioural responses in utilizing these card details for various transactions. Stealing and using credit/debit card details of account holders also constitute an interplay between structure and agency. However, actor expression of fear of credit/debit card fraud victimization falls neither within a strict structure or agency realm. Instead, the expression of fear of victimization is a product of the interplay of structure and agency. This implies that theory construction ought to be seen in a similar light.

Fear of cybercrimes, such as credit/debit card fraud victimization, is an exciting area of focus for researchers because it allows one to conclude the nature of risks using empirical analyses of a technologically driven phenomenon. By studying prior experience of victimization as a determinant of fear of credit/debit card fraud victimization, one can understand how risk is experienced/manifested in today's technologically driven society. As noted earlier, even though knowledge of cybercrimes and socio-demographic backgrounds were found to be insignificant predictors of fear of credit/card fraud, they offer critical information on how to understand risk. Research on conventional (physical place-based) crimes reveals that knowledge is a significant determinant but, in the context of credit/card fear, is non-significant. Such findings mean that risk and fear are different in physical and non-physical settings.

Finally, the inescapability of risk in the contemporary technology-driven era implies that the study of fear of crime, and victimology in general, must consider the unique differences between the different crime forms, i.e., conventional and cyber-based crimes. Doing so would reveal predictors of fear of criminal victimizations that are different depending on the type and context of crime. Underscoring this notion is the predictive insignificance of socio-demographic variables found in the present study, which is contrary to their overwhelming significance in predicting the fear of 'conventional' crimes. Such consideration, therefore, ensures that theory is responsive, progressive, and relevant. Herein, it was rendered apparent that credit/debit card fraud victimization is not amenable to strict classical sociological or criminological theories. This study also argues that prior victimization experiences reveal that risks and fears are not becoming obsolete but are merely changing forms. At the same time, this study finds continuity with past sources/forms of risks and fear. Prior victimization experience is a significant predictor of fear of both cybercrimes and conventional physical place-based crimes. Thus, rather than reject conceptualizations of fear and risk, one must see risk as fluid, changing as context changes (physical to the non-physical world).

Conclusion

This work was an exploratory study that examined how knowledge of cybercrime, socio-demographic variables, and experience of victimization affect fear of credit/debit card fraud victimization. Generally, and substantively, the study found that students with prior experience of victimization tend to express considerably more fear of becoming victims of credit/debit card fraud. However, knowledge of cybercrime and socio-economic factors had no significant influence, which suggests that risk and fear are different in physical and non-physical settings. Overall, the results indicate that credit/debit card fraud victimization is not amenable to strict classical sociological or criminological theories and that risks and fears are not becoming obsolete but are merely changing forms.

Acknowledgements

This study is the outcome of funding support from the Centre for Forensic Behavioural Science and Justice Studies at the University of Saskatchewan. Data collection was facilitated by the Social Science Research Laboratories (SSRL) at the University of Saskatchewan. Also, I thank Dr. Hongming Cheng (my supervisor) and Drs. Carolyn Brooks, Mark Olver, and John Hansen (members of my advisory committee) as well as Dr. Oral Robinson and Dr. Laura Wright, for the useful comments and suggestions. Finally, I am grateful to the study participants for their role in this research.

References

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

Alshalan, A. (2006). *Cyber-crime fear and victimization: an analysis of a national survey* (Ph.D.). Available from ProQuest Dissertations & Theses Global. (305312893).

Anderson, R., Barton, C., Böhme, R., Clayton, R., Van Eeten, M. J., Levi, Moore, T., & Savage, S. (2013). Measuring the cost of cybercrime. In: *The Economics of Information Security and Privacy* (pp. 265-300). Springer Berlin Heidelberg.

Anderson, K. B. (2006). Who are the victims of identity theft? the effect of demographics. *Journal of Public Policy & Marketing, 25*(2), 160-171. doi: 10.1509/jppm.25.2.160

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.

