Association for Information Systems
AIS Electronic Library (AISeL)

CONF-IRM 2019 Proceedings

International Conference on Information Resources Management (CONF-IRM)

5-2019

The impact of cybercrime on e-banking: A proposed model

Delroy A. Chevers
The University of the West Indies, delroy.chevers@uwimona.edu.jm

The impact of cybercrime on e-banking: A proposed model

Delroy A. Chevers
The University of the West Indies
delroy.chevers@uwimona.edu.jm

Abstract
Each day cybercrime attacks are getting more frequent, dangerous and sophisticated. In 2016 the FBI's Internet Crime Complaint Center received 1,408,849 complaints and a reported loss of $4.63 billion. The concept of cybercrime is complex, and as such the drive to overcome the problem is very difficult. However, the continual escalation of cybercrimes can have a negative impact on businesses and by extension the economies of countries. As a result, it is imperative that measures be identified to overcome the problem. Hence, this study seeks to propose a research model which can be used to evaluate the significance of cybercrime in deterring the use of e-banking in the financial sector. It is hoped that the proposed research model will influence other researchers to conduct empirical research in their context.

Keywords
Cybercrime, electronic banking, e-commerce, financial institutions

1. Introduction
Information technology has pervaded all aspects of our lives (Deb, 2014). This development includes the emergence of electronic commerce (e-commerce). However, cybercrime attacks is a deterrent to the adoption of e-commerce (Martin & Rice, 2011). Cybercrime is defined as all criminal and illicit activities done using computers, the Internet, and the worldwide web (Nfuka, Sanga, & Mshangi, 2014). There is the notion that these illicit activities are generating higher payback than drug trafficking (Saini, Rao, & Panda, 2012). This trend is expected to grow exponentially as the usage of technology expands in both developed and developing countries (Boateng, Longe, Mbarika, Avevor, & Isabalija, 2010; Saini et al., 2012; van de Weijer & Leukfeldt, 2017).

With each passing day cybercrime attacks are getting more frequent, dangerous and sophisticated (Smith, 2017). In 2016, the Federal Bureau of Investigation (FBI) - Internet Crime Complaint Center received 1,408,849 complaints and a reported loss of $4.63 billion (Smith, 2017). In 2016, the older folks (i.e. age group over 60 years old) suffer the most loss with 55,043 reported cases at a total loss of $339,474,918. The number one cybercrime attack in 2016 was business email compromise/email account compromise (BEC/EAC) with a total loss of $360,513,961. This was followed by identity theft, credit card fraud, phishing and hacking at $58,917,398, $48,187,993, $31,679,451 and $55,500 respectively (Smith, 2017).

Undoubtedly, cybercrime poses a dangerous threat to our society and it is becoming a part of everyday living (van de Weijer & Leukfeldt, 2017). If the threat of cybercrime is not controlled and managed, it can manifest in low adoption of e-commerce in developed and

developing countries (Boateng et al., 2010). A low adoption rate can have a negative impact on businesses, and by extension nations.

E-commerce is about conducting business via electronic media, with the most common medium being the Internet (Kinuthia & Akinnusi, 2014). The term e-commerce refers to all online business transactions such as purchases made on Amazon, online flight booking, online auctions and electronic banking (Nemat, 2011). The scope of this study is business-to-consumer (B2C) e-commerce, with particular focus on electronic banking (commonly called e-banking). Electronic banking is defined as the use of the Internet as a remote delivery channel of banking system services via the World Wide Web (Hamid, Amin, Lada, & Ahmad, 2007), a medium in which cybercrime is prevalent.

The concept of cybercrime is complex because it encompasses a wide range of crimes which can be motivated by economic, emotional, psychological and ideological factors (Leukfeldt, Lavorgua, & Kleemans, 2017). This makes the task of combatting the problem very difficult (Liao, 2017). But the continual escalation of cybercrime attacks can have a negative impact on business performance and the economies of nations (Holt, Freilich, & Chermak, 2017; van Erp, 2017). Consequently, it is important that efforts be made to overcome the problem. This study seeks to propose a research model which can be used to evaluate the effect of cybercrime on e-banking in the financial sector. Hence, the research question is, what is the significance of cybercrime attacks in deterring the use of e-banking in the financial sector? The contribution of the study is the presentation of a proposed research model to the information systems community. It is hoped that the proposed research model will influence other researchers to conduct empirical research in various contexts.

