Center for Global & Strategic Studies

Preventing Cybercrime: A Criminological Perspective

By

Masud Ahmed Malik

Published: 3rd March, 2018

Center for Global &

Strategic Studies, Islamabad

1-E, 3rd Floor, Ali Plaza, Jinnah Avenue, Islamabad, Pakistan

Tel: +92-51-8319682

Email: info@cgss.com.pk

Web: www.cgss.com.pk

The Author:

Masud Ahmed Malik MSc Criminal Justice Studies (UK) is an Adjunct Faculty, Department of Sociology, Pir Mehr Ali Shah Arid Agriculture University, Rawalpindi, Pakistan & Member Advisory Board, Center for Global & Strategic Studies, Islamabad and a certified Criminal Profiler.

Table of Contents:

Summary

In this paper, effort will be made to explore the applicability of ideas drawn from situational crime prevention theory to cybercrime. The theory of situational crime prevention is based on the principle that crime can be reduced, if not altogether prevented, by altering various dimensions of the opportunity structures that are available to potential offenders. An attempt will be made to establish that the situational crime prevention theory offers a new and potentially effective approach to cybercrime control.

In recent times, Criminal opportunities are recognized as an important cause of almost all types of crimes. Criminologists believes that crime results when a potential offender perceives a situation as a criminal opportunity and decides to take advantage of it. This development leads to both theoretical and practical benefits. Theoretically, it has led to a greater understanding of how and why crime rates vary over time and over geographical areas. These variations often appear to be driven more by differences in criminal opportunities rather than by differences in the supply of potential offenders or their motivations. In addition, the focus on criminal opportunities has helped to recognize why particular crimes recur repeatedly in particular places at particular times. In this paper, it will be explored that how situational crime prevention might be applied to cybercrime.

The paper will begin by attempting to identify some distinctive motivations, characteristics and types of cybercrimes. There would be a due discussion by describing the origins, assumptions, and basic tenets of the situational crime prevention approach. Next, the attempt to illustrate how the situational approach can be applied to cybercrimes. The paper would conclude with a general discussion of current methods used to control cybercrime and the benefit of using the situational approach as a framework for choosing among crime control techniques.

Abstract

Digital technology has a unique characteristic that has enabled the world to deal and store immense amounts of information into a compressed or small storage devices which can be easily preserved and transported within no time. This preservation, communication or transportation of information either through physical or virtual medium within a cyber space has become vulnerable at the hands of criminals as they exploit this network which has an international scope. Cybercrime is not only on the rise but has developed a fear within the consumer of cyber space and among its growing users. Theoretically cybercrime prevention is a new phenomenon for researchers. Although large amounts of research work has been done, there is still room for much more research to take place. Modern inventions and upgradation of systems are inviting or leading towards technical crime. The problem is growing as the new techniques for committing cybercrimes are developed. These developments take place at enormous pace and the existing preventive and investigative methods/models/techniques to tackle cybercrime are not fully tested or developed and yet become obsolete. A situational crime prevention approach may resolve the problem if implemented in combination with other crime prevention techniques. Keywords: Digital Technology, Cyber Space, Cybercrime, Situational Crime Prevention.

Introduction

Crime is seen as an omnipresent temptation to which all humankind is vulnerable and so the prevention of crime is like a beast to tame. Crime is an act perpetrated by criminals against the law-abiding majority of the population and crime prevention is an understood purpose of any deliberate strategy of crime control pursued by state or private agencies. Thus, crime prevention has become a part of an overall strategy of governance. Reith (1956) points out that the prevention of crime has been "the principal object" of the police, while the codification of the criminal law in the nineteenth century, the rationalization of penal policy around the central institution of the prison; and eventual extension of penal discourses and practices into the community in the early twentieth century have all been similarly justified in the name of crime prevention.

The latest of the crime on the forefront has unique properties as it has appeared in a space that is universally shared across the globe commonly known as cyber space and the crime itself is defined as cybercrime. Cybercrime is an evil originating from the growing dependence on computers in modern life. In today's modern day era everything from microwave ovens and refrigerators to nuclear power plants is being run on computers, cybercrime has assumed rather threatening implications. Major Cybercrimes in the recent past include the Citibank[1] rip off in 1994, when a

[1] https://ctovision.com/the-first-great-cyber-crime-1994-attack-against-citibank/

Russian Hacker group led by Vladimir Leonidovitch Leven fraudulently transferred US $ 10 million into a bank account in Switzerland. The group compromised the bank's security systems. In 1994, the Control of Hydro-Electric System of Salt River Water project computers to gain control of water levels, in 1997 the airport disruption at Massachusetts, in 2000 hackers succeeded in gaining control of Gazprom gas pipeline Russia, in January 2003 the safety monitoring system of Ohio's Davis-Besse nuclear power plant was offline for five hours due to the Slammer Worm. While in 2005, CardSystem Secure Server was hacked affecting VISA, Master Card, Amex and Discover and their customers. In 2012, the South Carolina Department of Revenue was hacked and data from 3.8 million tax fillers was removed. South Carolina has spent over $12 million in response and remedy costs to this data breach.