Arnold, H. (1991). Fear of crime and its relationship to directly and indirectly experienced victimization: a binational comparison of models. In K. Sessar & H. Kerner (Eds.), *Developments in crime and crime control research: German studies on victims, offenders, and the public* (pp. 87-125). New York: Springer-Verlag.

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

Box, S., Hale, C., & Andrews, G. (1988). Explaining fear of crime. (Includes bibliography) (Great Britain). *British Journal of Criminology, 28*(3), 340-356. doi: 10.1177/0022427884021003004

Braungart, M. M., Braungart, R. G., & Hoyer, W. J. (1980). Age, sex, and social factors in fear of crime. *Sociological Focus, 13*(1), 55-66. doi: 10.1080/00380237.1980.10570360

Callanan, V., & Rosenberger, J. S. (2015). Media, gender, and fear of crime. *Criminal Justice Review, 40*(3), 322-339. doi: 10.1177/0734016815573308

Carcach, C., Frampton, P., Thomas, K., & Cranich, M. (1995). Explaining fear of crime in Queensland. *Journal of Quantitative Criminology, 11*(3), 271-287. doi: 10.1007/bf02221140

CloudMask. (2016). The *Cost of Data Security: Are cybersecurity investments worth it?* Ottawa: CloudmaskInc. Retrieved from: https://cloudmask.com/data_protection_under_breach/the-cost-of-data-security-are-cybersecurity-investments-worth-it/

Eurostat. (2017). Digital Economy and Society Statistics - households and individuals. Retrieved from https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Digital_economy_and_society_statistics_-_households_and_individuals#Internet_access.

Ferraro, K. F. (1995). *Fear of crime: Interpreting victimization risk*. Albany: State University of New York Press.

Fox, N. (1999). Postmodern reflections on 'risk', 'hazards' and life choices. In D. Lupton (Ed.), *Risk and sociocultural theory: New directions and perspectives* (pp. 12-33). Cambridge: Cambridge University Press.

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

Friedman, K., Bischoff, H., Davis, R., & Person, A. (1982). *Victims and helpers: Reactions to crime*. New York: US Department of Justice, National Institute of Justice.

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

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

Holt, T. J., & Bossler, A. M. (2014). An assessment of the current state of cybercrime scholarship. *Deviant Behavior*, *35*(1), 20-40. doi: 10.1080/01639625.2013.822209

Internet Crime Complaint Center. (2007). 2006 *Internet Crime Report*. Washington, DC: The National White Collar Crime Center and The Federal Bureau of Investigation. Retrieved from https://pdf.ic3.gov/2006_IC3Report.pdf.

Internet Crime Complaint Center. (2008). 2007 *Internet Crime Report*. Washington, DC: The National White Collar Crime Center and The Federal Bureau of Investigation. Retrieved from https://pdf.ic3.gov/2007_IC3Report.pdf.

Internet Crime Complaint Center. (2009). 2008 *Internet Crime Report*. Washington, DC: The National White Collar Crime Center and The Federal Bureau of Investigation. Retrieved from https://pdf.ic3.gov/2008_IC3Report.pdf.

Internet Crime Complaint Center. (2010). 2009 *Internet Crime Report*. Washington, DC: The National White Collar Crime Center and The Federal Bureau of Investigation. Retrieved from https://pdf.ic3.gov/2009_IC3Report.pdf.

Internet Crime Complaint Center. (2011). 2010 *Internet Crime Report*. Washington, DC: The National White Collar Crime Center and The Federal Bureau of Investigation. Retrieved from https://pdf.ic3.gov/2010_IC3Report.pdf

Internet Crime Complaint Center. (2012). 2011 *Internet Crime Report*. Washington, DC: The National White Collar Crime Center and The Federal Bureau of Investigation. Retrieved from https://pdf.ic3.gov/2011_IC3Report.pdf.

