ASSESSING THE PREVALENCE OF CYBERCRIME IN MAURITIUS

VANISHA OOGARAH-HANUMAN[1] – YANNICK LI LUEN CHING[2] – ANNICK YEUNG PAT WAN[3] – DAREN CHETTY[4]

Hodnotenie výskytu kybernetickej kriminality v štáte Maurícius

Abstract: *The ICT sector is a key sector in Mauritius and the Vision 2030 of the Government is to transform Mauritius into a SMART island, an evolution of the Cyber Island which was envisioned in 2001 (Cybercrime Strategy, 2017). With the goal to embed the use of technology in the day-to-day life of every Mauritian, the ICT sector has brought along new opportunities, but at the same time new threats. With cyber criminals becoming more sophisticated and continuing to develop malicious software and devising improved methods for infecting computer systems and networks, the government has set up a legal framework to limit potential cybercrime attacks on the island of Mauritius (Republic of Mauritius). In order to address the dearth of research relating to the prevalence of online crime and its consequences to the general public, we administered one of the first surveys on the prevalence of cybercrime among Mauritius citizens. 276 respondents were surveyed and the results show that while 98% of the respondents have a high level of awareness about cybercrime, there is the need for more sensitization campaigns about the dangers pertaining to cybercrime.*

Keywords*: Cybercrime, Mauritius, ICT Sector*

[1] Vanisha Oogarah-Hanuman, University of Mauritius , Faculty of Law and Management, Réduit, 80837 Mauritius, e-mail: v.hanuman@uom.ac.mu

[2] Yannick Li Luen Ching, University of Mauritius , Faculty of Law and Management, Réduit, 80837 Mauritius.

[3] Annick Yeung Pat Wan, University of Mauritius , Faculty of Law and Management, Réduit, 80837 Mauritius.

[4] Daren Chetty, University of Mauritius , Faculty of Law and Management, Réduit, 80837 Mauritius.

JEL Classification: M 15

1 Introduction

Cybercrimes have been gaining ground during the past recent years and authorities around the globe have been sending out alarm signals over the damaging effects that cybercrime can induce. There is actually no agreed single definition of cybercrime and broadly, cybercrime is depicted as fraudulent activities perpetrated through the use of a computer system. Cybercrime is causing huge losses to countries around the globe and even a small island like Mauritius has not been spared by this growing threat. Cyber criminals can operate from anywhere in the world, targeting large numbers of people or businesses across international boundaries, and there are challenges posed by the scale and volume of the crimes, the technical complexity of identifying the perpetrators as well as the need to work internationally to bring them to justice. The Internet opens new opportunities to cyber criminals and enables aspiring criminals to enter the environment, based on a belief that law enforcement struggles to operate in the online world. Cybercrimes are affecting millions of people around the world and the impacts of a successful cybercrime attack can have profound implications on the mental state of a person, the society and the economy as a whole. Consequently, this paper will aim at analyzing the prevalence of cybercrime in Mauritius and to achieve this aim, the following research objectives have been set:

- Assess the occurrence of cybercrime in Mauritius
- Identify the potential loopholes in the regulations governing cybercrime in Mauritius
- Evaluate the awareness of Mauritians on cybercrime.
- Determine if victims of cybercrimes reported their cases to the appropriate authorities

2 Literature Review

In the attempt to explain why cybercrime occurs three most cited frameworks have been considered for this study namely: the Self Control theory, the Routine Activity theory and the theory of Technology-Enabled Crime.

2.1 Self Control theory

Self-control theory has been the focal point of several experimental studies, in the attempt to test the authenticity of the theory in explaining crimes [21]. The self control theory states that criminal motivation is unbridled; however only people with low self control act upon this motivation [8]. This is because these people are considered to be reckless, cold-blooded, physical, thrill-seeking, and thoughtless, and as such are more susceptible to embark in criminal activities [11].

A vital question stem from this theory, does an individual's level of self control expand over time or does it remain constant throughout an individual's lifetime right from his or her birth [9]. According to Hirschi and Gottfredson [11], a particular level of self control is not acquired from birth; it is mostly through their parents and upbringing that individuals learn self control. Self control theory can be used not only to predict deviant activities but also to provide explanation on an individual's partaking in crimes [20].

