Vol 4 Issue 10 April 2015 ISSN No :2231-5063

International Multidisciplinary Research Journal

Golden Research Thoughts

Welcome to GRT

RNI MAHMUL/2011/38595 **ISSN No.2231-5063**

Golden Research Thoughts Journal is a multidisciplinary research journal, published monthly in English, Hindi & Marathi Language. All research papers submitted to the journal will be double - blind peer reviewed referred by members of the editorial board.Readers will include investigator in universities, research institutes government and industry with research interest in the general subjects.

International Advisory Board

Editorial Board

Address:-Ashok Yakkaldevi 258/34, Raviwar Peth, Solapur - 413 005 Maharashtra, India
Cell : 9595 359 435, Ph No: 02172372010 Email: ayisrj@yahoo.in Website: www.aygrt.isrj.org

Golden Research Thoughts ISSN 2231-5063 Impact Factor : 3.4052(UIF)
Volume-4 | Issue-10 | April-2015 Available online at www.aygrt.isrj.org

AN EXAMINATION OF CYBERCRIME AND CYBERCRIME RESEARCH

Mane Ajay
I.T. Department D.G.Tatkare College. Mangaon - Raigad

Co-Author Details :

Khedekar Ajinkya Raman (T.Y.B.Sc. I.T.) [1] and Nileshraje Bhonsale (T.Y.B.Sc. I.T) [2]
I.T. Department D.G.Tatkare College. Mangaon - Raigad

ABSTRACT:
This paper provides an overview of the growing cybercrime problem and reviews two criminological theories that have been applied to the study of cybercrime and cybercrime victimization. Legislation which defines cybercrimes, establishes jurisdiction, and provides the legal base for prosecuting such crimes has been developed at both the federal and state level. Many federal law enforcement agencies have departments that attempt to combat a broad range of computer crimes from computer intrusions to intellectual property theft. Cyber victimization has affected many individuals and businesses in the United States and this problem seems to have increased as the use of computers and the internet increased over the last decade. Finally this paper concludes with some suggestions for areas of future research.

KEYWORDS
Cyber Attacks, Cyber Crimes, Potential Economic Impact, Consumer trust, National Security.

INTRODUCTION :-

The growing problem of cybercrime is an important issue facing researchers today. In the current age of online processing, maximum of the information is online and prone to cyber threats. There are a huge number of cyber threats and their behavior is difficult to early understanding hence difficult to restrict in the early phases of the cyber attacks. Cyber attacks may have some motivation behind it or may be processed unknowingly. The attacks those are processed knowingly can be considered as the cyber crime and they have serious impacts over the society in the form of economical disrupt, psychological disorder, threat to National defense etc. Restriction of cyber crimes is dependent on proper analysis of their behavior and understanding of their impacts over various levels of society.

In 1969, the first message, "login", was sent over ARPANET, the predecessor of today's internet (Kleinrock, 2008). ARPANET was designed as a communication system that would allow researchers to access information from other researchers computers around the country, therefore allowing information to flow more freely (Kleinrock, 2008). From this humble beginning the internet has expanded far beyond the expectations of the individuals who created it. Computers and the internet have become intertwined into our daily lives.

One reason why individuals use the internet is because they can gather and share information with other individuals no matter where on the globe they are located. This advancement in the way individuals can communicate with one another, as well as the decreasing cost and size of computers, are some of the reasons why internet use has grown so rapidly. Today, the top three websites Google, Microsoft, and Facebook each have over 300 million unique users (Nielson ratings, 2011). People's use of the internet and computers continues to grow as more and more people have access to this technology. However, while this new technology has brought with it much advancement which makes our lives easier, it has also led to advancements in crime.

