International Journal of Applied Information Systems (IJAIS) – ISSN : 2249-0868
Foundation of Computer Science FCS, New York, USA
Volume 2– No.2, May 2012 – www.ijais.org

E-Crime: an analytical study and Possible Ways to Combat

Mohammad Talib
Department of Computer Science
University of Botswana, BOTSWANA

Virginiah Sekgwathe
Directorate on Corruption and Economic Crime, Gaborone, BOTSWANA,

ABSTRACT
The internet is a powerful tool for development, paradoxically it is a double edged sword providing opportunities for governments, business industry etc to develop and operate reaching the international landscape at the same time equipping the greed motivated individuals with risk free opportunities of committing crime. Cyber crime, and cyber attacks or remotely controlled attacks affect our daily lives hence no government, public and private sector can afford to ignore. E-crime observably requires that the cyberspace be regulated in order to achieve independent, in depth analysis of the phenomena and of course accomplish cyber justice and deterrence. Lack of Internationally harmonized legislation, penalty, the knowledge and expertise of cyber criminals, the lagging behind of the law enforcement agencies, judiciary, legislators, prosecutors, academia etc, and of course victims' failure to report cyber crime incidents seriously inhibit the combat against this high tech crime.

Keywords e-crime, online security, e-evidence, ICT

1.0 INTRODUCTION
ICT has resulted in traditional business evolving to online or e-business business with a view to reach more populace irrespective of their geographical location. The internet accessibility everywhere, anytime and at affordable cost, and the mobile phones capabilities to connect to the internet has augmented the possibilities that the criminal elements of the society may also employ this technology, its features and capabilities to commit crime hence the rise in e-crime.

Conventional crime has gone high tech that it renders the capability of the law enforcement, judiciary, and prosecution under uncertainty. Crimes involving ICT systems are now commonplace and are beginning to threaten the integrity of the International prosperity and will seriously impact on the growth of e-business if not cured. The escalation in the use of digital cash and credit cards in the internet endow with a greater incentive to digital criminals. Presently this syndrome is being tackled but faced with several challenges since in a networked environment [4] cyber criminals can easily evade conviction by acting from a country where the demeanor is either not a contravention of any legislation or not prosecuted due to outdated cyber law or possibly no cyber law at all, or there is a high probability of unsuccessful prosecution [17]. Furthermore there are tools [1] available in the market but the same tools maybe used by the criminals [13] to cover their tracks in some instances rendering cyber forensics tools ineffectual.

1.1 E-CRIME
There is currently no definition agreed upon; however the Association of Chief Police Officer (ACPO) of England defines e-crime as the use of networked computers, telephony or Internet technology to commit or facilitate the commission of crime [15]. For the purpose of this paper e-crime maybe defined as conventional crimes aided, facilitated and/or directed towards the automated systems, and committed through the exploitation of the information and communication technology. These include the use of computers, computer networks or the Internet as a tool for performing criminal activities or as a target for a criminal activity. E-crime short for electronic crime may also be referred to as high tech crime, cybercrime, online crime, Internet crime, and also computer crime such as identity theft, E-commerce scams, services scams, financial fraud, piracy, personal data intrusion amongst
others.

2.0 PROBLEM DISCUSSION
In today's Information and Communication Technology epoch, computers have become not only pervasive but also invisible [16] in that they form part of our environment and we interact with them daily sometimes even unaware of that fact. The nature of cyber crime and the fact that unlike conventional crimes this type of crime is committed within the virtual place and the victims and perpetrators may not necessarily be in the same jurisdiction pose a real challenge. In addition the culture of the cyberspace as it is believed this virtual place must be a free zone where laws must not be applied. This has led to the sudden increase in cyber crime which ultimately brought overwhelming challenges to the law enforcement [19], prosecution and judiciary. There are several questions that need to be answered:

- How business organizations and government alike ensure that systems and digital assets remain protected in a changing business and technological environment?
- How does the International Business community streamline information security and risk management systems with governance and compliance requirements?
- What is the best defense in the enterprise network and what organizations are doing to protect sensitive data from both internal and external threats?

- How do the Financial Institutions and e-business protect against fraud in their respective business, online and mobile environment?
- How does international community address this syndrome effectively if there are no figures and where the figures are available does not capture all incidents to quantity the syndrome due to reluctance of organizations to report to relevant authorities?

