Challenges of Using Information Technology To Combat Economic Crime

Monica N. Agu
Department of Computer Science
University of Nigeria
Nsukka, Nigeria.
monica.agu@unn.edu.ng

ABSTRACT

Information Technology is one of the most valuable asset for any organisation and any economic system. It is redefining the ways of conducting business and communication and is shaping the interaction between producers and consumers for sale and purchase of goods and services. Unfortunately, however in spite of the importance of IT to the economic system, information revolution has brought both negative and positive changes to business, international affairs and daily life. The growth of the internet for example has greatly influenced the way and speed with which information is shared by both the “good” and the “bad”. The revolution in IT and its attendant globalisation of the market have introduced more and new forms of opportunity for criminals. The paper discusses the concepts of and challenges posed by economic crimes and attempts to proffer measures for preventing and fighting economic crimes.

Keywords: Information Technology, Economic crime, Challenges, Prevention, Cybercrime.

1. INTRODUCTION

The importance of Information Technology (IT) in the growth and development of any economy is well documented in literature. Information Technology therefore, is one of the most valuable asset for any organisation and any economic system. It is redefining the ways of conducting business and communication and is shaping the interaction between producers and consumers for sale and purchase of goods and services. Internet and its global reach have created new opportunities. Its benefits can be measured in terms of enhanced processing speed, transmission rates and access time.

Unfortunately, however in spite of the importance of IT to the economic system, information revolution has brought both negative and positive changes to business, international affairs and daily life. The growth of the internet for example has greatly influenced the way and speed with which information is shared by both the “good” and the “bad”. The revolution in IT and its attendant globalisation of the market have introduced more and new forms of opportunity for criminals [7]. This paper attempts to discuss the challenges of combating economic crime through a revolution in IT.

The remaining part of the paper is organised as follows: in the next section we discussed the concept of economic crime. This is followed by a section that examines the challenges of combating economic crimes. The next section addresses the measures that can be used to prevent and fight economic crimes. The last section is the conclusion.

2. THE CONCEPT OF ECONOMIC CRIME

Economic Crime has been defined in various ways. It has been defined as an illegal act generally committed by deception or misrepresentation by someone who has special professional or technical skills for the purposes of personal or organizational financial gain or to gain an unfair advantage over another individual or entity [8]. Economic crime in [2] is generally referred to, as a crime committed by a person of a certain social status in the course of his occupation. In another definition, Economic crime is defined as “offences which cause or risk causing substantial loss” [5]. These crimes comprise a broad range of illegal activities and they occur as a deviation from the violator’s occupational role. Due to the rapid advances in technology new opportunities for these economic crimes have been provided.
It has been observed that economic crime has continued to grow rapidly because of the technological advances especially the rise of E-banking and the expansion of the internet. Examples of these crimes include corruption, corporate fraud, public fraud, tax evasion, goods smuggling, stock manipulation, currencies forgery, credit card fraud, environmental crime, money laundering, intellectual property infringement and the more recent phenomenon of cyber crimes.

In [2] people committing these crime steal large sums of money and employ technology and communications to carry out unlawful commercial transactions, disturb databases or orchestrate massive frauds. Victims of this are ignorant and naïve and most of the time are unaware of the fact that they have been cheated. He further argued that another characteristic of economic crimes is that they are often perceived as ‘good businesses and good business requires cutting corners. These crimes are, however, very costly for our society, and affect society as a whole. For instance, false advertising induces the public to invest in products that do not have the desired effect. In addition unsafe drugs, pesticides and food additives affect the health of thousands. The effects on society of economic crimes are hidden as public fear and concern are heightened in cases that affect personal security more directly. When Economic Crime becomes global, it does not just affect a selected group of financial institutions or regional areas; rather it affects international financial networks and economies at a national level.

