Journal of Sustainable Development in Africa (Volume 18, No.2, 2016)
ISSN: 1520-5509
Clarion University of Pennsylvania, Clarion, Pennsylvania

UNDERSTANDING CYBER SCAMS:

AN ASSESSMENT OF THE CHALLENGES OF LAW ENFORCEMENT IN BOTSWANA

[1]Tarisayi Andrea Chimuka and [2]Lesedi Mashumba- Paki

[1]Department of Theology and Religious Studies, University of Botswana

[2]Department of Social Sciences , University of Botswana

ABSTRACT

Richard Harriman[1] made a statement that scores of Batswana are still getting their hard earned money siphoned by investment scams from all around the world[2]. Batswana are continuously being hard hit by cyber scams and frauds. With the advancement of information communication technology (ICTs) the world has turned into one global marketplace for businesses and giving all nations a chance to develop. However, these ICTs pose a challenge to governments wishing to provide laws that govern online trade and other forms of social interaction. Much as ICTs are celebrated as the engines that drive global trade, they can expose governments, businesses and individuals to cyber-attacks. These attacks often take different forms including cyber scams.On the local scene, cyber scams tend to retard the impressive economic development that Botswana has been praised for by instilling fear of victimization in potential investors. This paper seeks to investigate the downside of cyber scams and their impact on sustainable development. It also assesses the challenges of law enforcement in investigating, apprehending, prosecuting and extraditing cyber offenders, as well as gives recommendations.

Keywords: Cybercrime, cyber scam, internet fraud, legal challenges, real-world crimes, crime control mechanisms, sustainability, Development

[1] *Richard Harriman is from the Consumer Watchdog*

[2] *Post 2008/9 recession, was a company by the name Stock Market Direct (SMD) which vanished from Botswana with P3 million of investment funds from multiple individuals. Then it was Eurex Trade which promised up to two per cent daily returns on online trading. It swindled individuals who had invested in the company and they lost millions of Pulas of their investment funds*.

INTRODUCTION

All over the world there are unscrupulous individuals trying to cheat other people of their hard earned money. Botswana is no exception to the experience of cyber scams or fraud. As Broadhurst et al outlines, the information revolution has given rise to many new ways to commit theft, and many new things to steal (Broadhurst, 2014, p. 1). It is not easy to define these computer based crimes (Matengu, 2012, p. 19). Cybercrime is one of the terms used to denote the use of computer technology to engage in unlawful activity (Hoscheid, 2014, p. 446). Yet, the advent of Information and Communication Technologies (ICTs) held the promise of sustainability and development.

At the centre of current thinking about development and economic prosperity are twin factors: (i) environmental sustainability and the possible role of ICTs (Souter, 2010, p. 4). Souter et al contend further that the notion of sustainability holds the promise of long- term benefits and prosperity for humans now and in the future (Souter, 2010, p. 4). In this vein, any development thinking that focused on short-term rewards is discouraged (ibid.).

Stouter further argue that the inception and development of ICTs has profoundly affected the way economic activities, social structures and the behavior of individuals (Souter, 2010, p. 4). They envision a "post-industrial Information Society, in which knowledge and networks play a more prominent role than capital and hierarchy" (ibid.). Alexander Schatten observes that also the development of ICTs has initially seen as a problem for sustainable development along with global warming, the degradation of biodiversity, dependency on non-sustainable energy non-management of natural resources and the lack of proper disposal of production waste among others, this perception has changed (Schatten, p. 1). ICTs can be used to monitor the transformation of global economic developments towards the direction of sustainability (ibid. p.2). For any development process to qualify as 'sustainable', that it meets the needs of the present without compromising the ability of future generations to meet their own needs (World Commission on Environment, 1987, p. sec 27).
This point is also highlighted by Nwabueze and Oziolo when they say; "Sustainable development leads to fulfilment of societal ideals considered relevant to the needs and aspirations of the society" (Nwabueze, 2011, p. 1)

Thus, knowledge and information has a role to play in sustainable development. As maintained by Amritah Singh, knowledge is an important resource together with others such as land, labour and money and has to be used to improve people's lives (Singh, p. 1). Some scholars notably Cader, have referred to it as the knowledge economy (Cader, 2008, pp. 117-8). In this regard, ICTs are an important component (Bandyopadhyay, 2005, pp. 1-3). To this end, theorists have been pondering on a number of questions concerning the role of ICT in sustainable development. Lorenz Hilty and David Hercheui have compressed the questions into the following:
(i) How can we use ICT to increase our understanding of ecosystems and to reduce environmental burden?
(ii) How can we use ICT to support (virtual) communities working towards the aim of sustainable development?
(iii) How can ICT contribute to a decoupling of economic growth from growth in resource consumption, to substitute virtual forms of production and consumption for energy-intensive processes, to dematerialize relevant parts of the economic system? (Hilty, 2010, p. 229).

Holden et al acknowledges the importance of the concept ‘sustainable development’ (Holden, 2014, p. 130). However, there is a potential problem if ‘sustainable development’ is seen only as key to human happiness and as a pathway to human progress (ibid.). There is need also to examine carefully what sustainable development amounts to. Apparently there is a down side to it, particularly in the use of ICTs. Singh cautions us:

> Information is not a magic cure for hunger or poverty. However, the right information at the right time can help in finding a solution. ICT have proven that they can help to aid SD when used appropriately, with the full participation of all stakeholders, especially the poor. The intrinsic value of ICT lies not in easing communications and information but rather in enabling growth and development (Singh, p. 7).