The advancement in Information Technology has transformed the world into a reality called 'Global Village'. Especially, in the past ten years the role of information technology has increased many folds. The 51.8% of the world population is connected to each other through internet as the past decade has seen 996.1% growth in the use of internet across the world. Until, 31 December 2017, there were 3,956,880,532 internet users in the world[2]. This enormous growth has posed a threat of equal magnitude not only for the users but for the law

[2] https://www.internetworldstats.com/stats.htm

enforcement agencies as well. This threat has taken a shape of crime, globally regarded as cybercrime. It's a crime that uses computer network or devices for fraud and identity theft by applying malware and hacking or phishing etc. The perpetrators use both "computer as a target" and "computer as a tool" for their criminal motivation including information warfare; phishing scams and spam. It appeared that no one expecteed the menace to grow at such a scale as the figures showed that globally cybercrime was the 2nd most reported crime in the year 2016 (GECS, 2016). While in proportion to the total number of crimes, cybercrime has accounted for more than 50% of all recorded crimes in UK alone. At university of Maryland in USA a study found that hackers are attacking computers and networks at a 'near-constant rate' with an average of one attack every 39 seconds (M. A. Kuypers et al).

Detection of such perpetrators is even more difficult than normal criminals involved in routine or existing conventional crimes, because an attacker of cyber activity resides within a network for an average 146 days before detection. The most common cybercrimes include financial crimes, cyber pornography, sale of illegal articles, online gambling, intellectual property crimes, email spoofing, forgery, cyber defamation and cyber stalking. In Pakistan we have 47.5 million mobile internet users along with another 2 million fixed broadband subscribers ranking 20th for online population in the world and these figures are accompanied

by ample challenges for the security of the users[3]. Pakistan's online space seems lawless mainly due to limited capabilities of our law enforcement agencies to handle cybercrime. The majority of users have nothing to do online except to use internet for basic telephony and to access social media. Seemingly people are technically handicapped and incognizant and this population is nothing less than an unguided mob that can be manipulated by anyone.

Criminals exploit the Internet and other network communications which are international in scope. Theoretically and practically this is a new subject for researchers which is growing exponentially. Much work has been done and endless has to be, because, the invention or up gradation of new technology leads to technical crime i.e. the digital crime, cybercrime or e-crime. This is because every day a new technique is being developed to carry out cybercrime and in most cases there is no access to proper detection, investigating method/model/technique to tackle that specific newly committed cybercrime.

Difference between Conventional Crime & Cybercrime

Crime tended to be seen as an absolute, largely understood in terms of theft and, to a lesser extent, violence, it is something perpetrated by 'criminals' on the law-abiding majority of the population and if detected will lead to some kind of sanction employed against the perpetrators. So, the crime is an act committed or

[3] https://www.techjuice.pk/broadband-internet-users-in-pakistan-cross-50-million/

omitted in violation of a law forbidding or commanding it and for which punishment is imposed upon conviction. In the contrary a cybercrime is defined as "Unlawful acts wherein the computer is either a tool or target or both. Cyber Criminal is a person who commits an illegal act with a guilty intention or commits a crime in context to cybercrime. Cybercriminals can be motivated criminals, organized hackers, professional hackers, discontented employees or cyber terrorists. Cybercrime can include everything from non-delivery of goods or services and computer intrusions (hacking) to intellectual property rights violation; economic espionage (theft of trade secrets), online extortion, international money laundering, identity theft; and a growing list of other Internet facilitated offenses. Further, it is not easy to identify immediately about the crime method used, and to answer questions like where and when it was carried out. The anonymity of the Internet makes it an ideal channel and instrument for many organized crime activities. Loss of evidence is another common & obvious problem as all the data could easily be destroyed making further collection of data outside the territorial extent also paralyzes this system of cybercrime investigation.

The Extent of Cybercrime

By the end of 2017, the global cyber security market had skyrocketed to $120.1 billion from a mere $63.7 billion in 2011. There were 556 million cybercrime victims in a year, while every new day 1.5 million people fall victim to cybercrime

and 18 people feel victim in the hands of cyber criminals every second across the world[4]. According to a report 1 in 10 social network users fall victim to a scam or fake link on social network platforms. Interestingly 59% of ex-employees admitted to stealing company data when leaving previous jobs. This data breach involves all types of industry and government organizations involving medical healthcare 38.9%, businesses 35.1%, education 10.7%, and financial departments 5.3%, while government and military faced 9.9%. And over 600,000 Facebook accounts are compromised every day.

Classification of Cyber Crime

The subject of cybercrime may be broadly classified under the following three groups:

1. **Against Individuals**, the crimes committed against individuals include harassment via e-mails, cyber stalking, dissemination of obscene material, defamation, unauthorized access over computer system, indecent exposure, email spoofing and acts of cheating and fraud. While these criminals also commit crimes against the property of an individuals and these include computer vandalism, transmitting virus, intellectual property crimes and internet time thefts etc.

[4] https://www.go-gulf.com/blog/cyber-crime/

2. **Against Organizations**, cybercriminals do vandalize big organizations including the government, private firms and private companies. This includes attacks involved to capture unauthorized access over the computer system, to get hold of unauthorized information, and cyber terrorism against the government organizations.

3. **Against Society at large**, these may be considered as petty crimes committed by cybercriminals and usually their scales are enormous and they target the whole society, considering the fact internet users comprised of a global village. This fact makes clear that no one is safe at the hands of cybercriminals. The type of crime committed against the society may include, pornography, polluting youth with indecent exposure, financial crimes, sale of illegal and contraband article, online gambling and forgery etc.

Motivations behind Cybercrime

There are many reasons for cybercriminals to commit cybercrime. A good knowledge of these reasons is necessary to formulate a prevention program. Few of the many are mentioned below:

i. For the sake of recognition.

ii. For the sake of quick money.

iii. To fight a cause, one thinks he believes in.

iv. Low marginal cost of online activity due to global reach.

v. Catching by law and enforcement agency is less effective and more expensive.

vi. Official investigation and criminal prosecution is rare.

vii. No concrete regulatory measure.

viii. Lack of reporting and standards

ix. Difficulty in identification

x. Limited media coverage.

xi. Corporate cybercrimes are done collectively and not by individual persons.

xii. Putting the public or any section of the public in fear; or

xiii. Affecting adversely the harmony between different religious, racial, language or regional groups or castes or communities; or

xiv. Endangering the sovereignty and integrity of the nation.