2. Literature Review

Cybercrime was the 2nd most reported crime in 2016 (Cook, 2017). It was also ranked as a major issue affecting e-commerce (Martin & Rice, 2011). The 2012 Norton Cybercrime Report stated that 556 million individuals in 24 countries were victims of cybercrime attacks in 2011 (Palmer & Merritt, 2012). These attacked resulted in $110 billion in financial losses. Sixty seven percent of individuals who were online became victims of cybercrime attacks. This resulted in 1.5 million cybercrime victims per day (Palmer & Merritt, 2012). Unfortunately, this figure is expected to increase because more and more persons are gaining access to computers and the Internet. In June 2017, about 51.7% of the world had access to the Internet (Internet World Stats, 2017) and the Internet serves as a vehicle that can facilitate cybercrime attacks (Liao, Balasinorwala, & Rao, 2017).

The risk of becoming a victim of a cyberattack is paramount on the agenda of individuals and companies (van Erp, 2017). Some examples of the main industries being targeted are health care, the chemical industry, defense systems, the prison system, energy services, airlines and the financial sector (van Erp, 2017). A number of cybercrime risks and threats have been identified in the literature. These as distilled by Eboibi (2017) include:

- Electronic auction or retail-based fraud schemes; Stock scams
- Work at home scams; Online advance fee fraud scams
- Web cloning; Piracy; Online lottery fraud
- Fraudulent loan scams; Job scams; Denial of service (DoS) attack
- Romance scams; Impersonation; Credit card fraud
- Phishing; Identity theft; Hacking

It is posited that the common types of cybercrime, especially computer assisted ones, are phishing, identity theft and hacking (Liao et al., 2017). Furthermore, it is reported that in 2015, 5.1% of citizens in the Netherlands were victims of hacking, 3.5% of online consumer fraud, and 0.6% of identity theft (Statistic Netherlands, 2016). In addition, it is posited that consumer-oriented cybercrime includes identity theft, credit card fraud and phishing (Riek, Bohme, & Moore, 2016). Equally important is the declaration that cybercrime attacks like phishing, identity theft and hacking are on the increase, while spams and denial of service attacks remain stable (Zappa, 2014). It is widely agreed that many of the attacks in the financial sector involve phishing, identity theft and hacking (Leukfeldt et al., 2017; Liao et al., 2017; van Erp, 2017). Hence, this study focuses on these three popular cybercrimes (i.e. phishing, identity theft and hacking) that affect financial institutions like banks, credit unions, building societies and insurance companies.

2.1 Combatting Cybercrime

In an effort to overcome cybercrime a multi-stakeholder approach is needed (Boateng et al., 2010). This would involve governments, legal institutions, the private sector and other social organizations (p. 2). (Arief, Adzmi, & Gross, 2015) explained that an improved understanding of cybercrime would contribute to better measures and awareness in preventing and combating cybercrime. In an attempt to combat cybercrime, financial institutions utilize a wide variety of techniques. According to (Anderson, Durbin, & Salinger, 2008), authentication can be classified into three categories: knowledge-based authentication, which speaks to information the consumer is expected to know such as password, personal details; token-based authentication, based on a physical token such as a credit or debit card or an actual security token and biometrics (fingerprints, retina scans or signatures).

Education can help victims to be aware of cybercrime like phishing. This view was supported by (Abdul-Rasheed, Lateef, Yinusa, & Abdullateef, 2016), who posited that education is a very important factor in combating cybercrime and that persons need to be educated on how to prevent cybercrime, how cybercrime works and the harmful effects of cybercrime in the society. The report also highlights that the private sector has outpaced the government in its recognition of the importance of cyber security.