Example: When billions of dollars are laundered in organized crime, this worsens national debt problems because the large sums of money are then lost as tax revenue to that country's government. Global Organized Crime can have a damaging effect on political structures, especially fragile democracies and developing economies. This is because people feel that the government is powerless and cannot stop organized crime, and so they turn to crime leaders for protection thereby making political institutions to begin to deteriorate.

The most prevalent form of economic crime is money laundering whereby criminal activities which generate illegal profits are deposited into the financial system. These include proceeds from tax crimes, fraud, and embezzlement; drug trafficking, bribery and corruption. This crime is prevalent in countries with weak regulations and control measures in the financial sector. Money laundering is a serious threat to the legal economy and affects the integrity of financial institutions. It also changes the economic power in certain sectors.

If left unchecked, it can corrupt society as a whole. Thus as result it damages the integrity of the financial institution, distorts financial markets and hampers foreign direct investment [1]. In developing countries money laundering hampers or slows down economic development. In a recent international survey, anti-money laundering experts identified tax crime as one of the top three sources of dirty money that criminals seek to hide in the financial system. Tax administrations can therefore play an important role in detecting and deterring money laundering, and at the same time tackle tax crimes. Criminals accumulate significant sums of money by committing crimes such as drug trafficking, human trafficking, theft, investment fraud, extortion, corruption, embezzlement and tax fraud.

In terms of credit card, fraud can be categorized in two forms-behavioural fraud and application fraud. Application fraud occurs when individuals obtain new credit cards using false personal information and spends as much within a such period of time, while behavioural fraud occurs when details of legitimate card have been fraudulently obtained and sales made on card holder not being present. For instance, e-commerce which requires only the card details.

Cybercrime is a growing threat in a world where most individuals and organisations rely upon the Internet and connected technologies, opening themselves up to the risk of attack from global criminals from anywhere in the world. Cybercrime is an economic crime committed using computers and the internet. It includes distributing viruses, illegally downloading files, phishing and pharming, and stealing personal information like bank details. [3] Whilst cybercrime isn’t that new for the Financial Sector (FS), it is a particularly prevalent issue for FS respondents in comparison to other industry sectors and one that puts its customers, brand and reputation at significant risk. FS organisations are expected to have appropriate systems and controls in place to fight the growing threat of cybercrime.
Table 1: showing major forms of economic crime in the listed countries [Source: [11]]

<table>
<thead>
<tr>
<th>Afghanistan</th>
<th>Mayanmar</th>
<th>Indonesia</th>
<th>Nepal</th>
<th>Zimbabwe</th>
<th>Japan</th>
<th>Pakistan</th>
</tr>
</thead>
<tbody>
<tr>
<td>money laundering</td>
<td>misuse of communication technologies</td>
<td>credit card fraud</td>
<td>Tax evasion</td>
<td>Fraud</td>
<td>Loan sharking</td>
<td>Embezzlement</td>
</tr>
<tr>
<td>Counterfeiting</td>
<td>embezzlement</td>
<td>Human trafficking</td>
<td>Forgery</td>
<td>Counterfeiting</td>
<td></td>
<td></td>
</tr>
<tr>
<td>human trafficking</td>
<td>illegal export and import</td>
<td>bank fraud</td>
<td>Money laundering</td>
<td>theft by conversion</td>
<td>Kickbacks</td>
<td></td>
</tr>
<tr>
<td>offences relating to the investment law</td>
<td>fraud of certificates of bill of lading.</td>
<td>violation of the prevention of the corruption act</td>
<td></td>
<td>banking investment frauds</td>
<td></td>
<td></td>
</tr>
<tr>
<td>offences relating to trade</td>
<td>smuggling</td>
<td>tax evasion</td>
<td>Tax evasion</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>bank frauds: get loan using bogus securities</td>
<td>tax evasion</td>
<td>smuggling</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>offences relating to foreign exchange</td>
<td>drug trafficking</td>
<td></td>
<td>telephone fraud</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>forgery</td>
<td>human trafficking</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>violation of copyrights</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

FS respondents from Afghanistan, Mayanmar, Indonesia, Nepal, Zimbabwe, Japan, and Pakistan reported cybercrime as the second most common type of economic crime “experienced by their organisations in the last 12 months”, after asset misappropriation (see Table 1). In these countries Cybercrime account for 38% of economic crime incidents for FS organisations, compared to 16% for other industries. This is not wholly surprising as the FS sector holds large volumes of the type of data cyber criminals are interested in and there is an established underground economy servicing the needs of the market for stolen and compromised data.