Internet Crime Complaint Center. (2013). 2012 *Internet Crime Report*. Washington, DC: The National White Collar Crime Center and The Federal Bureau of Investigation. Retrieved from https://pdf.ic3.gov/2012_IC3Report.pdf.

Internet Crime Complaint Center. (2014). 2013 *Internet Crime Report*. Washington, DC: The National White Collar Crime Center and The Federal Bureau of Investigation. Retrieved from https://pdf.ic3.gov/2013_IC3Report.pdf.

Internet Crime Complaint Center. (2015). 2014 *Internet Crime Report*. Washington, DC: The National White Collar Crime Center and The Federal Bureau of Investigation. Retrieved from https://pdf.ic3.gov/2014_IC3Report.pdf.

Internet Crime Complaint Center. (2016). 2015 *Internet Crime Report*. Washington, DC: The National White Collar Crime Center and The Federal Bureau of Investigation. Retrieved from https://pdf.ic3.gov/2015_IC3Report.pdf.

Internet Crime Complaint Center. (2017). 2016 *Internet Crime Report*. Washington, DC: The National White Collar Crime Center and The Federal Bureau of Investigation. Retrieved from https://pdf.ic3.gov/2016_IC3Report.pdf.

Internet Crime Complaint Center. (2018). 2017 *Internet Crime Report*. Washington, DC: The National White Collar Crime Center and The Federal Bureau of Investigation. Retrieved from https://pdf.ic3.gov/2017_IC3Report.pdf.

Jaishankar, K. (2007). Cyber criminology: Evolving a novel discipline with a new journal. *International Journal of Cyber Criminology*, *1*(1), 1-6.

Kohm, S. A., Waid-Lindberg, C. A., Weinrath, M., Shelley, T. O. C., & Dobbs, R. R. (2012). The impact of media on fear of crime among university students: A cross-national comparison. *Canadian Journal of Criminology and Criminal Justice*, *54*(1), 67-100. doi: 10.3138/cjccj.2011.e.01

Maguire, M., & Corbett, C. (1987). *The effects of crime and the work of victims support schemes.* Cambridge Studies in Criminology LVI. Aldershot: Gower.

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.
doi: 10.1080/01639620903004903

Mawby, R. I., & Gill, M. L. (1987). *Crime victims: Needs, services, and the voluntary sector* (Volume 377 ed.). Taylor & Francis.

McGuire, M., & Dowling, S. (2013). Cyber crime: A review of the evidence. *Summary of key findings and implications. Home Office Research report*, *75*.

Ministry of Public Safety. (2009). *Public safety and emergency preparedness Canada: 2009-10 report on plans and priorities*. Ottawa: Ministry of Public Safety. Retrieved from Ministry of Public Safety website: http://www.tbs-sct.gc.ca/rpp/2009-2010/inst/psp/psp-eng.pdf.

Office for National Statistics. (December 2018). Crime in England and Wales: year ending December 2018. Statistical Bulletin. Retrieved from 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. Retrieved from https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingseptember2018#computer-misuse-offences-show-a-decrease-in-computer-viruses.

Parker, K. D. (1988). Black-white differences in perceptions of fear of crime. *The Journal of Social Psychology, 128*(4), 487-494. doi: 10.1080/00224545.1988.9713768

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. doi: 10.1177/0022427810365903

Prensky, M. (2001). Digital natives, digital immigrants. *On the horizon*, *9*(5).

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. doi: 10.1080/13218719.2012.672275

Smith, A., & Anderson, M. (2016). Online Shopping and E-Commerce. *Pew Research Center*.

Smith, W. R., & Torstensson, M. (1997). Gender differences in risk perception and neutralizing fear of crime: Toward resolving the paradoxes. *The British Journal of Criminology, 37* (4), 608-634. doi: 10.1093/oxfordjournals.bjc.a014201

Smyth, S. M. (2010). *Cybercrime in Canadian Criminal law*. Toronto: Carswell.

