# Cyber crime and targets

Law, Crime

The internet has put the world literally at anyone’s fingertips with a vast quantity of information is a mouse-click away. Information that was once only available in obscure reference libraries or card catalogs can be accessed by everyone. Unfortunately the internet is an equal opportunity tool, and those with virtuous as well as nefarious intentions can use this open resource to further their efforts to levels heretofore unheard of. The internet is also soapbox for free speech that epitomizes the intentions of the founding fathers to allow everyone the same opportunity to have their opinions aired.

There is a line that often blurs between legitimate and illegal behavior, when does harsh criticism becomebullying, when does an expression of affection become harassment and how do the authorities differentiate between someone looking up an old classmate for rekindle afriendshipand stalking a former girlfriend that spurned their overtures. The constitutional protections of free speech and requirements of specificity of regulations make the criminalization of inappropriate behavior.

CAUSES OF CYBER – CRIME

There are many reasons why cyber-criminals commit cyber-crime, chief among them are these three listed below:

Cyber-crimes can be committed for the sake of recognition. This is basically committed by youngsters who want to be noticed and feel among the group of the big and tough guys in the society. They do not mean to hurt anyone in particular; they fall into the category of the Idealists; who just want to be in spotlight. Another cause of cyber-crime is to make quick

money. This group is greed motivated and iscareercriminals, who tamper with data on the net or system especially, e-commerce, e-banking data information with the sole aim of committing fraud and swindling money off unsuspecting customers.

Thirdly, cyber-crime can be committed to fight a cause one thinks he believes in; to cause threat and most often damages that affect the recipients adversely. This is the most dangerous of all the causes of cyber-crime. Those involve believe that they are fighting a just cause and so do not mind who or what they destroy in their quest to get theirgoalsachieved. These are the cyber-terrorists.

HOW TO ERADICATE CYBER – CRIME

Research has shown that no law can be put in place to effectively eradicate the scourge of cyber-crime. Attempts have been made locally and internationally, but these laws still have shot-comings. What constitutes a crime in a country may not in another, so this has always made it easy for cyber criminals to go free after being caught.

These challenges notwithstanding, governments should in the case of the idealists, fight them througheducationnot law. It has been proven that they help big companies and government see security holes which career criminals or even cyber-terrorist could use to attack them in future. Most often, companies engage them as consultants to help them build solid security for their systems and data.

“ The Idealists often help the society: through their highly mediatised and individually harmless actions, they help important organizations to discover

their high-tech security holes....”# The enforcement of law on them can only trigger trouble, because they would not stop but would want to defy the law. “ Moreover, if the goal of the cyber-crime legislation is to eradicate cyber-crime, it mint well eradicate instead a whole newculture, in education is a much better way to prevent their actions.

Another means of eradicating cyber-crime is to harmonize international cooperation and law, this goes for the greed motivated and cyber-terrorists. They can not be fought by education, because they are already established criminals, so they can not behave. The only appropriate way to fight them is by enacting new laws, harmonize international legislations and encourage coordination and cooperation between national law enforcement agencies.

WHO ARE INVOLVED:

Those involved in committing cyber-crimes are in three categories and they are: THE IDEALISTS (Teenager). They are usually not highly trained or skilful, but youngsters between the ages of 13 – 26 who seek social recognition. They want to be in the spotlight of the media. Their actions are globally damageable but individually negligible. “ Like denying a lot of important e-commerce servers in February, 2000 is said to have caused high damages to these companies.”# Most often they attack systems with viruses they created; their actual harm to each individual is relatively negligible. By the age of 26 to 26 when they have matured and understood the weight of their actions, they lose interest and stop.

THE GREED – MOTIVATED (Career Criminals).

This type of cyber-criminals is dangerous because they are usually unscrupulous and are ready to commit any type of crime, as long as it brings money to them. “ They started the child pornography often called cyber-pornography which englobes legal and illegal pornography on the internet.”# They are usually very smart and organized and they know how to escape the law enforcement agencies. These cyber-criminals are committing grievous crimes and damages and their unscrupulousness, particularly in child-pornography and cyber-gambling is a serious threat to the society.

