The state of cybercrime in the Jamaican Financial Sector: A consumer perspective

El estado del delito cibernético en el sector financiero de Jamaica: una perspectiva del consumidor

Amoya Mitchell[1]
Janice Small[1]
Salome McKenzie-Russell[1]
Delroy Chevers[1*]

[1]**Mona School of Business and Management – The University of the West Indies**

*__delroy.chevers@uwimona.edu.jm__

Abstract

The prevalence of cybercrime has been an emerging problem since the rise of the technological age. It is posited that cybercrime has been generating a higher payback than drug trafficking and that it is expected to grow further as technology usage expands in developing countries. If the risk of cybercrime is not properly managed, it can result in a decrease in the adoption of e-commerce in both developed and developing countries. This decreased adoption can have a greater impact in developing countries, who are in dire need of commercial activities to boost their economies. However, there is relatively little research in this domain in Jamaica. Hence, the purpose of this study is to assess the state of cybercrime in the Jamaican financial sector. The study found identity theft to be a major cybercrime act in Jamaica, and cybercrime victims exercising greater precautions when conducting online banking transactions. This study intends to provide useful insights to consumers to sensitize them about cybercrime risks, as well as providing guidance to business executives in the formulation of policies and strategies to combat cybercrime.

Keywords: banking industry, cybercrime, e-commerce, Jamaica, online banking.

Resumen

La prevalencia del cibercrimen ha sido un problema emergente desde el surgimiento de la era tecnológica. Se postula que el delito cibernético ha estado generando una recuperación de la inversión más alta que el tráfico de drogas y que se espera que siga creciendo a medida que el uso de la tecnología se expanda en los países en desarrollo. Si el riesgo de delito cibernético no se gestiona adecuadamente, puede provo-

car una disminución en la adopción del comercio electrónico tanto en los países desarrollados como en desarrollo. Esta disminución de la adopción puede tener un mayor impacto en los países en desarrollo, que tienen una gran necesidad de actividades comerciales para impulsar sus economías. Sin embargo, hay relativamente poca investigación en este dominio en Jamaica. Por lo tanto, el objetivo de este estudio es evaluar el estado del delito cibernético en el sector financiero de Jamaica. Elestudio descubrió que el robo de identidad es un acto importante de cibercrimen en Jamaica, y que las víctimas de cibercrimen ejercen mayores precauciones cuando realizan transacciones bancarias en línea. Este estudio pretende proporcionar información útil a los consumidores para sensibilizarlos sobre los riesgos del delito cibernético, así como proporcionar orientación a los ejecutivos de negocios en la formulación de políticas y estrategias para combatir el delito cibernético.

Palabras clave: banca en línea, cibercrimen, comercio electrónico, industria bancaria, Jamaica.

Introduction

The emergence of information technology has impacted almost all aspects of our lives (Deb, 2014). This includes the development of electronic commerce (e-commerce). However, a deterrent to the adoption of e-commerce is cybercrime (Martin and Rice, 2011). Cybercrime is generating higher payback over drug trafficking and this trend is expected to grow even further as technology usage expands in developing countries (Saini, Rao and Panda, 2012). If the risk of cybercrime is not properly managed, it can result in a decrease in the adoption of e-commerce in both developed and developing countries (Boateng, Longe, Mbarika, Avevor and Isabalija, 2010). A low adoption rate can have more negative impact in developing countries, because such countries are in dire need of commercial activities like purchasing, sales and trading to boost their economies.

E-commerce refers to conducting business via electronic media, and most commonly, the Internet (Kinuthia & Akinnusi, 2014). While the term e-commerce refers to all online business transactions, business-to-consumer (B2C) e-commerce applies to any business or organization that sells its products or services to consumers over the Internet, including online retail, online auctions and online banking (Nemat, 2011). The scope of this study is online banking, in which (Hamid, Amin, Lada and Ahmad, 2007) defines as the use of the Internet as a remote delivery channel of banking system services.

According to Riek, Bohme and Moore (2016), online banking has presented a reasonable and effective way of remotely handling financial transactions and that e-commerce has increased product availability while decreasing trading cost. In an effort to reduce operational cost some institutions have elected to adopt and utilize free and open source software (FOSS). In addition, the use of online banking services as a form of business-to-consumer (B2C) e-commerce has proven to be a very convenient, affordable and effective mode of conducting a variety of financial transactions. Studies have found that banks offer online banking services to remain competitive, to keep abreast of technological developments and also to benefit from lower transaction cost (Angelakopoulos and Milhiotis, 2011). Bakare (2015) posited that banks' efficiency in service to customers has improved due to the introduction of online banking. Other benefits highlighted as a result of online banking include the growth in the banking industry, the enhancement of bank- customer relations, improved customer satisfaction and the facilitation of numerous banking transactions (Ojokuku and Sajuyigbe, 2012).

