Cybercrime in Zimbabwe and Globally

1. Background

1.1. **Cybercrime, also known as Computer crime,** is any crime that involves a computer and a network. Cybercrime covers any illegal behavior committed by means of, or in relation to, a computer system or network.

1.2. Cybercrime is a major component of the Anti Money Laundering and Counter Financing of Terrorism (AML/CFT) concerns. It is on the list of twenty-one prescribed predicate offences as listed by the Financial Action Task Force (FATF).

1.3. In Zimbabwe's National Risk Assessment (NRA) Report, of 2015, cybercrime is listed as one of the crimes contributing to the US$1,8 billion estimated illicit proceeds generated from criminal activity annually in Zimbabwe.

1.4. Cybercrime is an offence that is committed against individuals, organizations or even states, with the intention to harm the reputation of the victim, or cause physical or mental harm, financial or proprietary loss, to the victim, using modern telecommunication networks such as internet, mobile phones phone networks and electronic payment systems.

1.5. Criminals are turning to the internet to facilitate criminal activities and maximize profits in the shortest time.

1.6. Examples of cases of cybercrime include credit card fraud, phishing, hacking, identity theft, unauthorized access, telecommunication piracy, malware, electronic money laundering, tax evasion, etc.

2. History of Cybercrime

2.1. Computers and networks gained widespread use from the 1980s. Responsible hacking was then used to explore computer networks and improve their efficiency. At this stage, hacking did not pose any threat to economies or individuals, but over the years the sector was penetrated by criminals who used their knowledge and expertise to derive benefit by exploiting and victimizing others. This marked the beginning of cybercrime.

2.2. Criminals exploit the speed, convenience, and anonymity of the internet to commit a range of criminal activities that know no borders, either physical or virtual.

2.3. Unlike the common crimes such as robbery, theft etc, cybercrime is regarded as a borderless crime, which can be committed by one person who will not require being physically present at a location, but can be based in a remote location thereby evading law enforcement agencies.

2.4. The systems that made it easier for people to conduct e-commerce and online transactions are now being exploited by cyber criminals to defraud the users.

3. International Trends on Cybercrime

3.1. Cybercrime is a growing threat, the world over, as the growth of the internet has also resulted in the ballooning of crime. It is estimated that proceeds from cybercrime constitute 3-5% of the global GDP.

3.1.1 In the UK, the cost of cybercrime is estimated at **£27** billion per year, whilst global cybercrime is estimated at **US1 trillion** per year – and growing (Thomson Reuters Accelus).

3.1.2 Research has shown that 23% of British web users have fallen foul to a phishing scam and 1 in 5 individuals has been a victim of an email or website scam, with an associated cost of about **£3.1** billion.

3.1.3 Experts believe that this makes cybercrime the number one strategic crime threat to the UK, overtaking the illegal import of drugs and illegal immigration. Over 20,000 hacking attempts on the government infrastructure of the UK are detected each week. Of major concern are trojans, worms and hackers infiltrating IT systems and stealing money and information.

3.1.4 Fraud and the theft of intellectual property have become major phenomena throughout the world.

3.1.5 In the US, online industrial spying presents a growing threat, with tens of billions of trade secrets, technology and intellectual property being siphoned each year from the computer systems of US Government agencies, corporations and research institutions.

3.1.6 Incidents of hacking into governments and private corporations data-bases have also exposed the vulnerability of both public and private IT systems.

- The Wiki-leaks – Julian Assange, who hacked into the US government databases and released the information into the public domain, resulting in serious compromise of the US government’s foreign relations.

- A whistleblower – Edward Snowden, an American computer professional, and former CIA employee, leaked classified information from the US National Security Agency, in 2013. The information revealed numerous global surveillance programmes.