The self control theory has been extended by many researchers to analyze the reasons why individuals get involved in cybercrimes. For instance, a study that applied self control theory to cybercrimes revealed that it was individuals with a low self control that were more attracted in viewing online pornography rather than those with a high self-control [3]. The self control theory has also been extended by many researchers to study the grounds on which some individuals are more prone than others to be a victim of cybercrime [9]. A research work carried out in 2010 on students attending college pointed out

that the students who had low level of self control were more vulnerable to be victims of fraud [12].

As illustrated by various studies, self control theory provides explanation on the diverse reasons on which some individuals base themselves to embark in criminal behaviours and also the reasons why some individuals are more susceptible to be victims of crimes [21].

2.2 Routine Activity Theory

The Routine Activity Theory (RAT) was developed in 1979 by Lawrence Cohen and Marcus Felson [7]; they contended that there should be three pre-requisites for a crime to occur notably:

(i) a motivated offender,

(ii) an appropriate target , and

(iii) the absence of a capable guardian.

In simpler terms, when a motivated offender manages to identify an appropriate target while a capable guardian is not present to preempt the crime from happening, crime occurs [7]. For instance, if an individual is motivated to rob a house but there is always someone in the house, that particular individual will not be able to undertake his robbery. The theory also emphasizes on the fact that only an opportunity is needed for a crime to be committed that is, when all three elements are present at the same time and in the same space.

However, the absence of any of the three elements will avert the likelihood of a criminal act [18]. Cohen and Felson [7] pointed out that an individual's daily routine activities are standardized and once a probable offender synchronizes his deviant activities with the daily routines of the target, the offender may find an opportunity to commit a crime.

The RAT was extensively used by many researchers to study cybercrime as the internet provides a platform where attractive targets are easily accessible by motivated offenders and the fact that the internet is so vast and unpredictable makes it almost impossible to monitor; thereby eliminating capable guardianship [9]. For example, a study carried out with college students demonstrated that those students that have multiple social networking accounts and who routinely used their accounts to engage in online communications and chats were most vulnerable to online harassment as they are more probable to come into contact with a potential offender [10].

Nevertheless, Yar [25] argued that the application of the RAT to the study of cybercrime can be challenged due to the difference that exist in time and space in the real world and the cyber world. He further added that cybercrime is a new crime as it takes place in a world where there is no physical or time restriction and new theories is required to explain it.

2.3 Theory of Technology-Enabled Crime

The most suitable theory to explain cybercrime is undoubtedly the Theory of Technology-Enabled crime, put forward by McQuade in 1998. This theory being a relatively new one encompasses numerous categories of criminological theories in view of providing reasonable explanations in the understanding of the evolving nature of cybercrimes [19].

As stated by McQuade [17] there exist three phases of technology-enabled impacts namely:

(i) ordinary crime

They are the conventional types of crimes that are well understood by everybody for example harassment, theft and frauds amongst others.

(ii) adaptive crime

Adaptive crimes are like deviations from the ordinary crime that is they

are orthodox crimes committed by using new technology for instance, cyber bullying, credit card fraud, online pornography etc…

(iii) new crime

New crimes are high-tech crimes that emerged from the use of new innovative technologies and that many do not understand due to its complexity like denial of service attacks, hacking, malware, and viruses. Until new crimes are understood, a policy lag is created as new laws have not yet been passed to deter such crimes. However, over time, after new forms of crimes are completely understood and relevant statutes are passed, new crimes shift into the category of ordinary crimes as illustrated in the figure below:

For this particular reason McQuade [17] reported that law enforcement must be in line with advancement in technology so as to control and prevent new crimes from happening.