On the other hand, the main disadvantages of online banking are the issues of security and confidentiality (Aribake, 2016). Bakare (2015) noted that despite the advantages brought about by the introduction of online banking in Nigeria, some customers' attitude is still negative due to cybercrime and inadequate or lack of legal protection for bank customers unlike in the USA and Europe. This was supported by Fianyi (2015), who stated that 'despite the successes of e-commerce in the electronic world, there remains an issue of security, often to the detriment of the online consumer and ultimately the business owners'. Its utilization has been plagued by various cybercrime activities, invoking fear and uncertainty into users, and possibly limiting the usage of these services. These security issues are of concern for both proprietory and FOSS applications. In fact, the major challenges affecting the adoption of FOSS are the likelihood of poor quality software being delivered, lack of support and security (Whyte, McNaughton, Chevers and McLeod, 2016). Security issues can be manifested with instances of hacking, phishing and identity theft (Zappa, 2014).

Based on these risks, it is vital that cybercrime be properly managed, as failure to do so may reduce the potential benefits of e- commerce. This study is concern about three popular cybercrime acts that affect consumers in the banking industry – hacking, identity theft and phishing. With regards to phishing, the Verizon Data Breach Investigation Report states that for every fourteen (14) cybercrime phishing e-mails received, only one is successful (Zappa, 2014). According to a report published by the Inter-American Development Bank (2016), Dominican Republic's government reported 963 cases of phishing in 2013, and 432 cases of banking theft from 2009-2014. This is primarily due to its growing quantity of Internet users and availability of e-commerce services and the lack of education relating to cyber security. Singleton (2013) highlighted that the Federal Trade Commission (FTC) ranks identity theft as the number one complaint on its list in 2012, for the thirteenth year in a row.

Additionally, there was a 32% increase in identity theft over 2011. Identity theft of government documents jumped up about 70% in 2012 over 2011 and that Florida continues to be the 'hotbed' for identity theft, which is ranked as number one. Kaur (2013) also found that cases of hacking reported in 2011 was 157 and reported in 2012 was 435 in which the percentage variation in increase in cases over 2011 was 177.1% in India. Strong concern about security is one of the common factors related to the unwillingness of consumers to use Internet banking services (Hamid et al., 2007).

Hamid et al. (2007) further stated that most hackers normally prefer to hack directly through the bank financial system and that in Malaysia, 240 cases of hacking were identified during August 2005 and that there are 10,000 cases reported in one day where hackers were trying to hack the Internet Banking system. It can also be seen where, along with phishing and identity theft, hacking is one critical type of cybercrime that needs immense attention, as well as the need for more data security and encryption.

This study is motivated by the fact that there has been relatively little research in this area, as most of the research relating to cybercrime focuses on the preventative measures to be taken to mitigate the risks and effects of cybercrime, especially at the organizational level. It is stated that cybercrime has become a global issue that requires a multi-stakeholder effort including governments, the private sector, civic and legal institutions, and other social organizations (Boateng et al., 2010).

The main purpose of this research is to assess the state of cybercrime in the Jamaican financial sector, from a consumer perspective. Jamaica was selected based on convenience, as well as the economic and human resource constraints being experienced by the country. Based on the constraints, it is imperative that Jamaicans be efficient at all commercial activities and transactions. As a result, the study focused on business-to-consumer (B2C) ecommerce, particularly online banking, in which consumers utilize electronic means to conduct their banking transactions. Hence the research questions are:

1. What is the level of awareness of cybercrime in Jamaica's banking industry?

2. What is the level of usage of online banking in Jamaica?

3. What is the level of cybercrime acts in Jamaica's banking industry?

4. What is the main cybercrime act being committed in Jamaica?

5. How significant is cybercrime in deterring the use of online banking in the Jamaican banking industry?

It is hoped that this study will provide useful insights to consumers to sensitize them about cybercrime risks, as well as providing guidance to business owners and executives in the formulation of policies and strategies to combat cybercrime.

Literature review

Cybercrime is defined as all criminal activities done using the medium of computers, the Internet, and the worldwide web (Nfuka, Sanga and Mshangi, 2014). It also includes traditional crimes in which computers or networks are used to enable illicit activity (Nfuka et al., 2014). However, in recent times, concerns regarding cybercrime has been one of the most significant issues affecting e-commerce (Martin and Rice, 2011). It is posited that cybercrime has been generating a higher payback than drug trafficking and that it is expected to grow further as technology usage expands in developing countries (Saini et al., 2012). Boateng et al. (2010) concluded that cybercrime is common to both developed and developing countries, but developing countries are faced with a worsening impact due to factors such as inadequacies in technological development.