Types of Cyber Criminals

Cyber-criminals' unique profiles are significantly different from those of conventional criminals. Non-existence of cyber-criminals' database with law-enforcement agencies has also hampered the latter's ability to solve

cybercrimes. In Russia, for instance, most hackers are young, highly educated, and work independently and thus do not fit the conventional Police profiles of criminals. Cyber-criminals operate in various invented forms of markets. For instance, in a hybrid market consisting of online and offline market activities, with each having different roles. According to an estimate there were over 300 cashiers in Paris, who regularly steal payment-card details from their customers. Most of the stolen data were sold face-to face between fraudsters who met online (Sutherland, 2008). Likewise, in first- and second-tier cities in India, data brokers and data merchants reportedly buy data from people working in offshoring companies (Aggarwal, 2009).

Furthermore, the cyber criminals constitute of various groups/categories. These divisions may be justified on the basis of the object that they have in their mind. The major motivation behind cyber-attacks remained the promotion of political ends mainly free speech, human rights and information ethics. The main four groups emerged as cyber criminals include Cyber Criminals 40%, Hacktivism 50%, cyber warfare 3% and cyber Espionage 7%. These criminals can be categorized on the basis of age, skill and intentions. Following is a list of few types of cybercriminals.

(a) Children and adolescents between the age group of 6 – 18 years

The simple reason for this type of delinquent behavior pattern in children is seen mostly due to the inquisitiveness to know and explore things. Other cognate reason may be to prove themselves outstanding amongst other children in their group. Many other reasons exist for example, as the physical grounds for crime shrink for teenagers and dependency on technology increased at early age, they move towards the cyber world. These kids are either working for fun or being paid to create virus and programs for hacking. Their amateur efforts to hack or infect virus makes them cyber criminals, but because of their crude skills they are easily caught by the law enforcing authorities. At times, their efforts are so elementary level that the teens end up crippling their own PCs by infecting them with viruses which they have been trying to create (Secure Teen, 2014).

(b) Organized hackers

Cybercrime offers the potential for immense profits. So, it is no surprise that the digital "mob" has moved into the space. Today, the average age of a cybercriminal is 35, and 80% of hackers are affiliated with organized crime. In other words, people are choosing it as a profession. This has led to the creation of increasingly sophisticated criminal organizations that operate with the professionalism, discipline, and structure of legitimate enterprises. (T. Armerding, 2015). These kinds of hackers are mostly organized together to fulfil certain objectives including their political bias and fundamentalism, etc.

(c) Professional hackers / crackers

Their work is motivated by the color of money. These kinds of hackers are mostly employed to hack the site of the rivals and get credible, reliable and valuable information. Further they are even employed to crack the system of the employer basically as a measure to make it safer by detecting the loopholes.

(d) Discontented employees

This group include those people who have either been sacked by their employer or are dissatisfied with their employer. They normally hack the system of their employee as an act of avenge.

(e) Cyber Terrorism/Terrorists

Attackers who targeted military installations, power plants, air traffic control, banks, trail traffic control, telecommunication networks are the most likely Cyber Terrorists. Cyber terrorism is an attractive option for modern terrorists for several reasons.

i. It is cheaper than traditional terrorist methods.

ii. Cyber terrorism is more anonymous than traditional terrorist methods.

iii. The variety and number of targets are enormous.

iv. Cyber terrorism can be conducted remotely, a feature that is especially appealing to terrorists.

v. Cyber terrorism has the potential to affect directly a larger number of people.

Cyber Crime in Modern Society & Challenges

Cybercrimes have become a real threat today and are quite different from old-school crimes, such as robbing, mugging or stealing. The same systems that made it easier for people to conduct e-commerce and online transactions are now being exploited by cyber criminals. Unlike these crimes, cybercrimes can be committed single handedly and does not require the physical presence of the criminals. The crimes can be committed from a remote location and the criminals need not worry about the law enforcement agencies in the country where they are committing crimes. Today, criminals that indulge in cybercrimes are not driven by ego or expertise. Instead, they want to use their knowledge to gain benefits quickly. They are using their expertise to steal, deceive and exploit people as they find it easy to earn money without having to do an honest hard work. On the other hand, Law enforcement agencies are 5 to 10 years behind the global crime curve in relation to technological capabilities (Alexander, 2002).

In recent years, countries have enacted stricter laws against cybercrimes while many countries are still without a law to deal such crime. To take one example, when a Philippine hacker launched the "Love Letter" virus in 2000, the estimated loss of damage in the United States was in the range of US $4–15 billion. But the US government could not do anything to prosecute the hacker or to recover the damages because at that time the Philippines had no laws prohibiting such crimes (Adams, 2001).

Additionally, unlike conventional crimes, most cybercrimes are skill-intensive. Cybercrimes are also likely to originate because of the legitimate IT industry is too small to absorb available talents. The serious cybercriminals tend to be from countries that emphasize on physics, mathematics, and computer sciences education, but lack high paying legitimate IT jobs (Sullivan, 2007). In the former Soviet Union economies, computer specialists gained experience in "disassembling, examining and hacking American systems to see how they worked in order to make them functional on Soviet systems" (Serio & Gorkin, 2003).