3. CHALLENGES OF COMBATING ECONOMIC CRIMES

3.1 Anonymity and Economic crime:
We have noted that the rapid growth of technology especially the seemingly limitless growth of the internet is changing the ways criminals operate. As a measure for detecting crimes and criminal advance, criminals also look for a means of remaining anonymous. Information technology itself enhances anonymity of economic crime perpetrators. The internet provides a hiding place for fraudsters who have simply migrated from the streets to an electronic platform [8]. Technologies such as e-mail, internet relay, chat rooms, newsgroup and online anonymizing services are often cited as providing criminals new ways to operate illicit enterprises.
As observed at the 2000 Annual Conference on Transitional crime, Corruption and Information Technology, criminal syndicates have started employing anonymizing e-mail services in the conduct of different types of criminal activities [10]. An example of this trend is the use of computers by Nigerian criminal groups to mass e-mail scan letters to persons around the globe- a variant of more traditional scam letter that once flowed from fax machines. [9] has argued that fraudsters who can pay for internet connection via fixed wireless lines can now perpetrate their evil acts within the comfort of their homes. The real challenge in combating these kinds of economic crimes is related to the fact that these crimes exist as long the internet exists.

3.2. Technology Enhance Economic Crime.
Apart from anonymizing effects of technology, it generally enhances the ability of criminals to engage in all sorts of organized crime to conduct their business. The pace of technology improvements is vast outstripping the abilities of the law enforcement to keep pace in terms of analysing how criminals might exploit the new technologies and how law enforcement might employ novel technologies in their investigations of these crimes. As the pace of technology improvement increases so is the popularity in its usage and services. With the growing number of people connected to the internet, for example, the number of targets and offender grow faster. As [6] opines it is difficult to estimate the number of people that use such technology(internet) for illegal activities and he argues that even if only 0.1 percent of users commit crime , the total number of offenders would be more than one million. It is also noted that the increasing number of internet users causes difficulties to the law enforcement agencies because it is relatively difficult to automate investigation process.

A very much related problem is that the criminals have found ways to employ technology to commit traditional forms of crime in enhanced or novel ways. For instance, a criminal can find detailed information on the internet that explains how to build a bomb using only chemicals available in a regular supermarket. Although information like this was available even before the internet was developed, it was however much more difficult to get access to that information. Another example is the piracy of the intellectual property that is plaguing the entertainment industry worldwide. Major criminal groups are funding themselves through global production, sale and distribution of copyrighted materials. To collaborate our argument [7] contend that economic crime is influenced by information revolution in two ways. First as a valuable and contained factor of production. Information itself is a direct or indirect crime committed by white collar criminals. Information according to them means profit and it can be a direct target. It represents the primary goal of an economic crime. Second, criminals need to adopt new instruments and new forms of organization in order to perform effectively.

3.3. International Dimension of Economic Crime.
Criminals and their targets are in many cases located in different countries. The digital revolution has dissolved physical boundaries of nations making those with inadequate cybercrime or internet related offences laws vulnerable to criminals that commit such crimes. Investigations of such crimes need the cooperation of law enforcement agencies in the affected countries. Unfortunately the cooperation of law enforcement agencies is not easy to come by because legal experts always disagree on matters relating to territorial jurisdiction for the investigation and trials of such criminals. Besides, the formal requirements and the time needed to collaborate with foreign law enforcement agencies often hinder investigations because investigations often occur in very short time frame. Data for tracing criminals are often deleted after only a short time [6]. In other words even when the country’s law enforcement agencies are prepared to cooperate it takes time to forge such co-operation.