The 2011 Norton Cybercrime Report disclosed that over 74 million people in the United States were victims of cybercrime in 2010. These criminal acts resulted in $32 billion in direct financial losses. Further analysis of this growing problem found that 69 percent of adults that are online have been victims of cybercrime resulting in 1 million cybercrime victims a day. However, it is believed by some scholars that cybercrime is a fact of doing business online (Al-Alawi, 2014).

Zappa (2014) identified various cybercrime risks and threats. These include fraud, identity theft, theft of sensitive data and intellectual property, espionage, extortion through ransomware, phishing, hacking, spam, pharming, denial of service (DoS) attack, defacement (unauthorized change of websites or web

pages), malware, botnet and social engineering. While these various risks are associated with cybercrime, this study will focus on three main types namely, hacking, phishing, and identity theft.

According to Riek et al. (2016), consumer-oriented cybercrime including identity theft, credit card fraud, hacking and phishing, making the use of online services unsafe for all Internet users. As a result, to avoid unwarranted situations many Internet users remain hesitant to the use of online banking services. Our justification to focus this study on phishing, identity theft and hacking is based on the European Network and Information Security Agency 2013 Trend Landscape Report which shows that cybercrime risks such as phishing, identity theft and data breaches as a result of hacking are on the increase, while those relating to spam and botnets remain stable (Zappa, 2014). In addition, these three acts are closely related with online banking.

Types of Cybercrime

The three types of cybercrimes relevant to this study are phishing, hacking and identity theft. In general, **phishing** is defined as any attempt by a third party to gain access to log-in details, such as usernames and passwords often by use of a false website that appears to be legitimate (Hughes, 2008). It is also described as a type of spam that attempts to

lure the potential victim to disclose certain information that would allow the attacker to gain access to banking profiles or to aid in stealing the victim's identity (Anderson, Durbin and Salinger, 2008).

E-mail users are constantly bombarded with phishing e-mails. Phishing is particularly popular amongst banking websites, pay online websites, and any other website in which an individual is required to enter their credit card information (Hughes, 2008). The perpetrators are referred to as 'phishermen' (Moore et al., 2009). Phishermen operate copies of genuine bank websites and encourage customers to log on to their bank accounts so that bank account numbers, passwords and security questions and answers can be copied and saved. They typically do so by sending e- mails that purport to come from the authentic bank, which is then saved and used to commit the cybercrime. A victim of phishing can become a victim of identity theft or hacking, as this type of personal data obtained about a person can be used in various unlawful ways.

Hacking on the other hand, is the illegal breaking into a computer system, deliberately passing through security measures, usually aimed at gaining access to information stored on that computer system or network (Hughes, 2008). Hacking can be considered a destination for a 'phisherman', as phishermen aim to gain access to sensitive data using their tactics so that they can bypass security measures and gain access to a victim's banking profile or details for their own personal gain. According to an article by Kaur (2013), hacking can be done easily by using a Trojan horse virus. Holt (2013) found that malicious software is increasingly being used by hackers in order to acquire sensitive information and compromise various systems. Holt (2013) further stated that "the sophistication of these tools has increased to such a point that individuals now sell various programs and services through electronic markets where data can be bought and sold". Demirdjian and Mokatisian (2015) posited that hacking is committed either for profit or for simple bragging. The actual cost of hacking is difficult to calculate and companies often hide the fact that they have been attacked or are unaware their confidential information have been stolen.

While **identity theft** is mostly associated with actual online shopping or purchases, the act of paying for online- purchased goods or services may be considered to be a banking transaction. Public awareness of identity theft has increased significantly, both as a public policy issue and a personal threat. Identity theft involves acquiring sufficient data about someone which enables the perpetrator to use the funds in the victim's account, usually to make payments for goods or services (Anderson et al., 2008). As such, fraudulent use of an individual's credit card or other account is a form of identity theft. Singleton (2013) also referred to identity theft (ID theft) as being probably the most common cybercrime perpetrated against individuals; stating that an important aspect of ID theft is that it can take on a wide variety of types: credit card theft and usage, falsified loans, mortgage fraud, medical benefits, theft of money in financial accounts, theft of IRS refunds, and government documents. Identity theft is continuously growing in prevalence. According to the findings of a study, 61% of all victims reported misuse of an existing credit card; 33% reported misuse of existing savings or chequing accounts; while the remainder reported that their existing telephone or wireless accounts have been misused (Anderson et al., 2008).

Effect on Consumers

In a study examining the emotional impact of cybercrime, it was discovered that the strongest reaction of the victims is feeling angry which accounted for 58%, followed by being annoyed which accounted for 51% and cheated which accounted for 40% (Das and Nayak, 2013). In many cases victims blame themselves for being attacked and only 3% believe it will not happen to them again. Sadly, nearly 80% do not expect cybercriminals to be brought to justice (Das and Nayak, 2013). Such statistics imply that there is a fall in the usage of e-commerce services especially in utilizing online banking services. The researchers found that victims often experience symptoms similar to those of post- traumatic stress disorder (PTSD) and that others have found a high risk of secondary victimization among people close to victims (Wiederhold, 2014).