In no time the internet has risen from a facility of immense fascination to an essential tool of life (Bargh, 2004, p. 2). The rise in ICT usage in the global economy has fermented the rise of internet based crime, also known as cyber-crimes (Saini, 2012, p. 202). These crimes are numerous (Kunz, 2004). Since there are a whole lot of different cybercrimes, for purpose of this paper the author seeks to understand specifically the phenomena of cyber scams/frauds. Kunz & Wilson assert that cyber scams/fraud remains one of the most popular crimes in cyberspace, especially with the success of online shopping and Internet auctions which have increased opportunities for offenders (Kunz, 2004, pp. 4,5). The most popular crimes are credit card fraud and auction fraud. Apart from that, the development of assets administered in computer systems (electronic funds, deposit money, e-gold) has become the target of manipulations.

Cyber scams also referred to as internet fraud**,** can specifically be defined as crimes involving the use of one or more components of the internet to deprive a person of property by providing false or misleading information. Examples of cyber scams or internet fraud, email letter frauds, false websites, credit card scams, romance scams, lottery scams (Huang, 2011, pp. 9-13). Since “Internet fraud/scam" generally refers to any type of fraud scheme that uses one or more online services - such as chat rooms, e-mail, message boards, or Websites (Brenner S. W., 2004, p. 4) - to present fraudulent solicitations to prospective victims, the scope of this paper boarders around various types of theft schemes/online fraud, internet investment scam, credit card scheme and money transfer fraud.

As per Brenner’s argument, most of the cybercrime we have seen so far is nothing more than the migration of real-world crimes into cyberspace (Brenner S. W., 2004, pp. 5,6). For example, fraud, theft, extortion constitute a significant proportion of cybercrime, traditional crimes like these are considered cybercrimes when they are committed in non-traditional ways (Brenner S. , 2007, p. 383). This proliferation of targets and techniques has occurred against a background of increasing recognition that the state is limited in its capacity to control human behavior, and that security and prosperity in cyberspace will depend on the proper functioning of not just agencies of government but a constellation of institutions and conventions in civil society.

Human societies has always been bound by rules that govern conduct and over the years systems have been put in place to maintain order and ensure that violators of rules are identified, apprehended and punished. Like all other countries of the world, Botswana established its police in 1885. It was something new for the country to institute an independent agency staffed by full time, uniformed professionals whose sole task was to maintain order by reacting to crimes and apprehending perpetrators (UNODC, 2011, p. 5). Brenner (2004) argues that this described model became, and continues to be effective in controlling the types of crime societies have dealt with over the past several millennia (Brenner S. W., 2004). It is not, however, effective against cybercrime.

It is important to note that with little literature available in Botswana, the researcher draws from various international literature for application to the context of Botswana. Additionally, in assessing the challenges of investigating cyber scams, it will from time to time be referred to as cyber-crime in general since identified challenges cut across the phenomenon of cybercrime in general.

BOTSWANA's EXPERIENCE IN CYBER SCAMS

As Olayemi has pointed out, cyber scams/Fraud remains one of the most popular crimes in cyberspace (Olayemi, 2014, pp. 116-7). The Botswana Consumer Watchdog spokesperson, Richard Harriman also pointed out in the Gazette newspaper, that scores of Batswana are still getting their hard earned money siphoned by investment scams from all around the world. Mr E.J Batshu, Former Commissioner of the Police, (2006) remarks that Batswana are still continuously being hard hit by cyber scams and frauds. From his presentation to the National Conference on the Evaluation of Crime Prevention Programs in September 2006, the commissioner stated that many Batswana have been victims of scam which include;

- *Advance FEE Fraud (419 Nigerian Letters)*- requests are made by individuals claiming to be related to famous people, seeking assistance to move or invest money abroad, which requires the victim to advance payment for expenses such as administration fees. Victims are lured into the trap by promises of substantial profits (Chawki, 2009, p. 2).
- *Black Money*- victims are offered the possibility to obtain substantial sums of money if they provide the funds necessary to purchase chemicals to clean black money and make it legally tender (Arora, 2012, p. 146).
- *Use of Fraudulent Identity cards*- authentic identity cards obtained fraudulently as well as falsified documents are presented as identity to withdraw money from banks or swipe in stores. The use of false labour and immigration documents is also prevalent in Botswana. It also involves the illegal sale of Botswana passports to foreigners. Some perpetrators are aided by some unscrupulous employees in government.
- *Counterfeit Currency*- this involves forged bank notes that are circulated in the market through purchase of goods
- *Computer fraud*- perpetrators gain unauthorized access into financial institutions' computer systems and fraudulently transfer funds into different bank accounts in neighbouring counties (Kunz, 2004, p. 9).
- *Telecommunications fraud* - involves swindling cellular phone companies' huge sums of money by using the company's reconfigured stolen prepaid sim-cards to phone or send messages overseas (de Sousa, 2014, pp. 1,6).
- *Cheque fraud*- fraud syndicates collude with insiders at the targeted institutions to steal blank cheque leaves and thereafter they approach members of the business community for business deals (Levi, 1991, p. 25). Upon success, the syndicate would push for the proposed business deal(s) to fall apart and demand their funds to be returned to them in cash.

On the 21st November 2013, in the Gazette Newspaper, the Consumer Watchdog, Richard Harriman made a statement that scores of Batswana are still getting their hard earned money siphoned by investment scams from all around the world. Post 2008/9 recession, was a company by the name Stock Market Direct (SMD) which vanished from Botswana with P3 million of investment funds from multiple individuals. Then it was Eurex Trade which promised up to two per cent daily returns on online trading. It swindled individuals who had invested in the company and they lost millions of Pulas of their investment funds.