2.4 Cybercrime in Africa

The amplifying increase in broadband services on the 'black continent' has expanded the internet user base with 167,335,676 users as at 30 June 2017 [14]. Despite its economic difficulties, there has been an increase in the internet penetration from Africa which engendered the proliferation of cybercrimes. Unfortunately, African countries have more pressing issues to solve, for example poverty, political instability, corruption, and aids amongst others consequently neglecting the rise and the dangers of computer crimes. As a result Africa has been branded the etiquette of 'safe haven' for cybercriminal due its inability to deal with cybercrime [5]. As a matter of fact, out of the 57 African countries only five countries implemented cybercrimes laws namely Botswana, Cameroon, Kenya, Mauritius, South Africa and Zambia [15]. Nigeria is one of the African countries that is more affected by

the cybercrime phenomena, being third on the list of the world cybercrime perpetrator countries [13].

2.5 Cybercrime in Mauritius

Mauritius is aiming at transforming itself into a cyber island and also an ICT hub in the Indian Ocean. The government of Mauritius strongly believes that the ICT sector will constitute one of the major pillars of the Mauritian economy [23]. However, conscious of the impeding dangers of IT, the government has tried overcome potential threats by implementing several legal measures pertaining to cybercrime namely:

2.5.1 Computer misuse and Cybercrime Act 2003

The Act is a representation of the COE's Convention on Cybercrime and is the main act to prevent and punish cybercrimes in Mauritius; it has been enacted to provide for the repression of criminal activities perpetrated by using computer systems. Crimes such as hacking, denial of service, virus, electronic fraud, and financial crimes are prosecuted under this Act. The various sentences to the different offences made are further described in Appendix 2.

2.5.2 Information Communication Technology Act 2001

This Act has been implemented to regulate and democratise ICT and related matters. The Act makes it an offence for people making wrongful use information and communication service. The Information & Communication Technology Authority (ICTA) has been established under this Act to license and regulate Internet Service Provider (ISP). An Information and Communication Technologies Appeal Tribunal has also been set up to hear and dispose of any

appeal against a decision of the ICTA. Offences such as cyber bullying and child pornography can be prosecuted under this Act.

2.5.3 Data Protection Act 2004

It has been enacted to protect the privacy rights of the Mauritians taking into account latest advancement in the techniques utilized to capture, process, manoeuvre, record or store data relating to individuals. A Data Protection Office has been established for investigation of any complaint that has been made under this Act. Crimes that can be prosecuted under this Act are credit card fraud and identity theft.

2.5.4 The Electronic Transaction Act (ETA) 2000

The ETA 2000 was enacted to facilitate the establishing of legal validity of electronic records, transactions, contracts, and digital signatures and by putting in place a legal framework for determining the time and place, when and where, an electronic communication is dispatched and received.

2.5.5 Budapest Convention on Cybercrime

Mauritius acceded to the convention in November 2013. The ideology of the Convention is being implemented through the Global Action on Cybercrime (GLACY) project. The objective of the GLACY project is to foster international cooperation in the fight against cybercrime. It is to be noted that priority was given to Mauritius along with six other countries to benefit from the project [6].

2.5.6 Enforcement Agencies in Mauritius

Various enforcement agencies have been established to combat cybercrime and to enforce the various laws promulgated notably:

The Cybercrime Unit

The cybercrime Unit was created considering the Computer Misuse and Cybercrime Act 2004. This special unit of the police force has the responsibility to investigate cases of cybercrime when complaints are received. They also need to take proactive measures to hinder the occurrence of potential cybercrime cases.

Information & Communication Technology Authority

The ICTA has the responsibility to take reasonable measures to restrict harmful and illicit content on the internet. In this optic, the ICTA launched the Child Sexual Abuse (CSA) Filtering whereby the images or videos of CSA are filtered and removed from the net consequently preventing access to internet users in Mauritius. Moreover, the ICTA has to consider and take action based on complaints made by the public in relation to any information and communication service.

National Cybercrime Prevention Committee (NCPC)

The NCPC has been set up under the aegis of the ICTA to handle cybercrime at national level, to foster cooperation of relevant bodies in investigating computer crime and to organize workshops in view of promoting awareness on cyber security.

The Mauritian Computer Emergency Response Team (CERT-MU)

CERT-MU is a division of the National Computer Board (NCB) that has been set up to provide information and assistance to the public in implementing proactive measures to mitigate the risks and dangers associated to cybercrime

and also reacting to such incidents as and when they arise.