It is also observed that the problem in guarding a computer system from unauthorized access is not due to human error but due to the complex technology. By secretly implanted logic bomb, key loggers can steal access codes, advanced voice recorders retina imagers etc. can fool biometric systems and bypass firewalls to get past many security systems. Another issue is, as the computers work on operating systems and these operating systems in turn are composed of millions of codes. Human mind is fallible and it is not possible that there might not be a lapse at any stage. The cyber criminals take advantage of these lacunas and penetrate into the computer system. Negligence is very closely connected with human conduct. It is therefore very probable that while protecting the computer system there might be any negligence, which in turn provides a cybercriminal to gain access and control over the computer system.

Furthermore, there are many challenges in front of us to fight against the cybercrime. Some of them here are as under:

i. Lack of awareness and the culture of cyber security, at individual as well as organizational level.

ii. Lack of trained and qualified manpower to implement the counter measures.

iii. No e-mail account policy especially for the defense forces, police and the security agency personnel.

iv. Cyber-attacks have come not only from terrorists but also from neighboring countries contrary to our National interests.

v. The minimum necessary eligibility to join the police/law enforcement agencies doesn't include any knowledge of computers so that they are almost illiterate to cyber-crime.

vi. The speed of cyber technology changes always beats the progress of government sector so that they are not able to identify the origin of these cyber-crimes.

vii. Promotion of Research & Development in ICTs is not up to the mark.

viii. Security forces and Law enforcement personnel are not equipped to address high-tech crimes.

ix. Present protocols are not self-sufficient, which identifies the investigative responsibility for crimes that stretch internationally.

x. Budgets for security purpose by the government especially for the training of law enforcement, security personnel's and investigators in ICT are less as compare to other crimes

Key Findings in the behavior of cybercriminals or Assumptions to commit crime

Considering cybercrime, it has been observed that most cyber criminals have a loose network wherein they collaborate and cooperate with one another. Unlike the real world, these criminals do not fight one another for supremacy or control. Instead they work together to improve their skills and even help out each other with new opportunities. Hence, the usual methods of fighting crime cannot be used against cyber criminals. While law enforcement agencies are trying to keep pace with cyber criminals, it is proving to be a Herculean task. This is primarily because the methods used by cyber criminals and technology keeps changing too quickly for law enforcement agencies to be effective. Once the modus operandi of cybercriminals is understood it will help to formulate an effective prevention strategy. The following five key elements could easily be derived from the discussion and literature review.

1) The decision of cybercriminals to offend is, to some extent, situationally determined.

2) Cybercriminals/Offenders freely choose to offend.

3) Cybercriminals are inflexible in relation to their time of operation and the target selected.

4) The motivation to offend is not constant and irrepressible.

5) Crimes prevented will not be totally displaced.

The Scope of Criminological Perspective in Cybercrime Management

The discussions in the preceding paragraphs have provided enough material to understand the extent of cybercrime along the vulnerability of its users. The types

of cybercriminals and their modus operandi had provided us an opportunity to design strategies to adopt the cybercrime prevention methodologies. There is a lot we can do to protect our cyber space not only by educating the masses but by enforcing certain strategies which could be adopted without much financial cost and by merely understanding the threat.

For instance, Crime Prevention methodologies provided in environmental criminological approach involve tending the physical environment from alterations to fences and alleyways in order to maximize the opportunities for surveillance. Brantingham and Brantingham suggest that a crime happens when four elements 'are in concurrence, a law, an offender, a target, and a place' (1981:7). They refer to those elements as the four dimensions of crime, and describe environmental criminology as the study of the fourth dimension. Environmental criminologists consider where and when crimes occur. Their questions concern the physical and social characteristics of crime sites, the movements that bring the offender and target together, the perceptual processes that bring about the selection of crime sites and the social processes of ecological labelling, the spatial patterning of laws and how this affects the creation of crime sites, the spatial distribution of offenders and targets in different settings and how the fourth dimension interacts with the other dimensions of crime in order for crimes to occur.

The environmental criminological methods have been clearly differentiated itself from contemporary crime prevention approaches by at least three types of shift in perspective. First, is to move away from the tendency for academics to keep their research into crime within the parameters of their own specific discipline. This approach suits very well to design cybercrime prevention techniques as the environmental criminologists have borrowed techniques and knowledge from many different disciplines in order to understand crime. The second, shift involves resisting the traditional search for causes of criminal motivation. This approach focusses instead on the criminal event, to find patterns in where, when and how crimes occur. The third shift involves moving from the sociological imagination to the geographical imagination. The following examples help to explain the different views which will be obtained about events, depending on which type of imagination is applied. They are anglicized versions of examples provided by the Brantinghams. Two burglaries committed in London and Manchester on different days of the week by different youths, both of whom are unemployed, could be

identical according to the sociological imagination, in that the same law is broken, the offenders are of the same age, and they are both out of work. To the geographic imagination, the burglaries would be seen as different from each other because of the gaps in time and setting. From another angle, a burglary committed by an unemployed youth within a quarter of a mile of his home 17 in the inner city, and a theft from a car by a middle-class youth within a quarter of a mile of his suburban home (both committed in the early hours) might be regarded as identical by the geographic imagination, but as quite different by the sociological imagination. Significance is given to different properties of the events, according to the perspective which is adopted.

While there is no need to replace the sociological imagination with the geographic one, both must be used together in an attempt to gain a better picture and understanding of crimes, and ultimately an increased capacity to control them. A potential cybercriminal calculates the legitimate opportunities of earing income open to him, the amount of reward the criminal activity offer including the amounts offered by illegal methods, the probability of arrest or apprehension, and the likely punishment. The perpetrator then chooses the activity (legal or illegal) which offers the highest discounted return. Preventive strategies to reduce the incidents of cybercrime must involve reform of the law and its administration in order to alter the equation and make cybercrime less attractive.