Example to show how serious a threat they pose to the society is “ the victim of the European bank of Antigua are said to have lost more than $10million”# “…theft of valuable trade secrets: the source code of the popular micro-soft windows exploration system by a Russian based hacker could be extremely dangerous… the hackers could use the code to break all firewalls and penetrated remotely every computer equipped with windows were confirmed. Another usage could be the selling of the code to competitors.”#

THE CYBER – TERRORISTS. They are the newest and most dangerous group. Their primary motive is not just money but also a specific cause they defend. They usually engage in sending threat mails, destroying data stored in mainly government information systems just to score their point. The threat of cyber-terrorismcan be compared to those of nuclear, bacteriological or chemical weapon threats. This disheartening issue is that they have no state frontiers; can operate from any where in the world, and this makes it difficult for them to get caught. The most wanted cyber-terrorist is Osama Bin Laden who is said to “ use steganography to hide secret messages within pictures,

example, a picture of Aishwarya Rai hosted on the website could contain a hidden message to blow up a building.”# A surprising fact is that these hidden messages do not alter the shape, size or look of the original pictures in any way.

HOW TO DETECT A CRIMINAL MAIL

A criminal mail is usually sent to networks with the aim of either corrupting the system or committing fraud. The way to detect such mails is by putting security measures in place which would detect criminal patterns in the network. News Story by Paul Roberts, of IDG News Service says that Unisys Suite has a system called the “ Unisys Active Risk Monitoring System (ARMS) which helps banks and other organizations spot patterns of seemingly unrelated events that add up to criminal activity.”#

ActimizeTechnologyLtd based in New York has developed technology that enables organizations to do complex data mining and analysis on stored information and transaction data without needing to copy it to a separate data warehouse. “ The actimize software runs on the Microsoft Corp. Windows NT or Windows 2002 platform and can be developed on standard server hardware with either four to eight processors, Katz said.”#

Eric J. Sinrod in his article ‘ What’s Up With Government Data Mining’ states that the United States “ Federal Government has been using data mining techniques for various purposes, from attempting to improve service to trying to detect terrorists patterns and activities.”# The most effective way to detect criminal mails is to provide security gadgets, educate employees

on how to use them, and to be at alert for such mails, above all, making sure no security holes is left unattended to.

CONCLUSION

It has been deduced from this study that reliance on terrestrial laws is still an untested approach despite progress being made in many countries, they still rely on standard terrestrial laws to prosecute cyber-crimes and these laws are archaic statutes that have been in existence before the coming of the cyberspace. Also weak penalties limit deterrence: countries with updated criminal statutes still have weak penalties on the criminal statutes; this cannot deter criminals from committing crimes that have large-scale economic and social effect on the society.

Also a global patchwork of laws creates little certainty; little consensus exist among countries regarding which crimes need to be legislated against. Self-protection remains the first line of defense and a model approach is needed by most countries; especially those in the developing world looking for a model to follow. They recognize the importance of outlawing malicious computer-related acts in a timely manner or in order to promote a secureenvironmentfor e-commerce.

Cyber-crime with its complexities has proven difficult to combat due to its nature. Extending the rule of law into the cyberspace is a critical step towards creating a trustworthy environment for people and businesses. Since the provision of such laws to effectively deter cyber-crime is still a work in progress, it becomes necessary for individuals and corporate bodies to fashion out ways of providing security for their systems and data.

To provide this self-protection, organizations should focus on implementing cyber-security plans addressing people, process and technology issues, more resources should be put in to educate employees of organizations on security practices, “ develop thorough plans for handling sensitive data, records and transactions and incorporate robust security technology- -such as firewalls, anti-virus software, intrusion detection tools and authentication services.

By way recommendations, these kinds of actions are suggested following the weak nature of global legal protection against cyber-crime:

•Firms should secure their network information. When organization provides security for their networks, it becomes possible to enforce property rights laws and punishment for whoever interferes with their property.

•Laws should apply to cyber-crime—National governments still are the major authority who can regulate criminal behavior in most places in the world. So a conscious effort by government to put laws in place to tackle cyber-crimes would be quite necessary.

•There should be a symbiotic relationship between the firms, government and civil society to strengthen legal frameworks for cyber-security. An act has to be crime in each jurisdiction before it can be prosecuted across a border. Nation must define cyber-crimes in similar manner, to enable them pass legislation that would fight cyber-crimes locally and internationally.