3 Methodology

During the last decade, Information Technology (IT) has revolutionized the way business is conducted in Mauritius. Businesses that used to rely on cash transactions and physical printed dissemination of information, have already shifted to digital content. The level of risk that comes along with the free flow of information has increased in parallel. In response to this concern, the Government of Mauritius has come up with a National Cyber Security Strategy in 2017 to empower law enforcement agencies with the right tools to "detect, handle and prosecute cybercriminals" [24].

This aim of this study is to investigate the degree to which Mauritians are aware of the potential threat of cybercrimes in order to devise strategies to sensitise the population. Our research question relates to whether factors including age and education have an impact on cybercrime rates in Mauritius.

In order to answer our research problem, the research objectives are:

- Assess the occurrence of cybercrime in Mauritius
- Identify the potential loopholes in the regulations governing cybercrime in Mauritius
- Evaluate the level of awareness of Mauritians on the issue of cybercrime
- Determine whether victims have reported cases of cybercrime

The hypotheses that have been established are as follows:

H_0: Age is not a factor in being a victim of cybercrime

H_1: Age is a factor in being a victim of cybercrime

H_0: Users of the internet believe that crimes cannot be committed on the internet

H_2 and H_3: Users of the internet believe that crimes can be committed on the internet

H_0: Education is not related to awareness of the Computer Misuse and Cybercrime Act 2003

H_1: Education is related to awareness of the Computer Misuse and Cybercrime Act 2003

4 Data Sources and Data collection methods

Semi-structured interviews and surveys were used as research instruments in this study. A questionnaire covering the themes "demography", "Computer and Internet Usage", "Cybercrime awareness" and "Personal opinions and experiences of the community" was designed. Before administering the questionnaire to the target audience, pilot testing was carried out on a sample of 10 people chosen at random during lunch time (noon) on a busy main road in the city centre of Port Louis. Some questions were rephrased to ensure clarity and understanding.

Based on a 90% confidence interval with an estimated Mauritian population of 1,265,309 inhabitants [16], the sample size was estimated to be at 271. We rounded off the figures and took a sample of 300 respondents.

The stratified random sampling method was used. The 300 questionnaires were allocated to 9 districts over the island. 288 out of the 300 questionnaires were filled out. This represents a response rate of 96%. From the 288 questionnaires collected, 12 were considered as unusable since they were incomplete. Consequently, 276 questionnaires were deemed adequate for data analysis.

5 Findings

The SPSS software package was used to process the data collected from the questionnaires. Out of the 276 respondents surveyed, 142 and 134 were males and females respectively (51% male and 49% female). 43% of the respondents fell within the age group 18-30 years old. Those within the age group 51-60 and above 60 years represented 5% and 1% respectively. These data show that people making up the elder age group were more reluctant to participate in the survey. The educational background of the respondents was mainly the Higher School Certificate and an undergraduate degree accounting for 48% and 39% respectively.

An overwhelming majority of respondents corresponding to 93% reported owning a personal computer. When asked about the location of internet access, 85% of the respondents favoured accessing the internet at home while other modes included the workplace, educational institution, free WIFI hotspots, public libraries and through their mobile data.

When prompted about their notion of cybercrime, a majority representing 98% of the respondents agreed that the internet cyberspace is a place where cybercrimes are committed. The remaining 2% disagreed claiming that they were unaware of this potential threat. The respondents' knowledge and understanding of the main types of cybercrimes were assessed. "Virus attacks, pornography, hacking and email spam" bagged the highest scores as opposed to cybercrime threats such as "salami shaving, denial of service attacks, cyber terrorism, and malware" were among those ignored by a large number of respondents.

66% of the respondents believe there is an agency for investigating cybercrimes in Mauritius while 33% are unaware of the existence of such a law enforcement agency. An open-ended question was set to assess whether respondents knew any of the agencies investigating or preventing cybercrimes in Mauritius. Out of the 276 respondents, only 141 responded to this question. The most common response gathered (34 out of 141) indicated

the Independent Commission Against Corruption (ICAC). People were misinformed that this agency is mandated to fight against corruption and bribery cases and not against cybercrimes.