3.0 ANALYSIS OF SYNDROME

This study found that not all countries have appropriate legal and regulatory frameworks to address this syndrome and its impact on the economy, national security and the populace. Furthermore there are no frameworks to address the general lack of cyber security awareness, evolving complexity of systems, increasing capacity and reach of ICT, an anonymity afforded by these technologies and the transnational nature of the communication networks. Cyber crime commands secure web sites, critical infrastructure and mandates that security must neither be an afterthought nor a problem left for ICT department to deal with rather government, business etc must consider security as part of the business planning, intelligence and strategy.

Traditional evidence in criminal cases has substance and shape and is tangible while e-evidence is latent hence making retrieval of such evidence burdensome. While cyber crime requires application of forensic techniques in data extraction for those investigating, prosecuting and those ultimately passing judgments in regard to disposition of offenders and the redress of offenders. The e-criminals are technologically advanced and the law enforcement have resorted to the aid of the forensic tools, though in most countries the academia, prosecution, judiciary and business have been left behind, consequently impeding on the success of this battle. On the other hand there is yet another challenge brought about by the e-criminals who always research current technologies and how they can use these technologies to make cash. This necessitates for the academia, prosecution, judiciary and business to fully understand the syndrome as needing partnership as such keep abreast with the cyber forensic tools, capabilities and limitations and of course research in ways to combat the syndrome.

The framework below (fig 1) depicts the characteristics of e-crime glimpsed through e-business as the study assumes that most of the vulnerabilities emanate from online business.