2.2 Model Development

Cybercrime has developed into an industry in which attackers are now operating internationally (Arief et al., 2015). This growth is due mainly to the fact that cyberattacks can be conducted with a high degree of anonymity (Singleton, 2013). As a result, the likelihood of being able to identify the perpetrator is very low. In addition, victims usually blame themselves for being attacked, only 3% don't think it will happen to them and 80% do not believe that these criminals will be brought to justice (Abdul-Rasheed et al., 2016; Das & Nayak, 2013). These startling statistics result in a reluctance to adopt e-commerce in the banking sector. This reluctance can lead to missed opportunities in an Internet-connected world. Furthermore, it was discovered that the more confident Internet users are, the less they perceived being attacked by cybercriminals, which by extension can increase the likelihood of adopting e-commerce (Anderson et al., 2008).

Studies have discovered that banks engage in e-banking to keep abreast of technological development, lower transaction cost, achieve greater efficiency, enhance bank-customer relationship, improve customer satisfaction, and to gain competitive advantage

(Angelakopoulos & Milhiotis, 2011; Bakare, 2015; Ojokuku & Sajuyigbe, 2012). Electronic banking has offered a useful and efficient way of remotely handling financial transactions and also that e-commerce has increased product availability while decreasing trading cost (Riek et al., 2016). So non-adoption can have a negative impact on firm's operations. In the midst of these potential benefits there remains the issue of security, fear and uncertainty by online consumers and ultimately business owners (Fianyi, 2015). These issues can limit or retard the utilization of e-commerce services. (Kumar, 2009) found numerous instances of hacking and phishing attacks being taken place in India. These attacks (i.e. phishing and hacking) can deter a lot of consumers from employing the use of electronic mediums for carrying out their banking transactions.

Phishing as defined by (Liao et al., 2017) is "the act of sending fake messages to the victim, often in the disguise of bank notifications or emails promising monetary gains and romantic relationships, luring the victim into handing over sensitive information such as account number and password, or install malware on the victim's system" (p.444). It is a type of spam that seeks to lure targeted victims to disclose certain information like usernames and passwords, which can then be used by the attacker to gain access to further banking information or can assist in stealing the victim's identity (Anderson et al., 2008; Hughes, 2008).

Phishing activities are popular on websites in which individuals are required to enter their credit card information (Hughes, 2008). Websites such as banking and pay online are prone to these activities. The attackers operate copies of genuine bank websites and encourage potential victims to log on to their bank accounts. At this point sensitive information such as bank account numbers, passwords and the answers to security questions can be copied, saved and stored. Attackers typically perform these activities by sending emails under the disguise that these emails are coming from their authentic bank. Upon retrieval of such information, the attackers commit various cybercrimes.

Some major categories of phishing are clone and spear phishing (Khan, 2013). Spear phishing is a technique in which a specific victim is targeted. Basic information is known about the potential victim prior to the attack. Potential victim could receive an email from a would-be friend, relative or financial institution which prompt the victim to provide certain confidential information or perform certain task. In these instances, because the email is coming from a friend or relative, there is a high level of trust. As a result, the likelihood of success of these attacks is very high (Khan, 2013). On the other hand, as distilled by Khan (2013) clone phishing is a case where "a legitimate previously sent email containing an attachment or link has had its content and recipient address (es) taken and used to create a cloned email (p. 7). These two categories of phishing are modelled as indicator variables for the construct 'Phishing' in the proposed research model (see Figure 1).

H1: Phishing will have a negative impact on the adoption of electronic banking

A victim of phishing can become a victim of hacking or identity theft because the information gathered on the victim can be used in many unlawful ways (Moore, Clayton, & Anderson, 2009). Although identity theft is mainly associated with online shopping, the act of payment being made for online purchasing of goods or services can be considered a banking transaction. Identity theft is described as the acquisition of sufficient information about a victim which enables the attacker to use the funds in the victim's account to make payments

for goods and services (Anderson et al., 2008). It can include personal information such as credit card numbers, phone numbers and email addresses (Liao et al., 2017). Credit card theft and usage, falsified loans, mortgage fraud, medical benefit fraud, and theft of funds in financial accounts are some of the identity theft attacks (Singleton, 2013).

Identity theft is believed to be the most common cybercrime being done to individuals (Singleton, 2013). It was found that 61% of all cybercrime victims reported misuse of their credit card, 33% reported misuse of savings or chequing accounts and the others reported that their wireless account or telephone have been misused (Anderson et al., 2008).