62% of the respondents reported to have been victims of cybercrime (171 respondents). Out of the 171 respondents, only 12% of them have been victims of cybercrime only once while 88% reported being cybercrime victims more than twice. It can be deduced that no preventive measures have been taken by victims after the first attack. When asked about whether they reported the case to the relevant authorities, only 36% responded favourably. The reasons why the majority has not reported anything is that they managed to fix the problem themselves or did not know who to report to. The preventive measures taken by the respondents to minimize the risk of being cybercrime victims were also evaluated. 20% of the respondents believed that using strong passwords, updated antivirus software (19%), avoiding disclosure of confidential information to third parties online (17.1%) would help reduce the risk of being a cybercrime victim.

6 Analysis of hypotheses

Table 1

Outcomes of the hypothesis testing

	Factor	Pearson Chi-Square	Decision
1	Age and Victim of cybercrimes	0.073	Accept H_0
2	Users' belief and Occurrence of crime on the Internet	0.000	Reject H_0
3	Education and awareness of the Computer Misuse and Cybercrime Act	0.000	Reject H_0

Source: Author's calculations.

6.1 Hypothesis 1

Since p=0.073 (>5%), we fail to reject the null hypothesis and hence conclude

that age is not a factor in being a victim of cybercrime at the 5% significance level. This finding contradicts what Campbell and Wabby [4] and Bick [1] found out in their research. According to Campbell and Wabby [4], elderly people are "easy and attractive targets" since they are not well versed with the latest technologies. This is further supported by Brick [2] (2003) who found that elderly people are the "most likely to be affected by cybercrimes" as they have more free time to spend on the internet.

6.2 Hypothesis 2

Since p=0.000 (<5%), we reject the null hypothesis in favor of the alternative hypothesis. This shows that at the 5% significance level, internet users believe that crimes can be committed online. This finding aligns with Cohen and Felson [7] who found that the risk of being a victim of cybercrime increases when one is virtually exposed to offenders. Users become exposed by accessing phishing emails, communicating with malevolent individuals or making online transactions through unsecured portals.

6.3 Hypothesis 3

Since p=0.000 (<5%), we reject the null hypothesis in favour of the alternative hypothesis. We conclude that at the 5% significance level, education has a relationship with being aware of the Cybercrime and Computer Misuse Act 2003. This implies that the more educated a person is the more aware will he be of the laws in place. Saxena [22] found that the enhancement of the educational system about cybercrime laws will likely lead to a more conscious and secured country.

7 Recommendations and Future Research

In order to mitigate the risks of cybercrimes in Mauritius, the views of

participants in the survey have been gathered. Out of 260 responses obtained from this question, 102 respondents believe that there should be more sensitization campaigns in schools and over the national broadcast network about the dangers related to cybercrimes. By educating the population about the potential root causes and consequences of cybercrime, internet users will be more cautious.

76 respondents out of 260 believe that the laws governing cybercriminal activities should be reinforced to act as a deterrent. Instead of engaging into a "name and shame" activity, preventive measures such as virtual security barriers should be installed to block potential malevolent activities. Also, there should be a reward system and guaranteed protection of whistleblowers. Other respondents recommended curative measures such as the presence of additional cybercrime agencies as well as hiring more cybercrime experts to monitor the national IT system.

An interesting area for future research could be the impact of cybercrimes on businesses, more specifically about the vulnerability of various businesses in Mauritius.

8 Conclusion

The aim of this study was to assess the prevalence of cybercrimes in Mauritius and it was found that despite several legal measures adopted by the government, the problem remains unresolved. The findings of the study gives a glimpse of the level of awareness Mauritians have towards cybercrimes. The study also revealed that the majority of the victims of cybercrimes do not report to the authorities concerned, thus it can be deduced that cybercrimes are much more prevalent in Mauritius than what is being reported by Statistics Mauritius.