EFFECTS OF CYBER SCAMS

As Kshetri has argued, recent developments in information and communication technologies (ICTs) such as high speed broadband, mobile phones, social media and cloud computing have potential to spawn economic, social and political changes (Kshetri, 2013, pp. 3,7,9). Steven R. Chabinsky adds that "today's cyber criminals have evolved their practices to make their crimes more profitable. Regrettably, this works against the goal of promoting the good life and the life of bliss and happiness which has always constituted the grand vision of human existence (Yacobi, 2015, p. 82).

Cyber criminals sometimes gang together, choose specialties, master their skills, create networks of colleagues, and organize their crimes." (Chabinsky). These criminal activities can victimize individuals and organizations (Das, 2013, p. 147). They are motivated by self-interest and profit (Grabosky, 2000, p. 9). One estimate has placed the annual cost of cybercrime across the globe at a conservative estimate of $375 billion (Center for Strategic and International Studies, 2014, p. 3). In addition to the economic impact, cybercrimes can have public health and national security consequences, among others. Certainly, this works against the goal of development.

Internet users have become victims and targets of almost all types of cybercrimes. The most often cited figure for the annual worldwide loss to cybercrime is US$1trillion. In Botswana, statistics are unknown as there is no compilation of figures due to the problem of 'the dark figure of the crimes- meaning that most of the time it is unreported'. Two huge scams being Stock Market Direct (SMD) and Eurex Trade are the ones speculated to have vanished with millions of Pulas combined and some individuals have not yet recovered from it, perhaps due to the fact that there are no relief schemes for victims of such scams. However, the most important factor according to Brenner (2004) is that we simply do not have accurate cybercrime statistics because many cybercrimes go undetected and many go unreported and this also applies to the case of Botswana. Increasing digitization as per Moitlamo, the Botswana's National ICT Policy is likely to make Botswana more attractive targets hence the need for preparedness in tackling the rise of cyber frauds and crime in general.

CHALLENGES OF LAW ENFORCEMENT

Cyber scams as computer crimes are requiring law enforcement departments in general and criminal investigators in particular to tailor an increasing amount of their efforts toward successfully identifying, apprehending, and assisting in the successful prosecution of perpetrators (Hinduja, Computer Crime Investigations in the United States: Leveraging Knowledge from the Past to Address the Future, 2007, p. 2)

The Law

Molokomme (2012) notes that in Botswana, an attempt was made through the Cybercrime and Computer Related Crimes Act, to elevate certain so-called “traditional” crimes found in our Penal Code, such as extortion and fraud, to the cyber-domain. Hence the Act criminalises cyber extortion and cyber fraud at sections 14 and 15, respectively (Molokomme, 2012, p. 4). In 2006, the Botswana Cabinet approved the drafting of a cybercrime bill for Botswana and Botswana’s Cybercrime and Computer Related Crimes Act was passed by Parliament in 2007 (Molokomme, 2012, p. 2). This was a result of the realization that with the advent of emerging, sophisticated technology, there would invariably be those who would be only too willing to exploit such modern advances to further their own criminal pursuits (Molokomme, 2012, p. 3). There are also bits and pieces of cybercrime related laws such as in the Telecommunications Act, The Electronic Record Evidence Bill, The Criminal Procedure and Evidence Act. However, the law on cybercrime and computer related offences remain inadequate as there are still a lot of grey areas.

Number of Users

Currently more than 3.1 billion people worldwide use the Internet and it is likely that this number will increase continuously in the coming years (West, 2015, p. 1). Due to the international dimension of the network the number of possible offenders is significant. Even if only one per cent of the users made use of information technology to commit criminal offences the total number of offenders would be more 10 million. The number of users and Internet websites is related to the question how to identify web pages with illegal content within billions of web pages available in the Internet. This is only one example that shows how difficult it is for investigating authorities to fight cyber scammers (Finklea, 2015, p. 1).

Jurisdiction and Extradition Issues

Section 3 of the Cybercrime and Computer Related Crimes states that the courts of Botswana shall have jurisdiction: “where an act done or an omission made, constituting an offence under the Act, has been committed –

(a) in the territory of Botswana;

(b) by a national of Botswana outside the territory of Botswana, if the person’s conduct would also constitute an offence under the law of the country where the offence was committed, and if the person has not been prosecuted for the offence in that country;

(c) on a ship or aircraft registered in Botswana;

(d) in part in Botswana; or

(e) outside the territory of Botswana and where any result of the
offence has an effect in Botswana.”

The above section defines the jurisdiction of Botswana in crimes that affect its citizens and brings out extradition conditions and procedures of cyber criminals (Cole, 2008, pp. 17,18). The bill also holds accountable Botswana nationals for infringements committed not only in Botswana but outside the borders of Botswana (Botswana National Assembly, 2007). However, when it comes to cyber scams they are unbounded crimes; all the perpetrator needs is a computer to commit fraud on a grand scale. This means that perpetrators can commit thousands of crimes quickly with little effort to many. Law enforcement officers may not be able to determine who the perpetrators are or where they are. Even if they could identify them, gathering evidence and apprehending them can be difficult; 1) the country that hosts them may not regard what they did as illegal and may therefore decline to extradite them, or 2) they may be no extradition treaty in place that governs the conduct (Brenner S. , 2007, p. 422). Hence the issue of Botswana courts having jurisdiction is limited to countries having extradition treaties with them or regarding the act committed to be illegal. Gercke (2009) emphasize this by pointing out that the ability of national law enforcement agencies to investigate those crimes that have an international dimension is limited due to the principle of national sovereignty that restricts the authorization to carry out investigation in foreign territories (Gercke M. , 2011, p. 62).