Evolution of crime prevention strategies

Faced with the apparent failure of the police, courts and prisons to stem rising crime rates, the law enforcement agencies began a clear policy shift from the late 1970s towards research and initiatives in the area of crime prevention. This approach is an attempt to alter the physical environment, rather than the offender, because, certain perpetrators have a dispositional advantage to offend and hence the key to crime prevention lies in changing them. This led eventually to the formation and development of 'situational crime prevention' methodology. This approach set out to use detailed crime pattern analysis to pinpoint areas of the environment which could be altered in such a way to make it less easy or less attractive for potential offenders to commit particular types of crime. This alteration of environment or situation might be through any of the variety of

initiatives, including extra physical security, new design of buildings or vehicles, increased surveillance and the marking of property. Resultantly, this 'targeting' approach necessitated detailed knowledge about the prevalence, geographical and temporal patterning, as well as the physical 'mechanics' of particular offence.

It's a criminological perspective that calls for expanding the crime-reduction role well beyond the justice system. This appraoch calls for minutely analyzing specific crime types to uncover the situational factors that facilitate their commission. Intervention techniques are then devised to manipulate the related situational factors. In theory, this approach reduces crime by making it impossible for it to be committed no matter what the offender's motivation or intent, deterring the offender from committing the offense, or by reducing cues that increase a person's motivation to commit a crime during specific types of events. Situational Crime Prevention has given rise to a retinue of methods that have been found to reduce crime at local and sometimes national or international levels. Situation Crime Prevention's focus is thus different than that of other criminological theories because it seeks to reduce crime opportunities rather than punish or rehabilitate offenders.

It is considered that the strategies adopted to alter the situation conducive for crime could best suit to formulate a cybercrime prevention strategy. The situational crime prevention methodology has a clear potential to reduce the incidence of cybercrime if implemented in a thoughtful manner. The potential of this strategy has a preventive approach by focusing on methods to reduce the opportunities for committing cybercrime.

Prevention of Cybercrime & Situational Crime Prevention

In recent times, the criminologists have advocated for the methodologies specifically intended to reduce crime rather than only focusing the criminal. According to Hough et al., 'crime prevention is a rather elastic term, which at its broadest encompasses any activity intended to reduce the frequency of events defined as crimes by the criminal law' (1980:1). Such a definition would help to include techniques for diverting offenders from crime, as well as the use of the criminal justice system to discourage reoffending. Such methods are described, respectively, as secondary and tertiary prevention (Brantingham, 1986:103).

Situational crime prevention measures have been vigorously promoted since long, largely because of a growing recognition that the criminal justice system is of limited effectiveness in reducing crime. It has also been argued that efforts to change the criminal disposition of offenders have been unproductive (Hough et al., 1980:3: Wilson, 1975).

While situational crime prevention method 'attempts to prevent crime by changings the situation in which crime occurs' (Poyner, 1983:5). Within the situational crime prevention approach, opportunity is a key concept. The notion of opportunity affecting crime refer to material conditions in which a potential offender may commit a crime. Secondly, in crimes resulting from impulse, the opportunity is said to consist simultaneously in those conditions and in the inducement to commit opportunity exists not only where the material conditions are conducive to crime, but also where benefits can be gained at minimal risk (Hough et al., 1985:5, Clarke, 1980). This type of approach has the tendency to curb the cybercrime. Because, the situational crime prevention measures have the ability and adoptability tailored to the types of opportunity which they seek to foreclose as the methods are intended to operate at three levels (Bennett, 1986:42). Those levels relate to:

1. The Individual;
2. The Community; and
3. The Physical Environment.

1. Measures operating at the level of the individual

1.1 Target Hardening

Target hardening is probably the most popular and most recognizable form of situational crime prevention. The rationale behind these measures is that spontaneous offenders will be put off and determined offenders held up, thus increasing their likelihood of being caught. There has been increasing research in recent years illustrating the benefits of target hardening methods as it involves increasing the physical security of potential targets. Prevention is always better than cure. It is always better to take certain precautions while working on the net.

Precaution, Prevention, Protection, Preservation and Perseverance must be observed by every user rather one should make them a part of their cyber life.

a) Identification of exposures through education will assist responsible companies and individuals and firms to meet these challenges.

b) One should avoid disclosing any personal information to strangers, the person whom they don't know, via e-mail or while chatting or any social networking site.

c) One must avoid sending any photograph to strangers by online as misusing or modification of photograph incidents increasing day by day.

d) An update Anti-virus software to guard against virus attacks should be used by all the citizens and should also keep back up volumes so that one may not suffer data loss in case of virus contamination.

e) A person should never send his credit card number or debit card number to any site that is not secured, to guard against frauds.

f) It is always the parents who have to keep a watch on the sites that their children are accessing, to prevent any kind of harassment or depravation in children.

1.2 Target Removal

These measures involve removing targets from the working environment to which potential offenders have access. Examples include replacement of payment with card operated systems or quarterly billing and switching to paying wages by bank credit instead of cash. Target removal may sometimes be combined with target hardening, as in the case of schools where televisions are kept out of sight in a protected strong room. Houg et al. suggest another variation involves removal of the target from the subjective worlds of potential offenders, for example, where damage is repaired quickly so that further attacks will not be encouraged (1980:6).

