A comparative analysis of internet crimes and traditional crimes

Law, Crime

Cybercrimes refers to criminal activities that are sophisticated and done through the use computers and the internet (Brenner, 2010). Cybercrimes range from activities such as downloading music illegally from the internet to stealing money from online bank accounts. Cybercrimes are totally different from traditional crimes in a number of ways. The first difference is the complexity in which cybercrimes have emerged with and the need for urgent response that they pose to security agencies. Unlike traditional crimes, cybercrimes are applying sophisticated methods are not easily noticeable to the victims of these crimes. The most common form of cybercrime is identity theft where details of victims are stolen and used in various places to gain access to critical information.

Traditional crimes are easy for security agencies to investigate and control. This is because the level of skills that are employed when perpetrating these crimes is low as compared to what is applied when carrying out cybercrimes. Two most common techniques that those perpetrating cybercrimes are using include phishing and pharming. Cybercrimes also include a wide scope of criminal activities and they need much time before they can be understood clearly. Computers and the internet have made most activities in our lives easier but they have also caused so many problems that the rate of cybercrime is threatening our wellbeing. Traditional crime activities involved the perpetrators finding it difficult most of the times to plan and execute criminal activities (Engdahl, 2010). As a result of advancement in technology, criminal activities in the cyber world are planned and executed within a very short period of time. This indicates that cybercrimes involve

very easy connection to victims unlike in traditional crimes where communication and access to information has been greatly hindered.

Why hackers hack

There are a number of reasons why hackers hack in the process of committing cybercrimes. We are living in an age where access to information is very important and as result of this, sensitive information has been protected just to ensure that it does not get to a wrong group of people. Many of those people who hack can attribute that to their behavior to a number of factors. One major reason why most hackers do so is because normal rules have failed them and disobedience is the only option that they are left with (Poulsen, 2010). This is an expression of their dissatisfaction with rules and regulations that have been put in place and they therefore have to disobey them by illegally gain access to information that is not meant for them. Hacking cannot be defined in simple terms but rather complex ones whose understanding is based on the way the hacker has committed the crime.

The other reason why hackers hack is because they want to access information and use it for their benefit and gain. People tend to think that through hacking, sensitive information such as bank account statements and other forms of vital information will help them gain financial. Hacking of online bank accounts is one of the major problems that the world is facing today. Through hacking, criminals are able to access ATM passwords and other crucial information that always helps them to access funds in these accounts. The hope of many hackers is that they will be able to easily access

funds in these accounts connected to ATM cards. The purpose of hacking is therefore solely for personal gains in most cases and also to disobey or cause harm to those who have been targeted by the hacker. However, reasons for hacking continue to change as a result of change in the technological world and accessibility to information motivates the hacker depending on what he or she intends to achieve with the information.

Sentencing statutes for cybercrimes and hackers

They say that necessitate is the mother of invention and as a result of the increased rate of cybercrimes, statutes for sentencing those who have committed cybercrimes such as hacking have been legislated. The purpose of these legislations is to ensure that justice has been done for both victims and perpetrators of cybercrimes (Schell, 2004). The sentencing is also aimed at demonstrating the commitment that those who are serving in the criminal justice system have towards ensuring that cybercrimes have been combatted to the end. Those who have been convicted of cybercrimes and hacking are sentenced to a period of not less than two years in jail, a fine and a supervised life after their release from jail.

Despite all these being done, it can be argued out that statutes for sentencing those who have been found guilty of committing cybercrimes and hacking are not handle the situation. Special agents of the federal bureau of investigation are not doing much to ensure that they gather information on a timely manner. In addition to that, the process of gathering evidence against those who have been convicted of cybercrime and hacking. On major concern about the way the criminal justice system handles cases of

cybercrime is that they tend to be reactive instead of acting on intelligence information that they might have received before. The sentencing has also been described as one that is not that harsh enough to discourage other potential perpetrators of the crime from committing it again. There is need therefore to ensure laws have been enacted to ensure harsh penalties for those who are found guilty of having committed certain cybercrimes and hacking.

Identity theft

Identity theft under cybercrimes is a major problem that those trying to provide security in the cyber world are trying to deal with. Identity theft remains at the top of all cybercrimes that require much attention from the nation. This crime involves someone else pretending to be someone and then using that to gain information that is not meant to be his. In such situations, the main motive behind this is normally to hurt the victim of the identity that has been stolen. The implication that this might have on the victim is far reaching and cannot be ignored by any law enforcement agency. Whenever a criminal fraudulently presents himself or herself, the effect of this might be that the person whose identity has been stolen may end up facing charges that are wholly not necessarily his (Woll, 2007). This is to mean that the implications of identity theft are that harsh and security agencies need to step in detecting and preventing these forms of crime.

Fight against cybercrimes and hackers

Law enforcement agencies in the United States have been trying to ensure that they act swiftly to prevent activities of hackers and other cybercrimes.

The Central Intelligence Agency (CIA) is a body that is deemed with the task of carrying out investigation and handing over the intelligence report to the police concerning cybercrimes and hacking activities. This is aimed at mitigating activities that facilitate these crimes. The Federal Bureau of Investigation (FBI) has a branch under it that investigates cybercrime activities and then presents evidence to the team that moves for the necessary action. The criminal justice system is another arm that has the responsibility of ensuring that matters of hacking and cybercrimes are put under control by sentencing those who have been found guilty. Heavy fines are also imposed on those who found guilty so as to act as a lesson to others.