International investigations therefore require co-operation of the law enforcement agencies based on the legal frameworks for international co-operation. The related formal requirements and time needed to collaborate with foreign law enforcement agencies often hinders international investigations, with regard to the fact that in most cases there is only a very short time gap available, in which successful investigations can take place, the application of the classic mutual legal assistance regimes turns out to add to difficulties in Cybercrime investigations as mutual legal assistance in general requires time consuming formal procedures. There are different legislative approaches to speed up the investigation (Gercke M. , 2012, p. 146). So, as Smith says, when it comes to cybercrimes in general, there are difficulties in handling crimes that stretch across multiple jurisdictions and cybercriminals are benefitting from inter-jurisdictional arbitrage (Smith, 2004, p. 2).

Lack of Expertise and the Need for Complex Forensic Resources

Akuta et al (2008) identified that one challenge of serious concern is the high levels of computer illiteracy or expertise among law enforcement officers (Akuta, 2011, p. 135). Most law enforcement officers never had the opportunity to use a computer, talk less of having computer lessons while in the Police Academy. This is partly due to the fact that, entry levels into police academy are very low. Entry levels into the lowest rank of the police academy in African countries are very low (Robin, 2009, p. 1). In some instances, to be qualified to get into the Police Academy at the lowest rank which is Police Constable, candidates are expected to have completed secondary school with at least a pass in three papers of the General Certificate of Education. The same applies to Botswana, where from my experience entry levels are a minimum of 30 points[3] from secondary school and the rank is that of a Special Constable, who will in future be taken to the Police College for training.

This is a challenge in that law enforcement departments have procedural requirements for evidence collection that should be followed, but certain subtleties endemic to computer crime must be noted. Brown points to the complexity associated with the lack of tangible evidence and an actual scene to be examined (Brown, 2015, pp. 60,67). yet Botswana law enforcement officers are trained to deal with traditional or real-world crimes. Real-world crimes are situated in a physical environment and have four characteristics: proximity, scale, physical constraints and patterns. The most fundamental characteristic is that the perpetrator and the victim are necessarily physically proximate to each other when the offence is committed. Patterns are created as it becomes possible to identify the general contours and incidence of a crime.

[3] This is according to the Botswana Police Service - http://www.gov.bw/en/Ministries--Authorities/Ministries/State-President/Botswana-Police-Service-/About-the-BPS/Botswana-Police-College/

These characters shape the crime control strategy outlined above where there is victim-offender proximity, consequent victimization then investigation, identification and apprehension by law enforcement (Brenner S. W., 2004, p. 6).

Now police agencies around the world are employing technicians who can assist responding officers or detectives in the proper preservation, collection, and processing of evidence, as well as with interpretation and presentation of the technological details of crime commission (NIJ, 2001, pp. 11-21). Botswana finds itself battling with a lot of challenges when it comes to the issue of expertise and forensic resources. Molokomme (2012) asserts that Botswana does not have sophisticated technology at its disposal, nor the requisite manpower and expertise to adequately deal with such criminal activities (Molokomme, 2012). Hence, the most serious challenge in Botswana is the lack of resources and the limited capacity available to train our police officers to investigate such, and Molokomme continue to contend that the Police Service already has its hands full with the investigation of so-call "traditional" crimes. At present, Botswana has a very small Police Information Technology Unit which faces the challenges mentioned above due to the lack of training and manpower.

The Uncertainty of Criminal Prosecution

Authentication is a predicate to the admissibility of any physical evidence. To blunt potential authentication challenges to data extracted from a forensic image, it is useful to have a procedure to verify that the data on the image is an exact match of the original media (Baggili, 2015, p. 6). Computer forensic specialists have developed a procedure that guarantees just that. This process uses "hash" algorithms, which verify that the acquired image is the exact copy of the original media (Roussev, 2009, p. 49). Now even if this was achieved by investigators, the problem I see in Botswana would be the presentation of evidence since our courts have not been upgraded to include screens and computers to allow for evidence to be presented electronically. Botswana is a common law country and as Quidri et al points out those common law countries are characterized by an oral and adversarial procedure (Quadri, 2015, p. 31). However, there exist several exceptions to the hearsay evidence rule, such as business records, the question is whether computer files and print outs are inadmissible hearsay evidence of fall under this exceptions (The Law Commission, 1994, p. 87). The Botswana Electronic Records (Evidence) Act of 2014 in Section 3 states that electronic evidence 'includes all electronic records produced for inspection of a court' and Section 5(1) states that "nothing in the rules of evidence shall apply to deny the admissibility of an electronic record in evidence on the sole ground that it is an electronic record" However, still on the section on subsection (4) command that "a person who seeks to admit electronic record in any legal proceeding as evidence has the burden of proving its authenticity by evidence capable of supporting a finding that the electronic record is that which he or she supports it to be." (BOCRA) In other words, the investigator has to meet the hearsay requirements to proof that the matter they assert is reliable, trustworthy and authentic in order to be introduced as evidence, hence this high standard that has been set for electronic evidence is always difficult to achieve since evidence may change during its examination, such as last accessible dates, the physical memory and registry keys (The Law Commission, 1994, p. 87).