- Recently, massive hacking of over 4,000,000 US government employees' data by unknown hackers, took place and this confirms that cybercrime has escalated to a level of global threat.
- The recent hacking into the Canadian online dating website, Ashley Madison, exposed private details of 35 million users of the website, a few of whom have reportedly now committed suicide out of shame.

a) Many in Zimbabwe have encountered spam emails, phishing attempts and fake websites designed to defraud us. Cyber criminals are also able to track users' movements and passwords via malware and key-logger attempts, and even via USB sticks that may have been infected with viruses.

b) The funds generated through cybercrime are laundered through various channels that may include real estate, foreign and domestic investments.

3.2 Categories of Cybercrime

3.2.1 Cyber-crimes fall into three (3) broad categories, namely crimes against -

- Individuals and corporations;
- Property; and
- Government.

3.2.2 Each category can be exposed to a variety of criminal methods, varying from one criminal to the other.

- **Individuals:** This type of cybercrime can be in the form of cyber stalking, distribution of pornography, trafficking etc.

- **Property:** Examples abound where criminals –

  - steal a person's bank details which they use to steal money,
  - cloning of credit cards,
  - use malicious software to gain access to an organization's website and steal information or disrupt the systems of the organization.

In Zimbabwe, criminals have used the mobile money transfer platforms, tricking unsuspecting members of the public to make payments for non-existent services.

- **Government:** cybercrimes against a government are referred to as cyber-terrorism. Criminals hack into government websites, military websites with various motives, including stealing or destroying information or simply to embarrass the government. The perpetrators can be terrorist or individuals unfriendly to the Government of the day.

3.3 Types of Cybercrime

Although there are many examples of cyber crimes, a few relevant types are picked and discussed here.

3.3.1 **Card Fraud**

Card fraud is a major cybercrime that is experienced by many countries. Criminals steal or clone credit and debit cards issued by banks and use them to steal from bank customer bank accounts or making online purchases.

3.3.2 **Identity Theft**

Identity theft happens when fraudsters access enough information about someone's identity (name, date of birth, current and previous addresses) to commit fraud. Victims are either alive or deceased and through identify theft, victims lose money when criminals use their names to access bank loans, mortgages and credit cards.

3.3.3 **Fake lottery / inheritance**

These are advanced fee frauds, where victims are asked to make an advance payment for a favour or benefit to be derived from a transaction.

- These scams are common and a number of Zimbabweans have fallen victim with the authorities having received a number of such reports. For example, a victim is advised he/she has won a lottery or that his/ her account is due to be credited with a huge sum of money and is asked to make a small payment up-front to cover "administrative" or similar costs before disbursement.

3.3.4 **Electronic Money Laundering – Virtual Currency**

Electronic funds transfers have been used in concealing and moving proceeds of crime across jurisdictions. With the emergence and proliferation of various technologies of electronic commerce, criminals are using virtual currency to launder funds and evade tax.

Of interest is the use of **Bitcoins,** Webmoney, Paymer, and Perfect Money. Bitcoin is a new innovative payment network, which uses peer-to-peer technology to operate with no central authority or bank. It is a form of digital currency created and held electronically, through computer software which generates virtual value from a process called Bitcoin mining where people are tasked to solve complicated mathematical problems.

Proceeds from drugs, smuggling, money laundering are valued in Bitcoins which cannot be traced to its owner since it uses anonymous names and is independent of monetary authorities.

It has been reported that hackers are demanding Bitcoins as ransom for release of information that they would have hacked from governments and corporates.

3.3.5 **Electronic Vandalism, Terrorism And Extortion**

Criminals and terror groups are using telecommunications systems to vandalise, extort and terrorise societies and nations. A number of individuals and protest groups have hacked the official web pages of various governmental and commercial organisations and are vandalising databases.

In extortion cases, offenders obtained personal information and then use telephones or emails to demand bribes or payment for release of the information.

Cyber-terrorism, also known as e-terrorism is designed to cause advance terrorism and terrorist activities. Like conventional terrorism, it utilizes hacking to cause violence against persons or property, or at least cause enough harm to generate fear.

Currently the world has experienced e-terrorism through various terror groups operating in different parts of the world, whereby people are recruited through the internet.

3.3.6 **Sales and Investment Fraud**

As electronic commerce becomes more prevalent, the application of digital technology for fraudulent endeavours is on the increase.