To avoid uncertain and risky situations, many Internet users remain reluctant to use online services. Such reluctance leads to many missing out on social and economic benefits provided by an Internet-connected world. It is posited that the majority of cybercrime costs are indirect opportunity costs, created by users avoiding online services (Anderson et al., 2008). The effects are facilitated by the perceived risk of cybercrime and weakened by the user's confidence. The study confirmed the negative impact of perceived risk of cybercrime on the use of all three online service categories and support the role of cybercrime experience as an originator of perceived risk of cybercrime. The results also showed that the more confident Internet users are, the less cybercriminal risk they perceive and are more likely to use online banking and online shopping.

There is the notion that the increased usage of the Internet, combined with the nature of the Internet itself has presented a threat of cybercrimes that exceeds those of the past (Singleton, 2013). It is argued that a cybercriminal can conduct crimes in anonymity and in the safety of some geographic location where it is possible to be safe from extradition (Singleton, 2013). These factors are very attractive to the perpetrators and have indeed attracted a large number of them.

Angelakopoulos and Milhiotis (2011) conducted a research that examined the challenges and opportunities of e- banking for the Greek banking sector during the e-commerce era. The main factors that

negatively impact the adoption of e-banking services by customers in Greek are the relatively low Internet usage, the non-familiarity with technology advance devices and problems regarding security and privacy. As individuals feel threatened by uncertain situations and try to avoid them, perceived risk is an important factor potentially limiting the intention to use online services (Riek et al., 2016).

Zappa (2014) stated that the majority of Internet users in the European Union (EU) do not feel completely secure about their ability to use online banking or make purchases online and do not know how to safely navigate the exposure. It was further highlighted that many Internet users claim to gain knowledge of cybercrime through television and newspapers but do not feel informed about the risks that they could experience. As such, Zappa (2014) concluded that the lack of awareness about their vulnerability is exploited by cybercrime and is what determines the ease of implementation.

Singh, Kumar, Sengar and Wairiya (2011) cited various instances of hacking and phishing attacks reported throughout India. Cyber issues such as phishing attacks and identity theft continue to deter a lot of consumers from employing the use of electronic mediums for carrying out their banking transactions. They explained that cybercrimes prove that e- banking has several loopholes that can be easily exploited and users need to be extra cautious while making online transactions (Jamaluddin, 2013).

Methodology

This was a quantitative study in which the unit of analysis was individuals. The targeted respondents were consumers of e-banking services in Kingston and St. Andrew, Jamaica. The actual size of the population was unknown, because the information regarding consumers that use online banking is considered confidential. As a result, a convenience sampling approach was taken. More specifically, the researchers used the self-administered survey approach to collect the relevant data. The researchers conducted the data collection at the premises of banking institutions in Kingston and St. Andrew. Based on the self-administered approach, a 100% response rate was achieved. All together sixty completed questionnaires were analysed using the statistical package for the social sciences (SPSS). The scaled questions were anchored on a 5-point Likert scale with 1 being strongly disagree and 5 being strongly agree. The results of the analysis are shown in the findings section.

Findings

The profile of the respondents saw 26 males and 34 females. 51.7% of the respondents were 30 years old and younger, 45% between 31 – 40 years, 10% between 41 – 50 years and 3.3% over 50 years old. Table 1 provides an overview regarding the awareness of cybercrime, usage of online banking and the outcome of cybercrime experiences. A large majority of the respondents (98.3%) were aware of cybercrime but only 15% were victims of cybercrime. A large majority of the respondents (95%) used online banking as a means of transacting businesses with banks. For those who were victims of cybercrime 78% expressed the need to be more careful. It is interesting to note that no respondent had expressed the desire to stop using the online banking service after being a victim of cybercrime. In addition, 44% of the respondents considered the experience more of an inconvenience rather than a financial loss.

Figure 1 highlights the types of cybercrimes being experienced, with identity theft, such as credit card information theft, being the main act. The study found significance between the type of cybercrime experienced and the subsequent behaviour to further conduct online banking transactions (see Table 2). This means that the encounter of a cybercrime act will impact the behaviour of such individual. The p-value in Table 2 is 0.000, which is below the 0.05 threshold. Hence, significance was established.