University of Saskatchewan. (2015). Student headcount and demographics, information & communications technology – reporting and data services. Retrieved from http://www.usask.ca/isa/statistics/students/headcount-demographics.php.

Van der Meer, S. (2015). Enhancing international cyber security: A key role for diplomacy. *Security and Human Rights*, *26*(2-4), 193-205. doi: 0.1163/18750230-02602004

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. doi: 10.1093/esr/jcr053

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

Weinrath, M., Clarke, K., & Forde, D. R. (2007). Trends in Fear of Crime in a Western Canadian city: 1984, 1994, and 2004. *Canadian Journal of Criminology and Criminal Justice*, *49*(5), 617-646. doi: 10.3138/cjccj.49.5.617

Weinrath, M., & Gartrell, J. (1996). Victimization and fear of crime. *Violence and Victims*, *11*(3), 187-197. doi: 10.1891/0886-6708.11.3.187

Yu, S. (2014). Fear of cyber crime among college students in the United States: An exploratory study. *International Journal of Cyber Criminology*, *8*(1), 36-46.

APPENDIX A

Variables and Coding information

Variable	Description	Code
Fear of credit/debit card fraud victimization	During the past month, have you ever felt fearful about being the victim of credit/debit card fraud?	1 = Yes, ever felt fearful 2 = No, never felt fearful
Socio-demographic factors		
Gender	Please indicate your gender	1 = Male 2 = Female
Age	Please indicate your age range	1 = Under 17 2 = 17–23 years 3 = 24–30 years 4 = 31–37 years 5 = 38-44 years 6 = 45-51 years 7 = 52 and over
Marital status (marriage)	Please indicate your current marital status	1 = Single (Never legally married) 2 = Legally married (and not separated) 3 = Separated, but still legally married 4 = Living with a common-law partner 5 = Divorced 6 = Widowed
Ethnicity	What ethnicity do you identify with	1 = Aboriginal 2 = White/Caucasian 3 = African 4 = Asian 5 = Other (please specify)
Annual family income	What category best describes your annual total family income, from all sources before taxes?	1 = Less than $25,000 2 = $25,000 to less than $50,000 3 = $50,000 to less than $75,000 4 = $75,000 to less than $100,000 5 = $100,000 to less than $125,000 6 = $125,000 or more 7 = Don't know/Prefer not to say
Residency status	What is your Residency status	1 = Domestic student (citizen/permanent resident) 2 = International student
Level of studies	Please indicate your level of studies	1 = Undergraduate 1st year 2 = Undergraduate 2nd year 3 = Undergraduate 3rd year 4 = Undergraduate 4th year or more 5 = Graduate 1st year 6 = Graduate 2nd year

		7 = Graduate 3rd year 8 = Graduate 4th year or more 9 = Other (please specify)
Place of residence	Please indicate your place of residence	1 = University residence 2 = Off campus urban 3 = Off campus rural
Mode of study	Are you studying full time or part time	1 = Full time 2 = Part time 4 = Not applicable
Employment status	What best describes your current employment status	1 = Working part time 2 = Working full time 3 = Not working
Knowledge/perception of cybercrime	In your view, what constitutes cybercrime	1 = Crimes committed using computer or its systems as the tool (cyber-enabled) 2 = Crimes committed using computer or its systems as the target (cyber-dependent) 3 = Both above
Victimization experience	During the past 12 months, did anyone steal your credit/debit card or use your card information, without your permission to obtain money or credit	1 = Yes 2 = No
Recoded Variables and Coding Information		
Age		1 = 23 years or less 2 = 24-37 years 3 = 38-51 years or more
Annual family income		1 = $49,000 or less 2 = $50,000 to less than $100,000 3 = $100,000 or more
Marital status		1 = Single 2 = Married
Level of studies		1 = Undergraduate 2 = Graduate 3 = Other (please specify)
Mode of study		1 = Full time 2 = Part time
Place of residence		1 = University residence 2 = Off campus residence