The growth of the internet has also resulted in the creation and growth of cybercrime. The internet can help put offenders in contact with victims. Also, it provides individuals with the means of committing various cybercrimes. The growing threat of cybercrime and cybercrime victimization has resulted in President Obama appointing a Cyber Czar, someone who will oversee the defense of military computers and the development of offensive tactics in order to combat the growing threat of cyber warfare (Siobhan & Yochi, 2009). The President recently said, "Cyber security is not an end unto itself; it is instead an obligation that our governments and societies must take on willingly, to ensure that innovation continues to flourish, drive markets, and improve lives."

Our society is a little over two decades into the digital age, and our understanding of cybercrime is constantly changing; by looking at our understanding of cybercrime and cyber victimization today we can gain a better understanding of what we already know and, more importantly, what areas still need to be addressed.

Current era is too fast to utilize the time factor to improve the performance factor. It is only possible due the use of Internet. The term Internet can be defined as the collection of millions of computers that provide a network of electronic connections between the computers. There are millions of computers connected to the internet. Everyone appreciates the use of Internet but there is another side of the coin that is cyber crime by the use of Internet. The term cyber crime can be defined as an act committed or omitted in violation of a law forbidding or commanding it and for which punishment is imposed upon conviction. Other words represents the cyber crime as "Criminal activity directly related to the use of computers, specifically illegal trespass into the computer system or database of another, manipulation or theft of stored or on-line data, or sabotage of equipment and data". The Internet space or cyber space is growing very fast and as the cyber crimes. In general cyber crimes can be categorized as

follows-

1) Data Crime

a. Data Interception:

An attacker monitors data streams to or from a target in order to gather information. This attack may be undertaken to gather information to support a later attack or the data collected may be the end goal of the attack. This attack usually involves sniffing network traffic, but may include observing other types of data streams, such as radio. In most varieties of this attack, the attacker is passive and simply observes regular communication, however in some variants the attacker may attempt to initiate the establishment of a data stream or influence the nature of the data transmitted. However, in all variants of this attack, and distinguishing this attack from other data collection methods, the attacker is not the intended recipient of the data stream. Unlike some other data leakage attacks, the attacker is observing explicit data channels (e.g. network traffic) and reading the content. This differs from attacks that collect more qualitative information, such as communication volume, not explicitly communicated via a data stream.

b. Data Modification:

Privacy of communications is essential to ensure that data cannot be modified or viewed in transit. Distributed environments bring with them the possibility that a malicious third party can perpetrate a computer crime by tampering with data as it moves between sites.
In a data modification attack, an unauthorized party on the network intercepts data in transit and changes parts of that data before retransmitting it. An example of this is changing the dollar amount of a banking transaction from $100 to $10,000.

In a replay attack, an entire set of valid data is repeatedly interjected onto the network. An example would be to repeat, one thousand times, a valid $100 bank account transfer transaction.

c. Data Theft:

Term used to describe when information is illegally copied or taken from a business or other individual. Commonly, this information is user information such as passwords, social security numbers, credit card information, other personal information, or other confidential corporate information. Because this information is illegally obtained, when the individual who stole this information is apprehended, it is likely he or she will be prosecuted to the fullest extent of the law.

2) Network Crime

a. Network Interferences:

Network Interfering with the functioning of a computer Network by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing Network data.

b. Network Sabotage:

'Network Sabotage' or incompetent managers trying to do the jobs of the people they normally are in charge of? It could be the above alone, or a combination of things. But if Verizon is using the help the

children, hindering first responders line then they might be using network problems as an excuse to get the federal government to intervene in the interest of public safety. Of course if the federal government forces these people back to work what is the purpose of unions and strikes anyway.

3) Access Crime

a. Unauthorized Access:

"Unauthorized Access" is an insider's view of the computer cracker underground. The filming took place all across the United States, Holland and Germany. "Unauthorized Access" looks at the personalities behind the computers screens and aims to separate the media hype of the 'outlaw hacker' from the reality.

b. Virus Dissemination:

Malicious software that attaches itself to other software. (virus, worms, Trojan Horse, Time bomb, Logic Bomb, Rabbit and Bacterium are examples of malicious software that destroys the system of the victim.