Table 1. Awareness of cybercrime, usage of online banking and behaviour

Element	Percentage	Number of Respondents
Awareness of cybercrime	98.3%	59
Victim of cybercrime	15%	9
Users of online banking	95%	57
Subsequent use of online banking after being a victim More careful No impact Stopped using online banking	78% 22% 0%	47 13 0
Outcome of cybercrime experience Inconvenience	44% 25%	26 15
Financial loss **Stress, worry and fear**	25% 6%	15 4

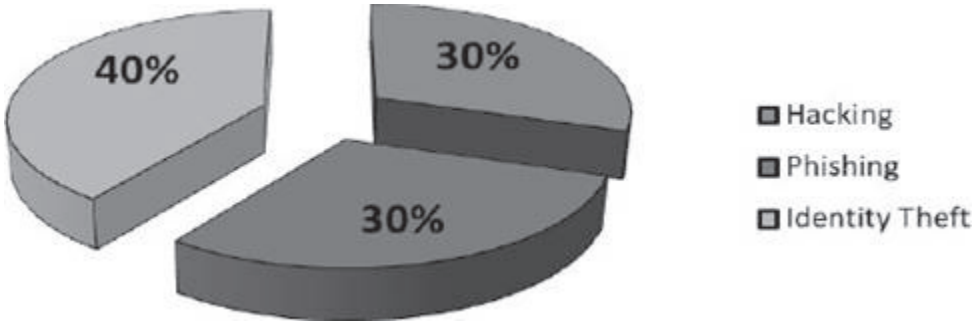

Figure 1. Types of cybercrime

Table 2. Significance test between cybercrime experience and subsequent behaviou

Chi-Square Tests			
	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	100.714[a]	8	0.000
Likelihood Ratio	57.487	8	0.000
Linear-by-Linear Association	36.916	1	0.000
N of Valid Cases	60		
a. 13 cells (86.7%) have expected count less than 5. The minimum expected count is .03.			

Table 3. Loss experienced due to cybercrime

		Hacking of Online Banking Profile	Identity Theft	Phishing	Never been a cybercrime victim	Hacking and Indentity Theft	Total
Suffer Financial Loss	n	0	1	1	0	0	2
	% of Type of Loss	0.0%	50.0%	50.0%	0.0%	0.0%	100.0%
	% of Type of Cybercrime	0.0%	33.3%	33.3%	0.0%	0.0%	
	% of sample total	0.0%	1.7%	1.7%	0.0%	0.0%	3.4%
I was inconvenienced	n	1	0	0	0	1	2
	% of Type of Loss	50.0%	0.0%	0.0%	0.0%	50.0%	100.0%
	% of Type of Cybercrime	50.0%	0.0%	0.0%	0.0%	100.0%	
	% of sample total	1.7%	0.0%	0.0%	0.0%	1.7%	3.4%
I have never been a victim of cybercrime	n	0	0	0	51	0	51
	% of Type of Loss	0.0%	0.0%	0.0%	100.0%	0.0%	100.0%
	% of Type of Cybercrime	0.0%	0.0%	0.0%	100.0%	0.0%	
	% of sample total	0.0%	0.0%	0.0%	85.0%	0.0%	85.0%
I was inconvenienced and embarrassed	n	0	0	1	0	0	1
	% of Type of Loss	0.0%	0.0%	100.0%	0.0%	0.0%	100.0%
	% of Type of Cybercrime	0.0%	0.0%	33.3%	0.0%	0.0%	
	% of sample total	0.0%	0.0%	1.7%	0.0%	0.0%	1.7%
I was inconvenienced and experienced stress, worry and fear	n	0	1	1	0	0	2
	% of Type of Loss	0.0%	50.0%	50.0%	0.0%	0.0%	100.0%
	% of Type of Cybercrime	0.0%	33.3%	33.3%	0.0%	0.0%	
	% of sample total	0.0%	1.7%	1.7%	0.0%	0.0%	3.4%
Financial loss, inconvenience, stress, worry and fear	n	1	1	0	0	0	2
	% of Type of Loss	50.0%	50.0%	0.0%	0.0%	0.0%	100.0%
	% of Type of Cybercrime	50.0%	33.3%	0.0%	0.0%	0.0%	
	% of sample total	1.7%	1.7%	0.0%	0.0%	0.0%	3.4%
Total	n	2	3	3	51	1	60
	% of Type of Loss	3.3%	5.0%	5.0%	85.0%	1.7%	100.0%
	% of Type of Cybercrime	100.0%	100.0%	100.0%	100.0%	100.0%	1
	% of sample total	3.3%	5.0%	5.0%	85.0%	1.7%	100.0%

On an average 3.75% of the respondents indicated adverse outcomes from their experience with cybercrime. These outcomes are inconvenience, financial loss, being stressed or embarrassed. Most of the adverse outcomes were related to hacking of online profiles (3.3%), phishing (5.0%) and identity theft (5.0%) or a combination of hacking and identity theft (1.7%). Table 3 provides a detailed breakdown of the outcomes. In addition, Appendix A - cybercrime experience by type and gender, as well as Appendix B – cybercrime experience by type and age group provide further details regarding the findings of this study. However, it is important to note that females experienced more cybercrime acts than males in Jamaica and also that individuals who are thirty years old and younger experienced more cybercrime acts than all other age groups.