4. PREVENTING AND FIGHTING ECONOMIC CRIME
As observed information technology and globalization enhance economic crimes. Consequently, fighting economic crime particularly with IT has become increasingly difficult. What can be done is preventing, controlling and managing economic crimes rather than eliminating economic crime altogether. The following measures can be employed to prevent and control and fight economic crimes.

4.1 Sound National Regulation and law Enforcement Agencies.
A key component of combating economic crime is effective regulations. Effective regulations act as a deterrent to intended criminal activities. Sound national regulations and enforcement agencies provide sound “investigative apparatus”. Effective investigative apparatus is also a significant preventive measure to serious economic crimes. Nations should establish appropriate and specialised agencies to tackle investigation of serious economic crimes. It is important to note that such specialised investigative agencies (like EFCC in Nigeria) must be “independent.” In fact the success of investigations of economic crimes depends largely on the independence of the investigative agencies. If, unfortunately, they are not independent, criminals will in most cases escape from the law enforcement agencies. Besides, a level playing field will not be there for everybody. Some with strong political and economic power will not be investigated when they commit economic crime. In other words, it is not only necessary to have sound national regulations; enforcement of such regulations plays a vital role in the prevention of economic crimes.
Sound law enforcement agencies give the regulations the needed teeth. [2] has rightly argued in favour of a high technology crime units in every country that respond to quick investigation and assist law enforcement agencies. The investigation of computer crime requires a team effort of police forensic scientists, lawyers and programmers or system administrators for effective and efficient prevention and management of economic crimes.

4.2 International Co-operation:
Since most serious economic crimes often involve transitional organized criminals and international transactions, international co-operation in the fight of these crimes is deemed one of the most important measures. All nations must be concerned about the seriousness of the problems and put united effort in their solution. A common global approach to deal with the problem could contribute to further strengthening international co-operation and law enforcement mechanisms. This would require standardization of legal definitions of economic crimes and expertise for investigating such crimes within law enforcement agencies. It is clear that national sovereignty does not permit investigations within the territory of different countries without the permission of the national authorities and legal experts always disagree on matters relating to territorial jurisdictions for the trial of economic crime offenders. Economic crime investigations need the support and involvement of authorities of all countries involved.

A suggestion has further been made for more effective action against IT economic criminal by international community and institutions [1]. The High Level Panel on Threats, Challenges and Change identified transitional organized crimes as a critical threat to the global community and has recommended that a comprehensive international convention on money laundering be negotiated. Although no international instrument deals specifically with the problem of economic and financial crime, both the United Nations Convention Against Transitional Organized Crime and the United Nations Convention Against Corruption include provisions of building an international framework to respond to such criminal activities [4].

4.4 Awareness.
Awareness can be a very important economic crimes prevention, control and detection measure. Increasing public awareness will play a very significant role especially in the case where regulations are not well enforced. Governments should have a clear concept, proper structure and process of enforcement for increasing public awareness. Educational systems have to be restructured to equip the youths and indeed the public to cope with the changing times in the economy in positive ways. Other ways of creating awareness is through workshops and seminars and through moral upbringing of young ones by homes and religious organizations.

5. CONCLUSION
The paper underscores the important of Information Technology to any nation and the world at large in terms of new ways of conducting business, transactions and communication. It however noted that these advantages of IT notwithstanding, it poses very serious problem to the society as well in terms of the growing rate of economic crimes associated with its development and enhanced by globalization.

In this paper an attempt is also made to discuss the concept and different forms of economic crimes. We discussed the anonymity of economic crime, international dimension of economic crimes and the role of IT in enhancing economic crimes and challenges. Finally we made effort to proffer measures for preventing and fighting economic crimes. These embrace sound national regulations and law enforcement agencies that are independent, international co-operation in terms of enforcement, investigating and prosecution of crime offenders, investing in protection measures as IT is developed and creating individual, private and national awareness.
REFERENCES