(a) Removing the means to commit crime

An example commonly used to illustrate this type of measure is the introduction during the 1970s of screening procedures to detect bombs and weapons at airports. This was followed by a reduction in incidents of

'skyjacking' (Wilkinson, 1977; Hough et al., 1980). At a more mundane level, householders are urged to store ladders securely, and not to leave keys in locks. While to deter cyber criminals, certain measures would help to reduce the cybercrimes:

i. Keep the Computer System Up-To-Date & Firewall turned-on Generally, Cyber criminals use software flaws to attack computer systems frequently and anonymously. Most Windows based systems can be configured to download software patches and updates automatically and this will help to monitor all online activity and protect the system from viruses and other malicious programs. To be safe on the Internet, the antivirus software should be configured to update itself every time the system connects to the Internet.

ii. Protect Your Personal Information Using many of the online services today involves sharing basic personal information to include name, home address, phone number, and email address. Using common sense is the best way to protect against and prevent Cyber Crime. Any financial transaction website should have an "s" after the letters "http" (e.g., https://www.mystore.com AND NOT http://www.mystore.com). The "s" stands for secure and should appear when you are in an area requesting you to login or provide other sensitive data. Another sign that you have a secure connection is the small lock icon in the bottom of your web browser (usually the right-hand corner). Hackers might try to gain access to crash it, delete information, or steal passwords and other sensitive information. Software firewalls are widely recommended for single computers. The software is prepackaged on some operating systems or can be purchased for individual computers. For multiple networked computers, hardware routers typically provide firewall protection.

iii. Choose a Strong Password and Protect It Usernames, passwords, and personal identification numbers (PIN) are used for almost every online transaction today. A strong password should be at least eight characters in length with a mixture of letters and numbers. Using the same password for various sites or systems increases the risk of discovery and possible exploitation. It is never a good practice to write a password down and leave it near the system it is intended to be used on. Changing a password every 90

days is a good practice to limit the amount of time it can be used to access sensitive information.

iv. Review Financial Statements Regularly Reviewing credit card and bank statements regularly will often reduce the impact of identity theft and credit fraud by discovering the problem shortly after the data has been stolen or when the first use of the information is attempted. Credit card protection services can often alert a person when there is unusual activity occurring on his or her account, for example, purchases in a geographically distant location or a high volume 22 of purchases. These alerts should not be taken lightly and could be the first indicator a targeted victim receives that something is wrong.

v. Never fall prey to luring slogans No one is going to receive a large sum of money from a dead Nigerian politician, win a huge lottery from being "randomly selected from a database of email addresses," or make big money from "passive residual income a few hours each day working out of your home." Many of these crimes go unreported because the victim is too embarrassed to admit to law enforcement that they were duped.

vi. Turn Off Your Computer With the growth of high-speed Internet connections, many opt to leave their computers on and ready for action. The downside is that being "always on" renders computers more susceptible. Beyond firewall protection, which is designed to fend off unwanted attacks, turning the computer off effectively severs an attacker's connection—be it spyware or a botnet that employs your computer's resources to reach out to other unwitting users.

(b) Reducing the pay-off The cybercrime landscape is rapidly changing in terms of hackers' monetary motives. "There is more of a financial incentive now for hackers and crackers as well as for virus writers to write for money and not just for glory or some political motive" (Blau, 2004). For instance, IT graduates with legitimate job in Romania earn about US $400 per month compared with several thousand per month in the cybercrime economy. A "security exploiter" can earn 10 times as much a security researcher (Claburn, 2008). Terri Forslof of TippingPoint Technologies put the issue this way: "Over a ten year period hack for fun and hack for fame has become hack for profit" (Webwire, 2008). "Today's online data thieves don't just run automatic scanners and jump on any network hole they find.

They're more likely to first choose a target that has data they can turn into cash, and then figure out how to break in" (Peter Tippett of Verizon Business, cf. Larkin, 2009, p. 33).

2. Measures operating at the level of community/organizations Web site owners should watch traffic and check any irregularity on the site. It is the responsibility of the web site owners to adopt some policy for preventing cybercrimes as number of internet users are growing day by day.

a. Formal Surveillance

A belief in the effectiveness of formal surveillance rests on the notion that potential offenders will be deterred by the threat of being seen, and that the agencies which perform formal surveillance represent such a threat. The first assumption corresponds with common sense and appears to be accurate (Mayhew, 1981:119). Authorities may perform physical surveillance utilizing security cameras, wiretaps and visual tracking to monitor employees' real-world movements. To keep tabs on digital activity the surveillance of computers and monitoring all elements of a suspect's computer use and online behavior. Computer surveillance may also involve sting operations like setting up a honeypot, which is an enticement to lure cybercriminals into a secured area of a computer server to illegally download files that can later be used against them as evidence

b. Natural Surveillance

Behind this form of surveillance lies the notion that by observing their environment as they go about their everyday business, people can provide themselves with some protection against crime. c. Surveillance by employees Hough et al, suggest there is promise in exploiting the capacity of certain employees to take on a surveillance role (1980). For example, apartment blocks with doormen are less vulnerable to burglary than those without them (Waller and Okihiro, 1978), two man buses suffered less vandalism than those with a driver only (Sturman, 1980), and after the installation of closed circuit television in four London Underground stations, thefts and robberies were reduced (Burrows, 1980). Cybercrime may require investigators to go undercover, adopting fake online personae to trap criminals. Undercover techniques could play a pivotal role in combating cybercrimes by tracking all interactions as evidence and may even arrange a face-to-face meeting to arrest the perpetrator.

d. Cross-Domain Solutions The best way to go about is using the solutions provided by Cross-Domain Solutions. When organizations use cross domain cyber security solutions, they can ensure that exchange of information adheres to security protocols. The solution allows organizations to use a unified system comprising of software and hardware that authenticates both manual and automatic transfer and access of information when it takes places between different security classification levels. This allows seamless sharing and access of information within a specific security classification, but cannot be intercepted by or 24 advertently revealed to user who is not part of the security classification. This helps to keep the network and the systems using the network safe.