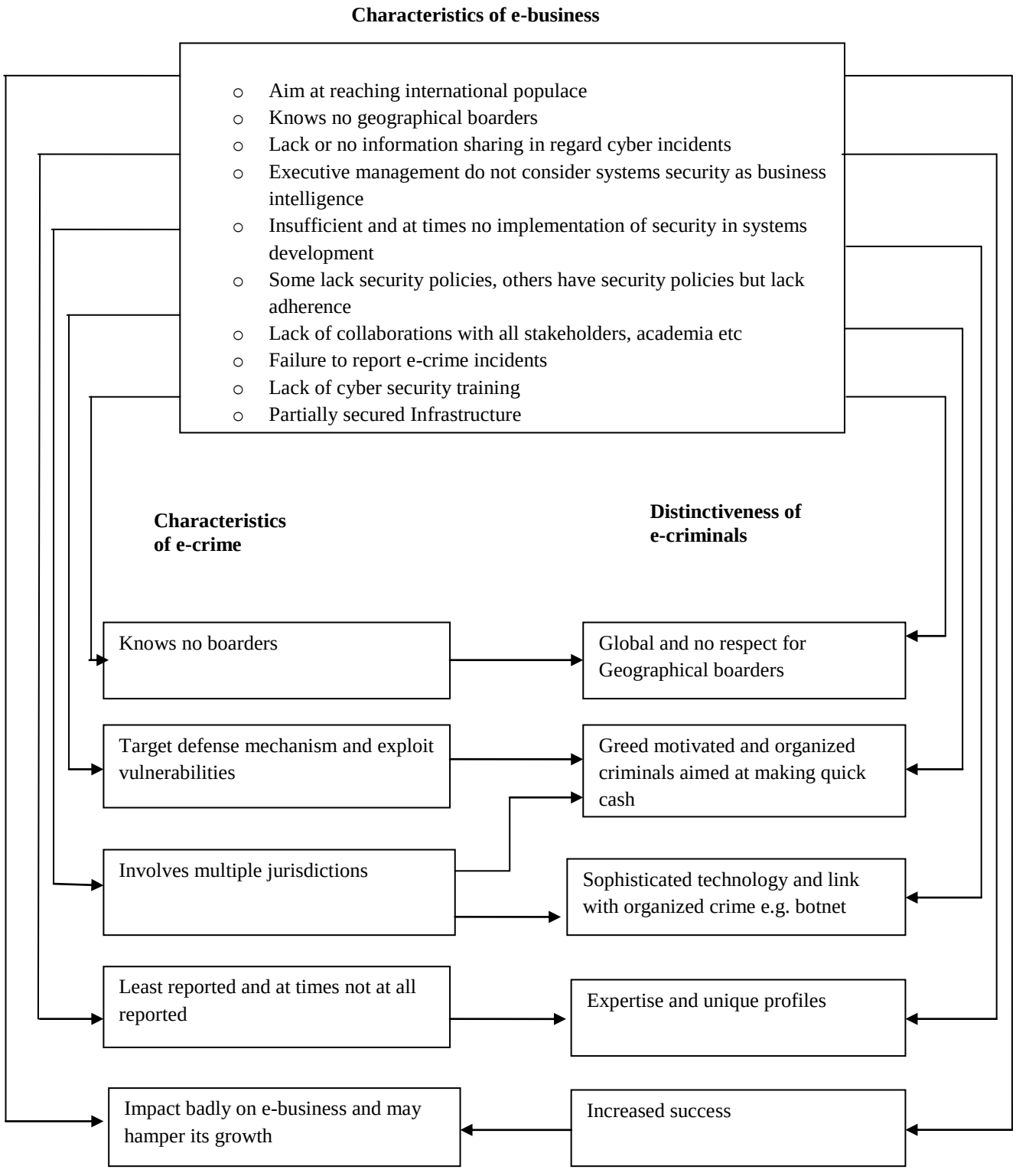

Fig 1: An Analysis of e-crime, e-criminals and e-business

4.0 IMPACT OF CYBER CRIME

The exact impact of cyber crime are often underestimated or unknown [2] hence the disastrous economic impact of these attacks are not well established. For instance the US Federal Deposit Insurance Corporation reported in cybercrime trend news that, businesses lost $120m in the third quarter of 2009 to phishing and Trojan-based online banking scams, and that small businesses lost $25m as part of these scams [5].

Cyber crime is categorically an economic crime for the purpose of this paper; hence the time has come for all countries to have compulsion to treat it as such, this phenomena prompted the United States Federal Bureau of Investigations (FBI) to make e-security or cyber security the third unit of its mission as noted by the Director Robert S Mueller that

> "*The globalization of crime-whether terrorism, international trafficking of drugs, contraband, and people, or cyber crime – absolutely requires us to integrate law enforcements efforts across the world. And that means having our agents working directly with their counterparts overseas…[14].*"

With potentially significant new developments in technology suggesting that techniques such as phase-change storage [11], holographic storage [10] and use of molecular memory becoming future methods for data storage [3], more research is required in this area.

The sophistication and impact of this high tech and global crime explode rapidly and continuously thus frustrating the very efforts of network security defenses, business systems, home and mobile internet access.

5.0 THE BOTSWANA SCENARIO

Botswana experienced recorded and reported incident of this syndrome in 2000, when a Bank of Botswana employee electronically transferred over P2million to an account outside the country from the Bank he was employed in. The circumstances surrounding the case were that November 9, 2000, the accused Pula 560 210 and later Pula 1 126 166, the money being the property of Bank of Botswana [20]. The accused siphoned money from the Bank of Botswana to South Africa via electronic transfer system. An Accountant General Officer received a query from the police about the two payments made to two South African companies namely; Pacific Gull Traders and SBF General Supplies. The payments of Rand 984 850 and Rand 1 979 800 were unprocedurally prepared in one day, though a single day in legitimate payments is devoted to preparing one journal. The case was concluded in the Magistrate court and the accused sentenced with the application of penal code law.

The country back then did not have any cyber crime or computer related legislation in place, hence the law enforcement officers were left with no alternative but to use the penal code [7] despite the fact that technology aided the accused to commit fraud. A magistrate's court in Gaborone, Botswana sentenced the offender to six years imprisonment on each of the two counts of stealing money which came into his possession by virtue of his employment [11], and sentences were to run concurrently, while two years of each sentence were suspended for three years on condition accused did not commit a similar offence. The accused appealed the sentence and the case was adjudicated by the High Court of Botswana [8]. Judge dismissed defense submission that his client had reasonable prospects of success on appeal. The defense argued that the accused exercised his constitutional right to remain silence and not to call any witnesses during his trial, thus leaving the state's claims unchallenged.

Botswana with an attempt to cure this syndrome formulated the law and an act known as Cyber Crime and Computer Related Crimes Act, 2007 No. 22 of 2007 [6] was passed, in order to discontinue the traditional use of the penal code of Botswana in addressing the high tech crimes. This piece of legislation [3] addresses most of the e-crimes but has not yet kept pace with the ever changing technology, as it does not include some of the contemporary e-crimes, for instance theft of a modem or dongle that is used to connect to the internet and provided to clients by most of the local service providers though not adequately secured by these Internet Service Providers (ISP) will obviously revert the local law enforcement to the traditional penal code, furthermore there is nowhere in this Act, no section whatsoever that criminalizes the cloning of Subscriber Identification Module (SIM).