References

[1] BICK, B. J. 2011. Internet Crime and the elderly. In: *New Jersey Law.* 2011. Vol. 2, 4.

[2] BRICK, A. 2003. *The elderly most at risk from cyber-crime.* UK, Engineering and Technology.

[3] BUZELL, T. – FOSS, D. – Middleton, Z. 2006. Explaining use of online pornography: A test of Self-control theory and opportunities for Deviance. In: *Journal of Criminal Justice and Popular Culture.* 2006. Vol. 13, 2.

[4] CAMPBELL, R J – WABBY, J. The Elderly and the Internet: A case study. In: *Internet Journal of Health.* Vol. 3, 1.

[5] CASSIM, F. 2011. Addressing the growing spectre of cyber crime in Africa: Evaluating measures adopted by South Africa and other regional role players. In: *The Comparative and International Law Journal of Southern Africa.* 2011. Vol. 44, 1.

[6] CHEDUMBRUM, T. P. 2014. *Explanatory Workshop on Budapest Convention.* 2014.

[7] COHEN, L. – FELSON, M. 1979. Social change and crime rate trends: A routine activity approach. In: *American Sociological Review.* 1979. Vol. 44, 4 .

[8] CULLEN, F. – AGNEW, R. 2006. *Criminological theory:past to present essential readings.* New York : Oxford University Press, 2006. 3rd edition.

[9] GRZYBOWSKI, K. M. 2012. *An examination of Cybercrime and Cybercrime Research: Self-control and Routine Activity Theory.* 2012.

[10] HENSON, B. – REYNS, B. W. – FISCHER, B. S. 2011. Security in the 21st century: Examining the link between online social network activity, privacy and interpersonal victimization. In: *Criminal Justice Review.* 2011. Vol. 36, 3.

[11] HIRSCHI, T. – GOTTFREDSON, M. R. 1990. *The General theory of Crime.* Stanford University Press, 1990.

[12] HOLTFRETER, K. et al. 2010. Low self-control and fraud: Offending,victimization and their overlap. In: *Criminal Justice and Behavior.* 2010. Vol. 37, 2.

[13] IC3, 2017. 2017. *Internet Crime COmplaint Center.* 2017.

[14] Internet World Stats, 2017. *Internet World Stat.* [Online] Availableat:https://www.internetworldstats.com/stats.htm [Accessed 12 August 2017].

[15] KHAROUNI, L. 2013. Africa: A new safe harbor for cybercriminals? *Trend Micro Incorporated Research Paper.* 2013.

[16] Mauritius, Statistics. 2018. *Population and Vital Statistics: Republic of Mauritiu.* 2018.

[17] MCQUADE, S. 1998. Technology enabled Crime, Policing and Security. In: *The Journal of Technology Studies.* 1998.

[18] MIETHE, T. D. and MEIER, R F. 1994. *Crime and its social context: toward an integrated theory of offenders, victims and situations.* Albany : State University of New York Press, 1994.

[19] OLAYEMI, J. 2014. *A socio-technological analysis of cybercrime and cyber security in Nigeria.* Nigeria : Civil Defence Academy, 2014.

[20] PRATT, T. C. and CULLEN, F. 2000. The empirical status of Gottfredson and Hirschi's general theory of crime: A meta-analysis. In: *Criminology.* 2000. Vol. 38, 3.

[21] REISIG, M. D. and PRATT, T. C. 2011. Low self-control and imprudent behavior revisited. In: *Deviant Behavior.* 2011. Vol. 32, 7.

[22] SAXENA, P. KOTIYAL, B. and GOUDAR, R. 2012. A cyber era approach for building awareness in cyber security for educational system in India. In: *International Journal of Information and Education Technology.* 2012. Vol. 2, 2.

[23] SOOKDAWOOR, O. 2005. *An investigation of information security policies and practices in Mauritius.* 2005.

[24] Strategy, Cybercrime. 2017. *Cybercrime: Any crime that involves a computer and a network.* 2017.

[25] YAR, M. 2005. The novelty of cybercrime: An assessment in light of routine activity theory. In: *European Journal of Criminology.* 2005. Vol. 2, 4.