Discussion

In general, there is a high level of awareness of cybercrime (98.3%) and a low level of cybercrime acts (15%) in Jamaica. The findings also indicate that the usage of online banking is very high (95%) in Jamaica. The most widely used e-banking service is online bill payment (75%), online shopping using debit and/or credit card (75%), electronic funds transfer (71.7%), and online balance inquiries (68.3%).

Importantly, (Saini et al., 2012) highlighted that many Internet users are unwilling to use online banking services which leads to many individuals missing out on the social and economic benefits provided by e-commerce, more specifically online banking. Similarly, Jamaluddin (2013) found that a significant number of online users do not utilize online banking. In another study conducted by the Internet and Mobile Association of India (IAMAI) it was discovered that security concerns accounted for 43% of the reasons why people are reluctant or hesitant to do banking or financial transactions through banks' Internet websites. In addition, the study by Makarevic (2015) showed that Bosnian clients were not very open to the idea of online banking. These findings differ significantly from the findings of this research. This may be attributable to the fact that physically going into banks in these other countries may be less time-consuming and more convenient than it is in Jamaica. The inconvenience associated with joining long queues in Jamaican banks may influence persons (particularly those of a younger age group) to use the more convenient, online banking avenues available to them.

In contrast to expectation is the finding in which the number of cybercrime acts are relatively low (15%). The findings in Table 1 shows that no cybercrime victim has completely stopped using online banking. Instead, they have become more conscious of the potential risks involved.

It was expected that once an individual becomes a cybercrime victim, then their behaviour with respect to online banking would change negatively. Of the nine (9) cybercrime victims in this study, a majority (78%) indicated that they are more careful when conducting online banking, while a few indicted that they have not been impacted in any way (22%).

The Federal Trade Commission ranks identity theft as the number one complaint in 2012 for the thirteenth consecutive year (Singleton, 2013). This finding is consistent with our study where identity theft was found to be the main cybercrime in Jamaica. All individuals who were victims of identity theft in this study, have reported that they are more careful when conducting online banking transactions. Similarly, Nemat (2011) found that despite the growing fears about identity theft, North American consumers spent $172 billion online, using credit cards to make purchases, compared to $38.8 billion in 2000. This therefore indicates that the threat of individuals having their identity stolen and used to conduct unauthorized transactions does not deter the use of the more convenient means that e-commerce provides.

Of importance, is the fact that 22% of the persons who were victims of cybercrime reported that their hacking experience did not impact them in anyway. This finding differs from expectation.

Another contradiction to our expectations is that none of the respondents indicated that they have stopped using online banking completely. The general expectation was that prior experience with cybercrime would have encouraged individuals to desist the use of online banking. As discussed by Riek et al. (2016), consumer-oriented cybercrime makes the use of online services unsafe for all Internet users and thus, many Internet users remain hesitant to use online banking services to avoid cybercriminal implications. Similarly, the study by Jamaluddin (2013) also found that; security concerns accounted for 43% of the reasons why people are reluctant or hesitant to do banking or financial transactions through banks' Internet websites.

The most significant result arising from previous cybercrime experience was inconvenience, followed by financial loss. While the expectation was that emotional impacts (stress, worry and fear) would account for majority of the feelings, this may be as a result of the geographical location from which the sample was taken. Kingston, Jamaica is characterized by a fast- moving culture. Therefore, a cyberattack for some individuals will be more about the inconvenience associated with being unable to execute their normal online banking transactions, rather than it is about the financial loss or emotional impacts. Das and Nayak (2013) made a different discovery. Upon examining the emotional impact of cybercrime they revealed that the strongest reaction of the victims is feeling angry which accounted for 58%, followed by being annoyed which accounted for 51% and cheated which accounted for 40%. Victims also blamed themselves for being attacked. This suggests that emotional impacts take precedence.

Conclusion

The five research questions were answered. In a few cases the findings in this study differ from prior research or expectation. The difference might be as a result of the constraints or cultural factors. For example, identity theft is a type of online banking risk, usually associated with online purchases via a credit or debit card. With the findings and other supporting statistics indicating that identity theft is the most prevalent type of cybercrime, the difference in the low cybercrime victim rate in this study may be due to the fact that the trend of online shopping is still at the emerging stage in Jamaica, since the advent of courier companies that facilitate shipping to an overseas address. As such, identity theft is likely to be higher in the other countries explored in prior research, particularly the United States, where online shopping has been well adopted. More frequent engagement in activities that expose users to cybercrime may increase the likelihood that they will be impacted.