6.0 RECOMMENDED FEASIBLE CURE

6.1 Integrating Security in Systems Design and Development

The most important point is to build security into the web application at the design stage itself, an assessment of employment of Intrusion Detection System, system audit etc. In fact, one of the key activities during the design phase should be a detailed risk assessment exercise whereby key information assets are identified and all possible vulnerabilities mitigated and addressed.

6.2 Mandatory Reporting Internationally

> *"When you can measure what you are speaking about, and express it in numbers, you know something about it; but when you cannot express it in numbers your knowledge is of meager and unsatisfactory kind; it may be the beginning of knowledge, but you have scarcely advanced to the stage of science"* **– Lord Kevin** [12].

The cure of this syndrome may not be found until and unless the statistics, nature and extent of the syndrome are well understood and documented. This therefore necessitate that there be an internationally amalgamated legislation obligating that all individuals, organizations including governments must report all forms of e-crime, and that failure to report constitute a stiff penalty on the concerned organization. Even so this must come with some form of protection against the victim (attacked organization, individuals etc) to guard against revealing vulnerabilities and inducing further attacks and of course credibility and loss of business.

6.3 Cyber Security Readiness

This will include formulation of a program to sensitize the populace on the benefits and dangers of the internet and how online users as this include children who are minors and needing supervision either online or otherwise. Training program relevant to each level of online users has been developed by developed countries whilst in developing countries this is either inadequate or utterly unavailable. In 2011, Norton reported that the top e-crime threat require the interaction of the internet user [9] includes, social media identity theft, smart phone and tablet hacking, trending topics, shortened web address and pharming. The success factors of a formal and interactive public cyber security training programs has been done by Albrechtsen [2], and their findings were that the success rate of this program is higher compared to other training mechanisms such as posters and presentations.

In addition the national and international priorities, guiding doctrine, directing criteria, functional arms has to exemplify harmony of views in what we may term public private partnership (PPP). Cyber security readiness may include use of international conferences devoted to discussion of the real nature and extent of this international problem, prevention and the substantive legislation. This type of conference as it is evident that some countries already established this may bring together experts in different fields hence the role of the academia, law enforcement, legal, judiciary, prosecution, telecommunications industry, internet service providers, designers and manufacturers of both the computer hardware and software may have joint efforts in preparing for the cyber security readiness.

6.4 Implementation of Analysis of Intrusions

The implementation by Governments and the International community at large irrespective of their business orientation and industry specialty of performing analysis which will be enhanced earlier detection of intrusion and response to such incidents, let alone reporting to relevant authorities including the law enforcement agencies. The model in fig 2 depicts intrusion detection and analysis which employs data mining in order to protect the integrity of systems and the critical infrastructure.