Furthermore, once evidence associated with a computer crime is lawfully discovered, multiple safeguards should be instituted to preserve its continuity and integrity (Watney, 2009). Extreme attention must be given to the specifications on the search warrant so that all relevant items are properly and legally seized (Kerr, 2005). Moreover, it is paramount to protect physical and removable media because of their sensitive nature (NIJ, 2001, pp. 6,35). Another critical point is that suspects in a case should be restricted from the computing environment because of the possibility that digital evidence might be altered or deleted (Sa’di, 2015, pp. 154,160). At this point, the forensic analysis of computer hard drives has proven to be beneficial in building a case against a suspected criminal. This method of evidence acquisition, however, is technically complex and laborious (Aseef, 2005).

While the number of cyber scams is increasing, many law enforcement departments do not have the expertise to perform these techniques and must outsource their forensic analysis requirements to other agencies that do have skilled personnel (Brown, 2015, p. 60). In addition, efficient interaction between law enforcement agencies and the judiciary is necessary.

One example of the need for co-operation is the court order. In a number of countries certain investigations require a court order. An inefficient interaction between law enforcement and the courts can delay investigations and as a consequence decrease the changes to identify and prosecute the offender. Cybercrime investigations do very often require access to certain data that is not under control of the law enforcement agencies but in the possession of private businesses such as Internet Service Providers (ISP) (Callanan, 2008, p. 4). Without the assistance of Internet Service Providers investigations can be very time consuming. A legal framework and related procedures that enable efficient co-operation between law enforcement agencies and Internet Service Providers can significantly increase the abilities of the law enforcement agencies to carry out investigations as it is challenging to secure a good case without this cooperation (Gercke M. , 2011, p. 209).

So all the above mentioned factors contribute to an uncertainty of a criminal prosecution since they are many standards to be fulfilled and many obstacles to pass through yet with limited time and limited resources, hence law enforcement agencies become reluctant to pursue cases with such uncertainties’. This would mean that cyber criminals are free to continue their endeavours putting businesses and customers in jeopardy of financial losses.

Non-Reporting

The first reason is the fact that a number of cybercrime scams are based on the principle of multiple offences with a rather small profit each instead of single offences with a high profit. If the damage caused by a single cybercrime is below a certain amount the victims will after evaluating the time and energy required to report and offence and provide the necessary evidence with the chance that the offender is identified decide not to report the offence (Fafinski, 2010, p. 12). Perhaps the problem of non-reporting may be attributed to the newness of cybercrimes (Warner, 2011, p. 741) and cross-border nature of the crimes (Koops, 2014, p. 41), or due to law-enforcement systems that are characterized by the lack of law enforcement resources (Schjølberg, 2009, p. 17), scale of crimes, and a low-governmental priority; there is generally victims’ unwillingness to report their victimization (Home Office, 2013, p. 5). Conventional crimes have overburdened law-enforcement agencies that in giving less priority to cyber frauds victims and the general public may lose confidence and trust that they police are able to help them (Tushabe, 2007, p. 379). In addition, the reason for non-reporting maybe due to low levels of awareness among governments, businesses and consumers about cybercrimes and protection measures and a lack of effective Internet safety groups to educate users on cybercrimes (Tushabe, 2007, p. 380).

Furthermore, businesses are being hacked or victimized, but they won’t report it because they don’t want to undermine consumer confidence (Saini, 2012, p. 206).

That is why a bank will be willing to put $500 back into a customer’s account rather then tell 500,000 customers that their information may have been compromised (Thomson Reuters). Often we will know that a certain corporation’s databases have been compromised, but when we ask them about it, they won’t cooperate. They look at their bottom line and assume that no one will want to do business with a company with a track record of having their customers’ information compromised (Lemieux, 2016, pp. 116-7). While this approach makes the situation easier for the victim and it may make sense for the businesses, there are significant disadvantages. If the victim’s first phone call is to the bank and the bank quickly reimburses the victim, the victim may never even think to report the crime to the police. If the crimes are never reported, they are not investigated by law enforcement agencies or counted in crime statistics. And the perpetrators remain free to commit more crimes (Police Executive Research Forum, 2014, p. 11).

Traditional Crime Measurements Underemphasize Cybercrime

Brenner (2001) argues that we can use existing rules to prosecute the traditional types of cybercrime, and can adopt new, cyber-specific rules for emerging varieties of cybercrime (Brenner S. , 2007, p. 447). The problem lies with the enforcement strategy. Brenner continue to argue that, our current crime control model cannot deal effectively with cybercrime (Brenner S. , 2004, pp. 9,12). That’s because real-world crimes are situated in a physical environment and has four characteristics: proximity, scale, physical constraints and patterns (ibid, p.9). The most fundamental characteristic is that the perpetrator and the victim are necessarily physically proximate to each other when the offence is committed (ibid). The scale of real world crimes is therefore limited (ibid. 9-10). During the commission of the crime the perpetrator focuses his attention to consummating that crime hence is constrained to complete one and move onto another, for example, a thief cannot steal into two houses at the same time (ibid). Finally, patterns are created as it becomes possible to identify the general contours and incidence of a crime (NIJ, 2005, p. 4). These characters shape the crime control strategy outlined above where there is victim-offender proximity, consequent victimization then investigation, identification and apprehension by law enforcement (Brenner S. W., 2004, p. 12).