3. Measures to improve Physical Environment Cyber security is an emerging threat to many critical industries as cyber intrusions pose a significant threat for contaminant releases that can result in damage to human health and the environment. Cybercrimes have the potential to cause catastrophic spills, waste discharges, and air emissions that result in bodily injury, property damage, environmental remediation expense and significant legal liability claims.

a) Web servers running public sites must be physically separately protected from internal corporate network.

b) It is better to use a security programs by the body corporate to control information on sites.

c) Strict statutory laws need to be passed by the legislatures keeping in mind the interest of citizens.

d) IT department should pass certain guidelines and notifications for the protection of computer system and should also bring out with some more strict laws to breakdown the criminal activities relating to cyberspace.

e) As Cyber Crime is the major threat to all the countries worldwide, certain steps should be taken at the international level for preventing the cybercrime.

f) A complete justice must be provided to the victims of cybercrimes by way of compensatory remedy and offenders to be punished with highest type of punishment so that it will anticipate the criminals of cybercrime.

3.1 Vulnerable Areas of Critical Systems

(a) Pipelines: Pipelines are very vulnerable to cyber-attacks due to their high reliance on SCADA (supervisory control and data acquisition) systems and computer networks. Oil and Gas pipelines, globally, have a favored target of terrorists, militant groups, and organized crime. A recent US Department of Homeland Security (DHS) study noted that most SCADA systems are protected by very weak passwords that are easily compromised.

(b) Pipelines, Oil production systems, refineries, manufacturing and chemical plants: operations that make extensive use of Digital Control Systems (DCS) are very vulnerable to cyber-attack. Control of a DCS system by an outsider can lead to severe consequences including fire, explosion or environmental release.

(c) Marine Systems: Maritime activity increasingly relies on ICT systems in order to optimize maritime operations. ICT is increasingly used to enable essential maritime operations, from navigation to propulsion, from freight management to traffic control communications, etc.

(d) Water Systems/Utilities: An attack on the control and/or SCADA system used in a water treatment and distribution system can significantly alter the system's performance and negatively impact public health and safety. In 2007 a faulty alarm at a water treatment facility in Spencer, Mass, caused release of excess sodium hydroxide into the water supply, ultimately injuring more than 100 people. Electric utilities are also prime targets because of the high visibility and wide-ranging impacts associated with power outages.

There is a lot to do for securing such installations. The prevention and guidance control need to be improved by appointing a specific security officer, by managing access control to computer systems (i.e. controls on what devices employees, vendors and other users can connect to the system). By introducing an appropriate level for each and individual access system for the employees by an effective password management setting.

Conclusion

Society as a whole needs to take measures toward reducing opportunities for cybercrime. According to the situational crime prevention theory, society plays a role in inadvertently creating crime, through the manufacturing of "criminogenic goods" (cars with no alarm systems, unprotected software, poor security devices, etc.), through leaky systems, and poor management/design of facilities. Cybercrime has high potential of causing unrest among people because being global or have no boundaries and thus creates high impact when it is done. Cybercrime is easy to commit without any physical existence required as it is global and this factor has become a challenge and risk to the crime prevention authorities and vice versa. The borderless nature of ICTs may not allow for rigid regulations and instead challenges the principle of criminal laws. As such, international laws and regulations combined with reliance on technologies are crucial to counter the cybercrime race.

The above narrated fact indicates that there is a temptation for criminals to engage in opportunistic behavior in the cyberspace. Compared to the physical world, the detection of opportunism is difficult in the cyberworld. The absence of appropriate measures to apprehend criminals reinforce the public distrust of law-enforcement agencies and increase the confidence of cyber-criminals, which results in more and serious cybercrimes. A Global Security Survey conducted by Deloitte Touche Tohmatsu in 2003, found that respondent companies spent 6% of their IT budgets on security. Nevertheless, cyberattacks are increasing rapidly. There is no pure technological solution for security-related problems involving technologies. Micro and macro-level measures combining technological and non-technological fixes are thus needed to combat cybercrimes.

In the conventional world, individuals and organizations can reduce the probability of becoming victims and their losses by buying insurance policies or by using safety measures such as anti-burglar systems and safety deposit boxes, or by living in safe neighborhoods (Ehrlich & Becker, 1972). Not all of these have their equivalents in the cyberworld. As noted above, certain "land use" types act as crime generators (McCord et al., 2007; Swope, 2001). While formal control mechanisms such as "hot spots policing" can be used to deal with land uses associated with high crime rates (Weisburd, Bushway, Lum, & Yang, 2004), there are no equivalents of such mechanisms in the cyberspace.

At the macro-level, development of national technological and manpower capabilities, enactment of new laws, a higher level of industry-government collaborations and international coordination are critical for combating this new form of crime. Investment in the skills of law-enforcement authorities is likely to enhance national capabilities to fight cybercrimes and thus increasing the probability of arrest and conviction. Measures taken so far have mainly emphasized on increasing penalty rather than on increasing the probabilities of arrest and conviction. This is arguably because law-enforcement agencies have been unable to catch up technologically with cyber-criminals (Downes, 2007). It is suggested that private citizens may be especially effective at combating cybercrimes as the costs are much less for individuals and private firms to protect their electronic records than those for the government to identify and prosecute criminals (Katyal, 2001; Mikos, 2006).