4) Related Crimes

a. Aiding and Abetting Cyber Crimes:

There are three elements to most aiding and abetting charges against an individual. The first is that another person committed the crime. Second, the individual being charged had knowledge of the crime or the principals' intent. Third, the individual provided some form of assistance to the principal. An accessory in legal terms is typically defined as a person who assists in the commission of a crime committed by another or others. In most cases, a person charged with aiding and abetting or accessory has knowledge of the crime either before or after its occurrence. A person who is aware of a crime before it occurs, and who gives some form of aid to those committing the crime, is known in legal terms as an "accessory before the fact." He or she may assist through advice, actions, or monetary support. A person who is unaware of the crime before it takes place, but who helps in the aftermath of the crime, is referred to as an "accessory after the fact".

b. Computer-Related Forgery and Fraud:

Computer forgery and computer-related fraud constitute computer-related offenses.

c. Content-Related Crimes:

Cyber sex, unsolicited commercial communications, cyber defamation and cyber threats are included under content-related offenses

Some of the kinds of Cyber-criminals are mentioned as below.

1. Crackers: These individuals are intent on causing loss to satisfy some antisocial motives or just for fun. Many computer virus creators and distributors fall into this category.

2. Hackers: These individuals explore others' computer systems for education, out of curiosity, or to

compete with their peers. They may be attempting to gain the use of a more powerful computer, gain respect
from fellow hackers, build a reputation, or gain acceptance as an expert without formal education.

3. Pranksters: These individuals perpetrate tricks on others. They generally do not intend any particular or long-lasting harm.

4. Career criminals: These individuals earn part or all of their income from crime, although they Malcontents, addicts, and irrational and incompetent people: "These individuals extend from the mentally ill do not necessarily engage in crime as a full-time occupation. Some have a job, earn a little and steal a little, then move on to another job to repeat the process. In some cases they conspire with others or work within organized gangs such as the Mafia. The greatest organized crime threat comes from groups in Russia, Italy, and Asia. "The FBI reported in 1995 that there were more than 30 Russian gangs operating in the United States. According to the FBI, many of these unsavory alliances use advanced information technology and encrypted communications to elude capture".

5. Cyber terrorists: There are many forms of cyber terrorism. Sometimes it's a rather smart hacker breaking into a government website, other times it's just a group of like-minded Internet users who crash a website by flooding it with traffic. No matter how harmless it may seem, it is still illegal to those addicted to drugs, alcohol, competition, or attention from others, to the criminally negligent.

6. Cyber bulls: Cyber bullying is any harassment that occurs via the Internet. Vicious forum posts, name calling in chat rooms, posting fake profiles on web sites, and mean or cruel email messages are all ways of cyber bullying.

7. Salami attackers: Those attacks are used for the commission of financial crimes. The key here is to make the alteration so insignificant that in a single case it would go completely unnoticed e.g. a bank employee inserts a program into bank's servers, which deducts a small amount from the account of every customer.

. The total cost to pay by victims against these attacks is in millions of millions Dollar per year which is a significant amount to change the state of un-developed or under-developed countries to developed countries. Some of the facts related to cyber crimes can be significantly marked by the information provided by a US base news agency

- Research study has found that one in five online consumers in the US have been victims of cybercrime in the last two years.
- RSA, the security division of EMC have released their Quarterly Security Statistics Review concerning identity theft online, phishing and malware, data breaches and data loss.
- The review found that 23 percent of people worldwide will fall for spear phishing attacks, while web pages are infected on average every 4.5 seconds.
- In Australia, cybercrime costs businesses more than $600 million a year, while in the US, one in five online consumers have been victims of cybercrime in the last two years, equating to $8 billion.
- The review also found that consumers are increasingly concerned about their safety online. The Identity Theft Resource Centre, 2009 Consumer Awareness Survey in the US found that 85 percent

of respondents expressed concern about the safety of sending information over the Internet, while 59 percent expressed a need for improvement in the protection of the data they submit over websites.