Brenner (2007) argues that since we cannot, as yet identify offender-offence patterns comparable to those for real-world crime, law enforcement may not allocate its resources to deal effectively with cybercrime (Brenner S. , 2004, p. 17). In Botswana, the police give priority to the most prevalent serious criminal incidents and records found at Botswana Police are that of; robbery, house break-ins, store break-ins, burglary, theft of motor vehicle, stock theft, murder, rape and defilement of persons under the age of 16 years. Clearly despite the prevalence and effects of cyber frauds to the economy, it shows that our law enforcement agency give priority to traditional crimes and measurements used for the official statistics of crime are that of traditional hence underemphasize cybercrime.

WHAT CAN BE DONE: A NEW CRIME-CONTROL STRATERGY

Following the discussion above, in order to protect Batswana, their businesses and potential investors we need a new crime-control strategy that involves harmonization of laws as Conventions on Cybercrime outlines (Marion, 2010, p. 703). There is need for the general population and users to have some awareness of cybercrime (Matengu, 2012, p. 21). There is also the need for law enforcement mechanisms that are strong (Reidenberg, 2003, pp. 215 -6), allocate resources needed and recruit, train and equip enough officers to make a reactive strategy a viable approach to cybercrime (Brenner S. W., 2005, p. 673), and prevention strategies such as educating and raising awareness, formation of civilian societies to assist in the fight and developing a cybercrime prevention law (McQuade, 2005) that establish duties and impose sanctions to deter risky behavior (Shavell, p. 19). Individual businesses too, must protect their interests by investing in cyber security (Sekgwathe, 2012, p. 130). But the security extends to governments as well (ibid.).

Akuta et al (2011) believe that, if the various stakeholders: law enforcement, legislators, anticrime commissions and researchers, come together and share a common knowledge, there will be a high probability that up to date laws and policies will be crafted by legislatures (Akuta, 2011, p. 131). The implementation process of these laws and policies will also receive some fine tuning based on findings from various researchers. In addition, student recruits into police academies should be selected from college graduates with degrees in IT, Criminal Justice, and IT related fields. Once all these are put together, it is evident that the rate of cybercrime perpetration will plummet.

IMPORTANCE OF CYBERSECURITY

The ability to effectively fight against cybercrime is an essential requirement for the creation on of a conducive and sustainable environment for citizens of the globe. Without creating the legal framework that enables law enforcement agencies to identify offenders and prosecute them, it is almost impossible to stop such cybercrime attacks. Despite the importance of technical protection measures in the prevention of cybercrime it is important to highlight, that especially in those cases, where such technology is not available, failed, or was circumvented the existence of a proper legal framework is of great importance for recreating and maintaining cyber-security (Akuta, 2011, p. 130). The importance of the ability to ensure that a legal framework for cybercrime investigation and prosecution exists is not limited to direct measures to identify and prosecute offenders. Creating and efficiently using such a legal framework can enhance the trust of individual users as well as businesses in the security of information technology (Akuta, 2011, p. 131). If users are losing trust in information technology, this can negatively influence the development of e-commerce in the affected countries. The existence of a sufficient legal framework for the fight against cybercrime can therefore be considered one essential requirement for e-commerce. The other dimension is to allow law enforcement agents such as INTERPOL to co-ordinate their activities and chase after fugitive criminals (Akuta, 2011, p. 133). In addition, there must be some eagerness to do forensic investigations once reports are received (Matengu, 2012, p. 23).

In conclusion, various stakeholders: law enforcement, legislators, anticrime agencies and universities and researchers, must come together and share a common knowledge, there will be a high probability that up to date laws and policies will be crafted by legislatures. The implementation process of these laws and policies will also receive some fine tuning based on findings from various researchers. However in order to create a sustainable environment for the good life, more needs to be done in the fields of consumer and citizen education, constant surveillance and the provision of funding for pre-emptive research ahead of the criminals. A lot of planning must be made on the security various types of data ranging from website and network security, card payments down to personal communications such as e-mails. Since, governments spend lots of moneys for ICT infrastructure, they have to maintain and protect that infrastructure for the benefit of their people.

REFERENCES:

Akuta, E. A.-M. (2011). Combating Cyber Crime in Sub-Sahara Africa; A Discourse on Law, Policy and Practice. *Journal of Research in Peace, Gender and Development*, 129-137.

Arora, R. (2012). Black money in India: Present Status and future Challenges. *International Journal of Science, Engineering and Technology Research (IJSETR)*, 145-153.

Aseef, N. a. (2005, Fall). *Cyber-Criminal Activity and Analysis.* Retrieved May 17, 2016, from https://courses.cs.washington.edu/courses/csep590/05au/.../team2-whitepaper.pdf

Baggili, I. a. (2015). Data Sources for Advancing Cyber Forensics: What the Social World Has to Offer. *Association for the Advancement of Artificial Intelligence Spring Symposium* (pp. 6-9). Washington: Association for the Advancement of Artificial Intelligence.

Bandyopadhyay, S. (2005, July). Knowledge-Based Economic Development: Mass Media and the Weightless Economy. *DARP 74*. London, United Kingdom: London School of Economics.

Bargh, J. A. (2004). The Internet and social Life. *Annual Review of Psychology*, 1-23.

BOCRA. (n.d.). *bocra.org.* Retrieved May 17, 2016, from Botswana Communications Regulatory Authority: http://www.bocra.org.bw/electronic-records-evidence-regulations

Brenner, S. (2004). Toward a Criminal Law for Cyberspace: Product Liability and other Issues. *Journal of Technology Law and Policy*, 1-112.