The use of telephone for fraudulent sale of products, deceptive charitable solicitations, or bogus investment proposals and jobs is becoming increasingly common.

Cyberspace now abounds with a wide variety of investment opportunities, which are used by criminals to defraud the public.

3.3.7 **Salami Attacks**

These attacks are often used in committing financial crime and are based on the idea that an alteration, so insignificant, would go unnoticed in a single case. For example, a bank employee inserts a programme, into the bank's servers, that deducts a small amount of money (say 5 cents a month) from the account of every customer. Such unauthorized debit is likely to go unnoticed by an account holder, because of its small size, but the criminal is able to reap huge profit from aggregate deductions from all the accounts.

4 Zimbabwean Typologies

As a country, Zimbabwe has not been spared from cyber crimes. A number of Zimbabweans have fallen victim to cybercrime and this has resulted in financial loss.

Zimbabwean banks have also been cybercrime victims. According to the Zimbabwe Republic Police, the most common types of cybercrime in Zimbabwe is ***phishing***, which is the theft of information through email, credit card fraud, through cloning (duplicating) of cards, identity theft, unauthorized access and hacking.

Tabulated below is a summary of the different types of cybercrime that were experienced in the country, during the period 2011 to date;

	2011	**2012**	**2013**	**2014**	**2015**	**Total**
Phishing	8	4	3	5	0	**20**
Credit Card Fraud	4	2	0	2	5	**13**
Identity Theft	3	5	0	1	1	**10**
Unauthorised Access	10	9	2	1	2	**24**
Hacking	20	15	3	26	8	**72**
Telecommunications Piracy	0	0	0	0	1	**1**
Total	45	35	8	35	17	**140**

Below are some typology cases which took place in Zimbabwe.

4.1 Investment Fraud/ Discounting of Fake Paper

4.1.1 This scam is currently associated with foreign fraudsters who approach local businessmen and offer them fake discount instruments.

4.1.2 The fraudsters would prepare fake bank drafts, worth millions of dollars, which they offer to sell to local businesspeople at very generous discounts of 30%.

4.1.3 In the case of telegraphic transfers, the fraudsters would offer a joint venture investment with local partners. They would then prepare a fake telegraphic transfer confirmation which they will show to local partners as proof of investment. The local partner would be requested to inject their capital contribution in the new entity.

4.2 419 Scams

4.2.1 This scam has various forms, but in Zimbabwe it generally starts with the victim receiving a letter advising him/her of a huge cash award, which may be from a fake deceased estate or a fictitious lottery.

- The victim would be requested to submit personal particulars, including identity and banking details.
- The victim would then be requested to make a "small" payment for certain administrative costs to facilitate processing of the funds.
- The payment requests usually start as small figures, but additional requests are then made which balloon the prejudice to thousands of dollars.
- Zimbabweans of all ages and social standing have fallen victim to this scam.

- The authorities has received several complaints over this type of scam but no recovery has been made due to the complexity of the scam as well as lack of co-operation from foreign authorities.
- Most, but not all, cases involve jurisdictions in West Africa.

4.3 Abuse of Debit Cards to Externalize Business Proceeds from Zimbabwe

4.3.1 This method is mainly perpetrated by some foreigners who run businesses in Zimbabwe, to externalize their business proceeds to foreign countries. It has, however, emerged that locally-owned businesses are now also using this method to externalise business proceeds to foreign countries.

4.3.2 Business proceeds, mainly daily cash collections from retail outlets are deposited into personal bank accounts of company directors, managers and associates. These funds are then loaded onto Visa and Mastercards and withdrawn outside the country.

4.4 Abuse of Debit Cards to Move Proceeds of Gold Smuggling into the Country

- Trends have been noted whereby Zimbabweans resident in South Africa, are using debit cards linked to South African bank accounts, to move cash from South Africa into Zimbabwe.