Hacking, phishing and identity theft are three (3) major risks that affect the use of ecommerce by consumers. Consumers do not have to be victims to be impacted by cybercrime, or to be aware and more vigilant of the potential effects of cybercriminal activities. Instead, it has been concluded that the mere knowledge of cybercrime, as well as the personal experience or experience by someone known to the consumer, impacts their behaviour towards cybercrime.

While online banking becomes a growing trend for convenience and simplicity of business transactions, cyber security continues to be a cause for growing concern.

How significant is cybercrime in deterring e-commerce in the banking industry? Cybercrime is not a significant deterrent. However, it impacts how consumers think when conducting business transactions using online banking, regardless of whether they have been victims or not. Concerns about cybersecurity will remain in the minds of the consumers and will impact their behaviour when conducting online banking transactions.

Two limitations of the study are the small sample size and the fact that the data was collected from only one parish in Jamaica – Kingston and St. Andrew. This prevents the results from being generalizable. Future research should expand the data collection into other parishes. In addition, deeper insights could be sought with respect to gender and age groups.

This study intends to provide useful insights to consumers to sensitize them about cybercrime risks, as well as providing guidance to business executives in the formulation of policies and strategies to combat cybercrime.

References

Al-Alawi, A. I. (2014). Cybercrimes, computer forensics and their impact in business climate: Bahrain status. *Research Journal of Business Management*, *8*(3), 139-156.

Anderson, K. B., Durbin, E., & Salinger, M. A. (2008). Identity theft. *Journal of Economic Perspectives*, *22*(2), 171-192.

Angelakopoulos, G., & Milhiotis, A. (2011). E-banking: challenges and opportunities in the Greek banking sector. *Electronic Commerce Research*, *11*(3), 297-319.

Aribake, F. O. (2016). Impact of ICT tools for combating cybercrime in Nigeria online banking: A conceptual review. *International Journal of Trade, Economics and Finance*, *5*(3), 56-60.

Bakare, S. (2015). Varying impacts of electronic banking on the banking industry. *Journal of Internet Banking and Commerce*, *20*(2), 1-9.

Boateng, R., Longe, O. B., Mbarika, V., Avevor, I., & Isabalija, S. R. (2010). Cybercrime and criminality in Ghana: Its forms and implications. Paper presented at the Americas Conference on Information Systems.

Das, S., & Nayak, T. (2013). Impact of cybercrime: Issues and challenges. *International Journal of Enginering Sciences & Emerging Technologies*, *6*(2), 142-153.

Deb, S. (2014). Information technology, its impact on society and its future. *Advances in Computing*, *4*(1), 25-29.

Demirdjian, Z. S., & Mokatisian, Z. (2015). *The cost of cyber crimes to business and society*. Paper presented at the American Society of Business and Behavioural Sciences.

Fianyi, I. D. (2015). Curbing cybercrime and enhancing e-commerce security with digital forensics. *International Journal of Computer Science Issues*, *12*(6), 78-85.

Hamid, M. R. A., Amin, H., Lada, S., & Ahmad, N. (2007). A comparative analysis of Internet banking in Malaysia and Thailand. *Journal of Internet Business*, *4*, 1-19.

Holt, T. J. (2013). Examining the forces shaping cybercrime markets online. *Social Science Computer Review*, *31*(2), 165-177.

Hughes, T. F. (2008). A report on safe use of the Internet: Some of the most common risks. *Hispania*, *91*(2), 408-411.

Inter-American Development Bank. (2016). Cybersecurity - Are we ready in Latin America and the Caribbean? *Inter-American Development Bank*, 1-193.

Jamaluddin, N. (2013). *E-Banking: Challenges and opportunities in India*. Paper presented at the 23rd International Business Research Conference.

Kaur, R. P. (2013). Statistics of cybercrime in India: An overview. *International Journal of Engineering and Computer Science*, *2*(8), 1-16.

Kinuthia, J., & Akinnusi, D. M. (2014). The magnitude of barriers facing e-commerce businesses in Kenya. *Journal of Internet and Information Systems*, *4*(1), 12-27.

Makarevic, N. (2015). Comparative analysis of perceptions towards IT security in online banking: Serbian clients vs clients of Bosnia and Herzegovina. *Journal of Business Studies Quarterly*, *7*(2), 242-257.

Martin, N., & Rice, J. (2011). Cybercrime: Understanding and addressing the concerns of stakeholders. *Computers & Security*, *30*(8), 803-814.

Nemat, R. (2011). Taking a look at the different types of e-commerce. *World Applied Programming*, *1*(2), 100-104.