Bibliography

1. Rieth, C. 1956. A new study of police history. Edinburgh: Oliver & Boyd.

2. Ehrlich, I., & Becker, G. (1972). Market insurance, serf-insurance and serfprotection.

Journal of Political Economy, 80(4), 623–648.

3. Hough, M, Clarke, RVG and Mayhew, P (1980), 'Introduction', in RVG Clarke and P Mayhew (eds), Designing Out Crime, London: HMSO.

4. Wilson, JQ (1975) Thinking about Crime, New York: Basic Book.

5. Poyner, B (1983) Design Against Crime: Beyond Defensible Space, London: Butterworths. President's Commission on Law Enforcement and Administration of Justice (1967) Task Force Report: Crime and its Impact—An Assessment, Washington, DC: US Government Printing Office.

6. Clarke, RVG (1980) 'Situational Crime Prevention: theory and practice', British Journal of Criminology, 20: 136-47.

7. Bennett, T (1986) 'Situational Crime Prevention from the offender's perspective',

in K Heal and G Laycock (eds) Situational Crime Prevention: From Theory into Practice, London: HMSO.

8. Wilkinson, P (1977) Terrorism and the Liberal State, London: Macmillan.

9. Laycock, G (1985) Property Marking: A Deterrent to Domestic Burglary? Crime Prevention Unit 3, London: Home Office.

10.Mayhew, P (1981) 'Crime in public view: Surveillance and Crime Prevention', in

PJ Brantingham and PL Brantingham (eds) Environmental Criminology, Beverly Hills: Sage.

11.Waller, I and Okihiro, N (1978) 'Delinquency areas in the county of London',

British Journal of Criminology, 7: 250-84.

12. Sturman, A (1980) 'Damage on buses: the effects of supervision', in RVG Clarke

and P Mayhew (eds) Designing Out Crime, London: HMSO.

13.Burrows, J (1980) 'Natural Surveillance and Vandalism to telephone kiosks', in RVG Clarke and P Mayhew (eds) Designing out Crime, London: HMSO.

14.Brantigham, PJ and Brantingham, PL (eds) (1981) Environmental Criminology, Beverly Hills: Sage.

15.Global Economic Crime Survey 2016, Adjusting the Lens Preparation brings Opportunity back into focus, www.pwc.com/crimesurvey

16.Marshall A. Kuypers, Thomas Maillart and Elisabeth Paté-Cornell, Department of Management Science and Engineering, Stanford University, Stanford, CA, An Empirical Analysis of Cyber Security Incidents at a Large Organization.

17. Aggarwal, V. (2009). Lead: Cyber crime's rampant, Express Computer, 03 August 2009.http://www.expresscomputeronline.com/20090803/market01.shtml.

18. Sutherland, B. (2008). The Rise of Black Market Data; Criminals who steal personal data often don't exploit it. Instead, they put it up for sale on one of the many vibrant online markets.Newsweek (International ed.), 152(24).

29

19.Alexander, D. (2002, June). Policing and the global paradox. FBI Law Enforcement Bulletin, 71(6), 6–13, 00145688.

20.Adams, J. (2001, May/June). Virtual defense. Foreign Affairs, 98–112.

21.McCleary, R. M. (2008). Religion and economic development. Policy Review, 148, 45–57.

22. Serio, J. D., & Gorkin, A. (2003). Changing lenses: Striving for sharper focus on

the nature of the 'Russian Mafia' and its impact on the computer realm. International Review of Law, Computers and Technology, 17(2), 191–202.

23.Blau, J. (2004). Russia - a happy haven for hackers, 26 May 2004. http://www.computerweekly.com/Article130839.htm. Accessed 1 October 2005.

24.Claburn, T. (2008). The Cybercrime Economy, April 9, 2008. http://www.informationweek.com/blog/main/archives/2008/04/the_cyber_crime.html. Accessed 1 October 2009.

25.Webwire. (2008, June 25). First told of Chinese PC hijack explosion. http://www.webwire.com/ViewPressRel.asp?aId=68776. Accessed 1 October 2009.

26.https://www.secureteen.com/cyberbullying/teens-enter-the-world-of-cybercrime-for-money-thrill-and-fame/

27.Taylor Armerding, 2015, Cybercrime: Much more organized. https://www.csoonline.com/article/2938529/cyber-attacksespionage/cybercrime-much-more-organized.html.

28. Swope, R. E. (2001). Criminal theory on the street: Analyzing why offenses take place. Law and Order, 49(6), 121–128.

29.McCord, E. S., Ratcliffe, J. H., Garcia, R. M., & Taylor, R. B. (2007). Nonresidential crime attractors and generators elevate perceived neighborhood crime and incivilities. Journal of Research in Crime and Delinquency, 44(3), 295–320.

30.Weisburd, D., Bushway, S., Lum, C., & Yang, S. M. (2004). Trajectories of crime

at places: A longitudinal study of street segments in the city of Seattle.

Criminology, 42(2), 283–320.

31.Becker, G. S. (1995, Fall). The economics of crime. Cross Sections, 8–15.

http://www.

32.rich.frb.org/pubs/cross/crime/crime.pdf.

33.Downes, L. (2007, March 6). Cybercrime treaty: What it means to you.

Baseline.com.

34.Mikos, R. A. (2006). “Eggshell” victims, private precautions, and the societal

benefits of shifting crime. Michigan Law Review, 105(2), 307–351.

35.Katyal, N. K. (2001). Criminal law in cyberspace. University of Pennsylvania Law

Review, 149(4), 1003–1114.