Brenner, S. (2007). At Light Speed: Attribution and Response to Cybercrime/Terrorism/Warfare. *Journal of Criminal Law and Criminology*, 378-475.

Brenner, S. W. (2004). Cybercrime Metrics: Old Wine, New Bottles? *Virginia Journal of Law & Technology* , 1-52.

Brenner, S. W. (2005). Distributed Security: Preventing Cybercrime, 23 J.Marshall J. Computer & Info. L. 659 (2005). *The John Marshall Journal of Information Technology & Privacy Law*, 659-710.

Broadhurst, R. a. (2014). Organizations and Cyber crime: An Analysis of the Nature of Groups engaged in Cyber Crime. *International Journal of Cyber Criminology*, 1-20.

Brown, C. S. (2015). Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice. *International Journal of Cyber Criminology*, 55-119.

Cader, H. A. (2008). The Evolution of the Knowledge Economy. *The Journal of Regional Analysis and Policy*, 117-129.

Callanan, C. a. (2008, March 17). Co-operation Between Service Providers and Law Enforcement Against Cybercrime – Towards Common Best-of-breed guidelines? . *Project on Cybercrime*. Strasbourg, France: Council of Europe.

Center for Strategic and International Studies. (2014). Net Losses: Estimating the Global Cost of Cybercrime. *Economic impact of cybercrime II*. Santa Clara, California, USA: McAfee.

Chabinsky, S. R. (n.d.). *Fbi.gov.* Retrieved May 16, 2016, from Federal Bureau for Investigations: https://www.fbi.gov/news/speeches/the-cyber-threat-whos-doing-what-to-whom

Chawki, M. (2009). Nigeria Tackles Advance Fee Fraud. *Journal of Information, Law & Technology*, 1-20.

Cole, K. C. (2008). *Cybersecurity in Africa: An Assessment.* Atlanta: Georgia Institute of Technology.

Das, S. a. (2013). Impact of Cyber Crime: issues and Challenges. *International Journal of Engineering Sciences & Emerging Technologies*, 142-153.

de Sousa, J. V. (2014, June 30). Telecommunication Fraud Detection Using Data Mining techniques. *Masters Dissertation*. Porto, Portugal: University of Porto Faculty of Engineering.

Fafinski, S. a. (2010, June). Mapping and Measuring Cybercrime. *OII Forum Discussion Paper No. 18*. Oxford, United Kingdom: University of Oxford.

Finklea, K. (2015). *Cybercrime: Conceptual Issues for Congress and U.S. Law Enforcement.* Washington: Congressional Research Service.

Gercke, M. (2011). *Understanding Cybercrime: A Guide for Developing Countries.* Geneva: ITU-D ICT Applications and Cybersecurity Division.

Gercke, M. (2012). *Understanding Cybercrime: Phenomena, Challenges and Legal Response.* Geneva: International Telecommunications Union.

Grabosky, P. (2000). Cyber Crime and Information Welfare. *Transnational Crime Conference* (pp. 2-19). Canberra: Australian Institute of Criminology.

Hilty, L. M. (2010). ICT and Sustainable Development. In J. Berleur, M. D. Hercheui, & L. M. Hilty., *What Kind of Information Society? Governance,Virtuality, Surveillance, Sustainability, Resilience* (pp. pp.227-235). IFIP Advances in Information and Communication Technology.

Hinduja, S. (2007). Computer Crime Investigations in the United States: Leveraging Knowledge from the Past to Address the Future. *International Journal of Cyber Criminology*, 1-26.

Hinduja, S. (2007). Computer Crime Investigations in the United States: Leveraging Knowledge from the Past to Address the Future . *International Journal of Cyber Criminology*, 1-26.

Holden, E. a. (2014). Sustainable development: Our Common Future Revisited. *Global Environmental Change*, 130–139.

Home Office. (2013). *Cyber Crime: A Review of the Evidence.* London: Home Office Research Report 75.

Hoscheid, M. M. (2014). Legal and Political Measures to Address Cybercrime. *UFRGS Model United Nations*, 445-477.

Huang, S.-Y. K. (2011). The Evolutional View of the Types of Identity Thefts and Online Frauds in the Era of the Internet. *Internet Journal of Criminology*, 1-21.

Kerr, o. S. (2005). Search Warrants in the Era of Digital Evidence. *Mississippi Law Journal* , 85-145.

Koops, B.-J. a. (2014, December). Cyberspace, the Cloud, and Cross-borderCriminal Investigation:The Limits and Possibilities of International Law. *WODC, Ministry of Security & Justice*. The hague, The Netherlands: Tilburg Institute for Law, Technology, and Society.

Kshetri, N. (2013). *Cybercrime and Cybersecurity in the Global South.* Hampshire: Palgrave MacMillan.

Kunz, M. a. (2004). *Computer Crime and Computer Fraud.* Washington: University of Maryland.

Lemieux, M. (2016). Cyber Crime, Governance and Liabilities in the Banking and Payment Industries. *Banking & Financial Review* , https://www.cede.fd.ulaval.ca/sites/.../lemieuxmarc.presentation_16_mars_2016.pdf.

Levi, M. P. (1991). The prevention of Cheque and Credit Card Fraud. *Crime Prevention Unit Papaer No. 26*. London, Great Britain: The Home Office Crime Prevention Unit.

Marion, N. E. (2010). The Council of Europe's Cyber Crime Treaty: An exercise in Symbolic Legislation. *International Journal of Cyber Criminology*, 699-712.