- The individuals would obtain two debit cards, from their banks, a primary and secondary card.
- The primary card would be retained by one of the parties, in South Africa, whilst the secondary card would be kept by another party in Zimbabwe.
- The primary party would make large deposits, in South Africa, with the secondary withdrawing cash from Zimbabwean ATMs.
- The South African authorities are currently investigating a group of Zimbabweans who are involved in this scam.

4.5 Mobile Money Transfer Fraud

- This is probably the most common type of cybercrime in Zimbabwe, at the moment.
- Criminals use stolen or fake identity documents to register mobile telephone lines and register more mobile money transfer services such as Ecocash.
- They then flight newspaper adverts, usually for jobs, goods or services.
- In one case example, involving a job advert, the victims were given mobile telephone numbers to call for interviews.
- Interviews were done over the phone where candidates were told that had qualified for an oral interview. Candidates were told

that the said interviews would be done at the company head office, in Victoria Falls.

- The victims were told that the company runs a bus service and were instructed to send money for bus-fare to Victoria Falls. Those who sent in the bus-fare money, were further contacted and were induced to pay an additional amount, allegedly to bribe the selectors and beat the competition.
- The victim would only discover the fraud when they turn up at the appointed station, usually at the show grounds, where they will wait for hours before realizing they have been de-frauded.

5 Effects of Cybercrime

- ➢ The effects of cybercrime are far-reaching and these include: financial or property loss, theft of intellectual property, loss of customer confidence and trust and, in extreme cases, loss of lives.

- ➢ It also compromises national security in cases where national databases are hacked.

6 Control Measures

a) Adequate implementation of Anti Money Laundering requirements, especially the Know Your Customer (KYC) and Customer Due

Diligence (CDD) measures, will go a long way in addressing the threat of cybercrime in a country.

Institutions will be able to identify high risk individuals and entities that are using the internet or other network services to commit crime.

b) The country has a legal and regulatory framework, consistent with the international standards sets by the FATF, which sets out Anti Money Laundering standards that financial institutions and Designated Non-Financial Businesses and Professions must implement to mitigate the risk of money laundering, financing of terrorism and related predicate crimes.

c) Institutions can also have robust IT systems, which have access to world-class databases, and are able to monitor transactions generated from the internet. Also the use of keystroke dynamics, provides a potential solution to cybercrime. **Keystroke dynamics** or typing **dynamics** refers to the automated method of identifying or confirming the identity of an individual based on the manner and the rhythm of typing on a keyboard. This technology allows one to identify anyone using a keypad or a keyboard, within ten keystrokes. This can be applied to ATM devices, smart phones, tablets, laptops and computers. This will work as an extra level of identification when individuals log in to systems.

d) Training and awareness are important measures that should be undertaken in mitigating the risk of cybercrimes. Training of staff members of designated institutions is key in the fight against money laundering through cybercrime.

e) Key to the fight against cybercrime is national and international cooperation and information sharing across regulators and law enforcement agencies.

f) Setting up of specialized units for cybercrime**.** In many countries, high-tech crime, cyber-forensics units and specialized prosecution services have been created in recent years to deal with cybercrime.

g) All citizens, should be aware of the threats of cybercrime and must accordingly take precautions when using the internet and other networks that are vulnerable to attacks by cyber-criminals.

h) Listed below are some of the things that can be done to minimize the risk of becoming a cybercrime victim-

➢ Use strong passwords which are not easy to crack;

- Secure your computer through firewalls and use of anti-virus/malware software;
- Secure your mobile device – download applications from trusted sources only;
- Protect your identity;
- Avoid replying to emails that ask you to verify or confirm your personal information including passwords.

7 Global Cyber Threat: What other countries are doing

7.1 The USA National Security Agency data centre in Utah, has a USD2 billion development fund to help protect US interests, where it is able to monitor all data and any information that flows over the internet.

7.2 In the UK, the office for Cyber Security & Information Assurance (OCSIA) works across all sectors, including intelligence, defence and law enforcement, detecting internet crimes.

7.3 The UK and the USA have entered into an international cooperation agreement, designed to fight organised crime groups.