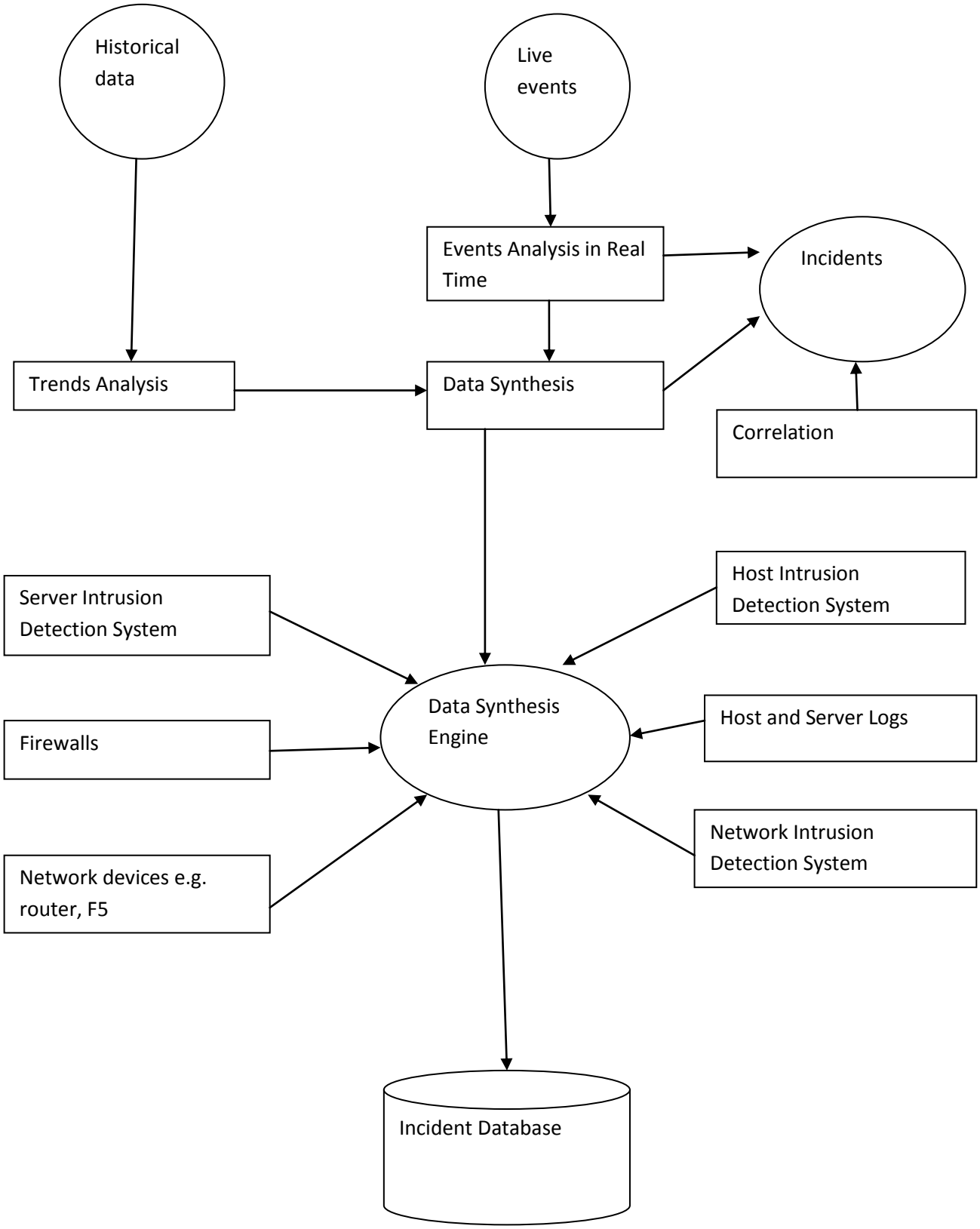

Fig 2: Proposed Intrusion Detection System and Intrusion Analysis model

6.5 Formulation of Security Policies and Monitored Adherence

In order to win the battle against curing the syndrome, organization need to understand the importance of policy formulation and monitored adherence, as a policy without proper implementation and adherence is the same as no policy at all.

6.6 Embed Security into Business Decision Making Process

The Executives throughout the world must ensure that cyber defense program that weaves preventative and detection measures including disaster recovery is implanted in the fabric of their daily operations and decision making.

6.7 Transfer Risk

Governments, financial institutions, e-business must assess risks and engage insurance policies to guard against loss, some insurance companies already has electronic crime risk or cyber risk policies.

6.8 Research and Development

Time has come for governments, industry, business and of course the academia to have joint efforts in researching on criminal behavior, monitoring and evaluation of implemented security systems, and coming up the best feasible solutions. This research will assist in addressing the challenges posed by the scale and volume of e-crime the technical complexity of identifying perpetrators and of course the understanding of the reality, nature and extent of the syndrome.

6.9 Cyber Security Education Internationally

This will assist in the prevention of e-crimes since online surfers will be well informed to make decision to surf the internet safely, also legitimate consumers will not become unwitting accomplices.

6.10 Impose Harmonized Stiffer Penalties

Forfeiture of all proceeds and suspected proceeds of crimes if instituted as part of the penalty since it removes unlawfully accumulated asserts from circulation at the same time stripping the offender of the status [18] thus tasting their own medicine. Young [18] further state that taking the instrumentalities of crime out of circulation, obtaining funds [21] for restitution, taking profit out of crime and achieving some measure of deterrence all constitute remedial aspects of forfeiture it cannot be denied that depriving a wrongdoer of the trappings of an expensive lifestyle or the items that gave him the influence, stature or resources to commit a criminal act in certain circumstances can serve as a form of punishment or retribution exacted by the criminal system.

7.0 CONCLUSION

Technology, legislation, secure infrastructure and cyber security awareness cannot afford the cyberspace security, encompassed with comprehensive understanding and willingness of online users to demonstrate knowledgeable and secure online behavior need be overemphasized, including the international cooperation of all concerned (academia, judiciary, law enforcement financial institutions etc). Protecting Cyber Space is an International concern and governments alike recognize the criticality to the economic and national security of protecting the infrastructure which ultimately translate into protection of the cyberspace conversely there are quite a few regulations of the cyber space. This calls for a forum to address laws in the International legislation for tracking cyber criminals outside the boarders, sharing of information and of course collaboration on incident response. If there is no deterrence, e-crime may continue to amplify thus hurting even the innocent children, the economy as online consumers will definitely lose confidence and trust in e-transactions and e-business, which is currently the backbone of International Business.