The literature makes reference to four categories of identity theft (Moskovitch et al., 2009). These are:

- Financial identity theft – Using another's identity to obtain goods and services
- Identity cloning – Using another's information to assume his or her identity in daily life
- Business identity theft – Using another's business name to obtain credit
- Criminal identity theft – Posing as another when apprehended for a crime

Criminal identity theft was scoped out of this study because posing as another when apprehended is not directly related with the adoption of e-commerce. Hence, the three former attacks (i.e. financial identity theft, identity cloning and business identity theft) were used as indicator variables for the 'Identity theft' construct (as shown in Figure 1 - The proposed research model).

H2: Identity theft will have a negative impact on the adoption of electronic banking

Hacking is considered a destination for a phishing attacker (Hughes, 2008). It is the illegal breaking into a computer system by deliberately passing through security measures with the aim of stealing information that is stored on the computer or network (Liao et al., 2017). These cyberattacks are easily executed by using a Trojan horse virus (Kaur, 2013). These attacks are usually committed for profit or for bragging purposes (Demirdjian & Mokatisian, 2015). The actual cost of hacking is difficult to quantify and many companies hide the fact that they have been attacked.

Hackers are generally described as white, black and grey hats (Furnell, 2001; PreuB, Furnell, & Papadaki, 2007). White hat hackers are scoped out of this study because they are hackers working for the good of system security (Furnell, 2001). They are usually employed by organizations to keep data safe from bad hackers by finding areas of vulnerabilities. They are sometimes referred to as 'ethical' hackers. This study is concerned about the impact of bad hackers.

The majority of hackers are black hat hackers (Furnell, 2001). These hackers intrude into systems in an unauthorized manner with malicious intentions. They usually steal, exploit and sell information and in general are motivated by personal gain. Grey hackers are those who hack mainly for fun. Their motives at times are unclear and it is expected that they can change their behavior quite easily (Furnell, 2001). Both black and grey hat hackers are incorporated into the proposed research model as indicator variables for the 'Hacker' construct.

H3: Hacking will have a negative impact on the adoption of electronic banking

The indicator variables for the 'Adoption of e-commerce' construct are taken form the information technology adoption literature. They are the actual usage of e-banking and the intention to use e-banking.

There are many technology adoption/diffusion theories that are applicable in this study. However, the technology acceptance model (Davis, 1989) is being recommended because it is the most widely used theory of users' acceptance and usage of technology (Venkatesh & Davis, 2000). The theory proposes that when users are confronted with a new technology, a number of factors influence their intention to use and decision to use the technology. In essence it depicts how users eventually accept and use a new technology. As a result, this theory is concerned about the acceptance and utilization of new technology. Hence, the dependent variable in this theory is the usage of the new technology - e-banking. The indicator variables for the 'Adoption of e-banking' construct are actual usage and frequency of use (see Figure 1). The resultant research model has three independent variables namely, phishing, identity theft and hacking and one dependent variable (i.e. adoption of e-banking).