Matengu, S. (2012, December). Cybercrime Awareness and Reporting in the Public Sector in Botswana. *Masters' Dissertation*. Cape Town, Republic of South Africa: University of Cape Town.

McQuade, S. (2005). Technology-enabled Crime, Policing and Security. *Jounal of Technology Studies*, http://scholar.lib.vt.edu/ejournals/JOTS/v32/v32n1/mcquade.html.

Molokomme, A. L. (2012). The Botswana Experience with Cybercrime Legislation and other Measures. *Octopus Conference on Cooperation Against Cybercrime* (pp. 1-5). Strasbourg: Council of Europe.

NIJ. (2001, July). Electronic Crime Scene Investigation. *NIJ Guide*. Washington, USA: National Institute of Justice.

NIJ. (2005). *Mapping Crime: Understanding Hot Spots.* Washington: U.S. Department of Justice, Office of Justice Programs .

Nwabueze, A. a. (2011). Information and Communication Technology for Sustainable Development in Nigeria. *Library Philosophy and Practice*, 1-6.

Olayemi, O. J. (2014). A Socio-technological Analysis of Cybercrime and Cyber Security in Nigeria. *International Journal of Sociology and Anthropology*, 116-125.

Police Executive Research Forum. (2014). *The Role of Local Law Enforcement Agencies In Preventing and Investigating Cybercrime.* Washington: Police Executive Research Forum.

Quadri, K. M. (2015). Adquisitorial: The Mixing of Two Legal dquisitorial: The Mixing of Two Legal dquisitorial: The Mixing of Two Legal dquisitorial: The Mixing of Two Adquisitorial: The Mixing of Two Legal Systems. *International Journal of Humanities and Management Sciences*, 31-36.

Reidenberg, J. R. (2003). States and Internet Enforcement. *university of ottawa law & technology journal*, 213-230.

Robin, S. (2009, October 16). Addressing the Challenges of Law Enforcement in Africa. *Policy Brief*, pp. 1-4.

Roussev, V. (2009). Hashing and Data Fingerprinting in Digital Forensics. *Digital Forensics*, 49-55.

Sa'di, M. M. (2015). Authentication of Electronic Evidence in Cybercrime Cases Based on Malaysian Laws. *Pertanika Journal of Social Sciiences & Humanities*, 153-168.

Saini, H. a. (2012). Cyber-Crimes and their Impacts: A Review. *International Journal of Engineering Research and Applications (IJERA)*, 202-209.

Schatten, A. (n.d.). *publik.tuwien.ac.at.* Retrieved May 17, 2016, from publik.tuwien.ac.at: publik.tuwien.ac.at/files/PubDat_178981.pdf

Schjølberg, S. a.-H. (2009). *A Global Protocol on Cybersecurity and Cybercrime: An initiative for Peace and Security in Cyberspace.* Oslo: Cybercrimedata.

Sekgwathe, V. a. (2012). Cyber Forensics: Computer Security and Incident. *International Journal on New Computer Architectures and Their Applications (IJNCAA)*, 127-137.

Shavell, P. M. (n.d.). *law.harvard.edu.* Retrieved May 17, 2016, from www. law.harvard.edu: www.law.harvard.edu/programs/olin_center/papers/pdf/225.pdf

Singh, A. (n.d.). *ceeindia.org.* Retrieved May 18, 2016, from www.ceeindia.org: www.ceeindia.org/esf/download/paper28.pdf

Smith, R. G. (2004). *Trends & Issues in in Crime and Criminal Justice.* Canberra: Australian Institute of Criminology.

Souter, D. a. (2010). *ICTs, the Internet and Sustainable Development: Towards a new Paradigm.* Winnipeg: International Institute for Sustainable.

The Law Commission. (1994). Evidence Law: Documentary Evidence and Judiciary Notice. *Discussion Paper No. 22*. Wellington, New Zealand: The Law Commission.

Thomson Reuters. (n.d.). *Cyber Crime - The Fastest Moving Menace.* Retrieved May 17, 2016, from accelus.thomsonreuters.com: https://risk.thomsonreuters.com/sites/default/files/GRC01950.pdf

Tushabe, F. a. (2007). Cyber Crime in Uganda: Myth or Reality? *International Scholarly and Scientific Research & Innovation*, 377-381.

UNODC. (2011). *Handbook on Police accountability,.* Vienna: United Nations Office of Drugs and Crime.

Warner, J. (2011). Understanding Cyber-Crime in Ghana: A View from Below. *International Journal of Cyber Criminology*, 736-749.

Watney, M. (2009). Admissibility of Electronic Evidence in Criminal Proceedings: An Outline of the South African Legal Position. *Journal of Information, Law & Technology*, <http://go.warwick.ac.uk/jilt/2009_1/watney>.

West, D. M. (2015). *Digital divide: Improving Internet Access in the Developing world Through Affordable Services and Diverse Content.* Brookins: Center for Technology.

World Commission on Environment. (1987). *Report of the World Commission on Environment and Development: Our Common Future.* Oslo: World Commission on Environment.

Yacobi, B. G. (2015). Life and the Pursuit of Happiness. *Journal of Philosophy of Life*, 82-90.

ABOUT THE AUTHORS:

Tarisayi Andrea Chimuka – (DPhil) - teaches Philosophy at the University of Botswana, Department of Theology and Religious Studies. Research interests: Philosophy of Culture, African Philosophy and Critical Thinking & Logic

Anitah Lesedi Mashumba-Paki – (Staff Development Fellow; studying towards MA): Department of Sociology at the University of Botswana. She has special interest in Criminology.