7. REFERENCES

[1] Amol Vyavhare, Cyber Forensic tools http://www.articleswave.com/computerarticles/top-cyber-forensic-tools.html last accessed on 02/11/2009

[2] Brian Stanford et. Al., Challenges and achievements in e-business and e-work, google books, 2002

[3] Bullis K (2007), Ultradense Molecular Memory, MIT Technology Review http://www.technologyreview.com/Nanotech/18100/ available from last accessed 10th March 2011

[4] Computer Forensics, Cybercrime and Steganography http://www.forensics.nl/links/ Accessed 02/11/2009

[5] Cyber crime losses almost doubled, available from http://www.theregister.co.uk/2010/03/15/cybercrime_complaint_surge/ last accessed on 30/02/2011

[6] Cyber Crimes and Computer related Crimes Act, of Botswana, 2007, available from http://www.itu.int/ITU-D/projects/ITU_EC_ACP/hipssa/Activities/SA/docs/SA-1_Legislations/Botswana/CYBERCRIMES.pdf last accessed 20/03/2012

[7] Fombard CM and Quansah EK, The Botswana Legal System, LexisNexis Interpak Books, Pietermaritzburg, 2008

[8] High Court throws out former BOB employee's bail bid, Botswana Daily News dated 9th June, 2003 available from last accessed 10th March 2012

[9] IOLScitech 2011, Top five cyber threats facing consumers, available from http://www.iol.coza/scitech/technology/security/top-five-cyberthreats-facing-consumers-1.1009335 last accessed on 22/04/2011

[10] Knight W, (2005), Holographic Memory Discs May Put DVDs to shame, NewScietist.com, available from http://www.newscientist.com/article.ns?id=dn8370 last accessed 10th March 2012

[11] Lai, S, Current status of the Phase Change Memory and its Future, available from http://www.intel.com/research/documents/Stefan-IEDM-1203-PAPER.PDF last accessed 12/03/2011

[12] Lecture on "Electrical Units of Measurement" (3 May 1883), published in *Popular Lectures* Vol. I, p. 73; quoted in *Encyclopaedia of Occupational Health and Safety* (1998) by Jeanne Mager Stellman, p. 1992 available from http://zapatopi.net/kevin/quotes/ and http://en.wikiquote.org/wiki/William_Thomson last accessed on 23/02/2011

[13] Marcella A and Doug Menendez, Cyber Forensics, A field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes, 2nd Edition, Library of Congress Cataloguing- in Publication Data, 2007

[14] Muller Robert, Statement to Senate Judiciary Committee, December 2, 2006, available from http://www.fbi.gov/congress/congress06/mueller200606.htm accessed on 30/03/2011

[15] Report on Progress of MP's e-strategy dated 25/01/2007, available from www.mpa.gov.uk/committees/mpa/2007/070125/10/, last accessed 05/03/2012

[16] Research Centre For Educational Technology (RCET), Ubiquitous Computing, available from http://www.rcet.org/ubicomp/what.htm, last accessed 02/02/2012

[17] Sekgwathe V. and Talib M, Cyber Forensics; Computer Security and Incident Response, available from http://www.sdiwc.net/digital-library/web-admin/upload-pdf/00000149.pdf last accessed 12/03/2012

[18] Simon Young, Civil Forfeiture of Criminal Property, Legal Measures for Targeting the Proceeds of Crime, Library of Congress Cataloguing- in Publication Data, 2009

[19] Stanley Brodsky, Expert Expert Witness, More Maxims and Guidelines for Testifying in Court, Library of Congress Cataloguing- in Publication Data, 2006

[20] Temane's over P1million case heard at the magistrate court, Botswana Daily News dated 19th February, 2002, available from http://www.dailynews.gov.bw/cgi-bin/news.cgi, last accessed 10th March 2011

[21] The World Bank Group, Financial Intelligence Units, An Overview, International Monetary Fund Publication Services, Library of Congress Cataloguing- in Publication Data, 2004

[22] United States Department of Justice, District of Oregon (1999). First Criminal Copyright Conviction Under "No Electronic Theft (NET) Act for Unlawful Distribution of Software on the Internet available from http://www.usdoj.gov/opa/pr/1999/August/371crm.htm last accessed 22/03/2011