Nfuka, E. N., Sanga, C., & Mshangi, M. (2014). The rapid growth of cybercrimes affecting information systems in the globe: Is this a myth or reality in Tazania. *International Journal of Information Security Science*, *3*(2), 182-199.

Ojokuku, R. M., & Sajuyigbe, A. S. (2012). The impact of electronic banking on human resources performance in the Nigerian Banking Industry. *International Journal of Economic Development Research and Investment*, *3*(2), 61-70.

Riek, M., Bohme, R., & Moore, T. (2016). Measuring the influence of perceived cybercrime risk on online service avoidance. *IEEE Transaction on Dependable and Secure Computing*, *13*(2), 261-273.

Saini, H., Rao, Y. S., & Panda, T. C. (2012). Cyber-crimes and their impacts: A review. *International Journal of Engineering Research and Applications*, *2*(2), 202-209.

Singh, A. P., Kumar, V., Sengar, S. S., & Wairiya, M. (2011). Detection and prevention of phishing attack using dynamic watermarking. *Information Technology and Mobile Communication*, *147*, 132-137.

Singleton, T. (2013). Fishing the cybercrime plague. *Journal of Corporate Accounting & Finance*, *24*(5), 3- 7.

Whyte, S., McNaughton, M., Chevers, D.A. & McLeod, M. (2016). Measuring software quality in open source communities through the lens of social capital. *Revista Cubana de Ciencias Informaticas*, *10*, 287-302.

Wiederhold, B. K. (2014). The role of psychology in enhancing cybersecurity. *Cyberpsychology, Behavior, and Social Networking*, *17*(3), 131-132.

Zappa, F. (2014). Cybercrime: Risks for economy and enterprises at the EU and Italian level. *United Nations Interregional Crime and Justice Research*, 1-138.

Appendix

Appendix A – Cybercrime experience by type and gender

Categories of Cybercrime Experienced by Respondents		Male	Female	Total
Hacking of Online Banking Profile	n	1	1	2
	% of category	50.0%	50.0%	100.0%
	% of gender	3.8%	2.9%	
	% of total sample	1.7%	1.7%	3.3%
Identity Theft	n	1	2	3
	% of category	33.3%	66.7%	100.0%
	% of gender	3.8%	5.9%	
	% of total sample	1.7%	3.3%	5.0%
Phishing	n	0	3	3
	% of category	0.0%	100.0%	100.0%
	% of gender	0.0%	8.8%	
	% of total sample	0.0%	5.0%	5.0%
Never been a cybercrime victim	n	23	28	51
	% of category	45.1%	54.9%	100.0%
	% of gender	88.5%	82.4%	
	% of total sample	38.3%	46.7%	85.0%
Hacking and Indentity Theft	n	1	0	1
	% of category	100.0%	0.0%	100.0%
	% of gender	3.8%	0.0%	
	% of total sample	1.7%	0.0%	1.7%
Total	n	26	34	60
	% of category	43.3%	56.7%	100.0%
	% of gender	100.0%	100.0%	
	% of total sample	43.3%	56.7%	100.0%

Appendix B – Cybercrime experience by type and age group

Categories of Cybercrime Experienced by Respondents		30 years or younger	31 - 40 years	41- 50 years	Over 50 years	Total
Hacking of Online Banking Profile	n	1	1	0	0	2
	% within category	50.0%	50.0%	0.0%	0.0%	100.0%
	% within age group	3.2%	4.8%	0.0%	0.0%	
	% of total saample	1.7%	1.7%	0.0%	0.0%	3.3%
Identity Theft	n	1	1	1	0	3
	% within category	33.3%	33.3%	33.3%	0.0%	100.0%
	% within age group	3.2%	4.8%	16.7%	0.0%	
	% of total saample	1.7%	1.7%	1.7%	0.0%	5.0%
Phishing	n	3	0	0	0	3
	% within category	100.0%	0.0%	0.0%	0.0%	100%
	% within age group	9.7%	0.0%	0.0%	0.0%	
	% of total saample	5.0%	0.0%	0.0%	0.0%	5.0%
Never been a cybercrime victim	n	26	18	5	2	51
	% within category	51.0%	35.3%	9.8%	3.9%	100.0%
	% within age group	83.9%	85.7%	83.3%	100.0%	
	% of total saample	43.3%	30.0%	8.3%	3.3%	85.0%
Hacking and Indentity Theft	n	0	1	0	0	1
	% within category	0.0%	100.0%	0.0%	0.0%	100%
	% within age group	0.0%	4.8%	0.0%	0.0%	
	% of total saample	0.0%	1.7%	0.0%	0.0%	1.7%
Total	n	31	21	6	2	60
	% within category	51.7%	35.0%	10.0%	3.3%	100%
	% within age group	100.0%	100.0%	100.0%	100.0%	
	% of total saample	51.7%	35.0%	10.0%	3.3%	100.0%