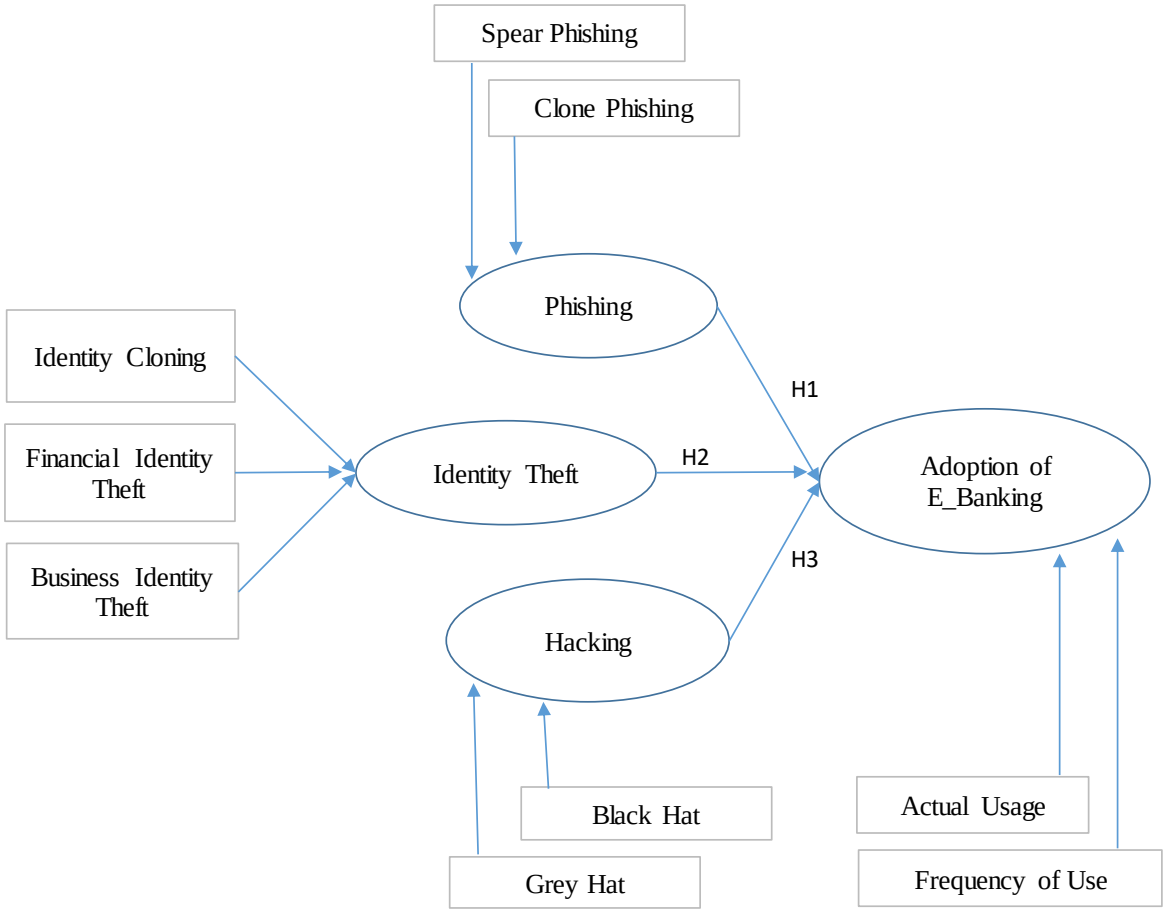

Figure 1: The Research Model

Based on the literature three hypotheses were derived for this study as shown in Figure 1. It is hoped that the proposed research model can be validated through empirical studies in the near future.

3. Methodology

This study is intended to be quantitative. The approach to be taken will be a survey, in which the three hypotheses will be tested. The unit of analysis is individual. The control variables are age, gender, income, occupation and race. These control variables will be captured among the demographic questions of the survey instrument. The other questions will be 5-point likert type scaled questions with 1 being strongly disagree and 5 being strongly agree. The statistic package for social sciences (SPSS) is recommended as the analytical tool to conduct the data analysis. The survey items will be newly developed and so a pre-test of the items is necessary. Based on the result of the pre-test, the necessary adjustments will be made to the items for reliability and validity reasons. The findings of the study will relate back to the research question and prior studies in the literature.

In an effort to further refine the proposed research model, a series of focus group sessions with non-users of e-banking method could be conducted to ascertain the reasons for not using e-banking. This additional approach could improve the robustness of the study and consequently provide deep insights in the domain of cybercrime and e-banking.

4. Conclusion

The contribution of this study is the submission of a proposed research model. Upon completion of the validation process, the study should be able to confirm or falsify the three hypotheses regarding phishing, identity theft and hacking and their impact on the adoption of e-banking. In addition, the study will be able to determine which of the three independent variables has the greatest impact on the adoption of e-banking. It is hoped that the proposed research model will influence other researchers to conduct empirical research in their respective context.

5. Reference

Abdul-Rasheed, S., Lateef, I., Yinusa, M., & Abdullateef, M. (2016). Cybercrime and Nigeria's external images: A critical assessment. *Africology: The Journal of Pan African Studies, 9*(6), 119-132.

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.

Arief, B., Adzmi, M. A. B., & Gross, T. (2015). Understanding cybercrime from its stakeholders' perspectives: Part 1 - attackers. *IEEE Security & Privacy, 13*(1), 71-76.

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.

Cook, S. (2017). Cybercrime stats and facts for 2016 - 2017. *Comparitech*, 1-11.

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

Davis, F. D. (1989). Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. *MIS Quarterly, 13*(3), 319-340.

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.
Eboibi, F. E. (2017). A review of the legal and regulatory frameworks of Nigerian cybercrimes Act 2015. *Computer Law & Security Review, 33,* 200-217.
Fianyi, I. D. (2015). Curbing cybercrime and enhancing e-commerce security with digital forensics. *International Journal of Computer Science Issues, 12*(6), 78-85.
Furnell, S. M. (2001). *The problem of categorising cybercrime and cybercriminals.* Paper presented at the 2nd Australian Information Warefare and Security Conference, Churchlands, Australia.
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., Freilich, J. D., & Chermak, S. M. (2017). Exploring the subculture of ideologically motivated cyber-attackers. *Journal of Contemporary Criminal Justice, 33*(3), 212-233.
Hughes, T. F. (2008). A report on safe use of the Internet: Some of the most common risks. *Hispania, 91*(2), 408-411.
Internet World Stats. (2017). Internet usage statistics: World Internet users and 2017 population stats. *Internet World Stats,* 1-6.
Kaur, R. P. (2013). Statistics of cybercrime in India: An overview. *International Journal of Engineering and Computer Science, 2*(8), 1-16.
Khan, A. A. (2013). Preventing phishing attacks using one time password and user machine identification. *International Journal of Computer Applications, 68*(3), 7-11.
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.
Kumar, G. (2009). Cyber warfare - A global threat. *International Journal of Information Technology and Knowledge Management, 2*(1), 119-122.
Leukfeldt, E. R., Lavorgua, A., & Kleemans, E. R. (2017). Organised cybercrime or cyber crime that is organised? An assessment of the conceptualisation of financial cybercrime as organised crime. *European Journal of Criminology Policy Research, 23,* 287-300.
Liao, R., Balasinorwala, S., & Rao, H. R. (2017). Computer assisted frauds: An examination of offender and offense characteristics in relation to arrests. *Information Systems Frontiers, 19,* 443-455.
Martin, N., & Rice, J. (2011). Cybercrime: Understanding and addressing the concerns of stakeholders. *Computers & Security, 30*(8), 803-814.
Moore, T., Clayton, R., & Anderson, R. (2009). The economics of online crime. *Journal of Economic Perspectives, 23*(3), 3-20.
Moskovitch, R., Feher, C., Messerman, A., Kirschnick, N., Mustafic, T., Camtepe, A., . . . Elovici, Y. (2009). Identity theft, computers and behavioral biometrics. *Informatics,* 155-160.
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.
Palmer, A., & Merritt, M. (2012). 2012 Norton Cybercrime Report *Norton,* 1-27.

PreuB, J., Furnell, S. M., & Papadaki, M. (2007). Considering the potential of criminal profiling to combat hacking. *Journal of Computer Virology, 3*, 135-141.
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.
Singleton, T. (2013). Fishing the cybercrime plague. *Journal of Corporate Accounting & Finance, 24*(5), 3-7.
Smith, S. S. (2017). 2016 Internet Crime Report. *Federal Bureau of Investigation - Internet Crime Complaint Center*, 1-26.
Statistic Netherlands. (2016). *Veiligheidsmonitor 2015*. Den Haag: Centraal Bureau voor de Statistick.
van de Weijer, S., & Leukfeldt, E. R. (2017). Big five personality traits of cybercrime victims. *Cyberpsychology, Behavior, and Social Networking, 20*(7), 407-418.
van Erp, J. (2017). New governance of corporate cybersecurity: A case of the petrochemical industry in the Port of Rottendam. *Crime Law Social Change, 68*, 75-93.
Venkatesh, V., & Davis, F. D. (2000). A theoretical extension of the technology acceptance model: Four longitudinal field studies. *Management Science, 46*(2), 186-204.
Zappa, F. (2014). Cybercrime: Risks for economy and enterprises at the EU and Italian level. *United Nations Interregional Crime and Justice Research*, 1-138.