- Reported cases of cases of spam, hacking and fraud have multiplied 50-fold from 2004 to 2007, it claims.
- One recent report ranked India in 2008 as the fourteenth country in the world hosting phishing websites. Additionally, the booming of call centers in India has generated a niche for cyber criminal activity in harvesting data, the report maintained.
- The words of Prasun Sonwalkar reflects the threat of cyber crime in India "India is fast emerging as a major hub of cyber crime as recession is driving computer-literate criminals to electronic scams, claimed a study by researchers at the University of Brighton. Titled 'Crime Online: cyber crime and Illegal Innovation', the study states that cyber crime in India, China, Russia and Brazil is a cause of "particular concern" and that there has been a "leap in cyber crime" in India in recent years, partly fuelled by the large number of call centers".

From Crime Desk of UK said that online fraud is worth around £50 billion a year worldwide, with criminal gangs increasingly using the latest technology to commit crimes, provoking the Association of Police Officers to state in the FT that "the police are being left behind by sophisticated gangs".

Computer spam refers to unsolicited commercial advertisements distributed online via e-mail, which can sometimes carry viruses and other programs that harm computers. For the year to date, the UAB Spam Data Mine has reviewed millions of spam e-mails and successfully connected the hundreds of thousands of advertised Web sites in the spam to 69,117 unique hosting domains, Warner said. Of the total reviewed domains, 48,552 (70%), had Internet domains "or addresses "that ended in the Chinese country code ".cn". Additionally, 48,331 (70%) of the sites were hosted on Chinese computers. Many of the African countries are lack of the cyber policies and laws (many articles and news are available at in this support). Due to this a cyber criminal may escape even then that is caught. Countries like Kenya, Nigeria, Tunisia, Tanzania etc. are almost free from the cyber laws and policies.

The above text only coated only some of the examples related to US, Europe, Asia and Africa to show the horrible situation of cyber crimes. Restriction of cyber crimes is dependent on proper analysis of their behavior and understanding of their impacts over various levels of society. Therefore, in the current manuscript a systematic understanding of cyber crimes and their impacts over society with the future trends of cyber crimes are explained.

Impacts of Cyber-Crime

Lunda Wright, a legal researcher specializing in digital forensic law at Rhodes University, has an interesting research finding on a blog posted in October 2005. It states that there has been an increased rate of prosecutions of cyber-criminals. There has been an increased clamping down on cyber-piracy related to the film and music works. There are novel lawsuits and strategies for litigation. There is a greater dependence on the skills of computer forensic experts in corporations and government. Finally, there is an increase in inter-government cooperative efforts.

Organized crime groups are using the Internet for major fraud and theft activities. There are trends indicating organized crime involvement in white-collar crime. As criminals move away from traditional methods, internet-based crime is becoming more prevalent. Internet-based stock fraud has earned criminals millions per year leading to loss to investors, making it a lucrative area for such crime.

Police departments across the nation validate that they have received an increasing number of

such crimes reported in recent years. This is in sync with the national trend resulting from increased computer use, online business, and geeky sophisticated criminals. In the year 2004, cyber-crime generated a higher payback than drug trafficking, and it is set to grow further as the use of technology expands in developing countries.

Scott Borg, director of the U.S. Cyber Consequences Unit, an agency supported by the U.S. Department of Homeland Security, recently indicated that denial-of-service attacks won't be the new wave of future. The worms, viruses are considered 'not quite mature' as compared to the potential of attacks in future.

1) Potential Economic Impact

The 2011 Norton Cyber crime disclosed that over 74 million people in the United States were victims of cyber crime in 2010. These criminal acts resulted in $32 billion in direct financial losses. Further analysis of this growing problem found that 69 percent of adults that are online have been victims of cyber crime resulting in 1 million cyber crime victims a day. Many people have the attitude that cyber crime is a fact of doing business online! .

As today's consumer has become increasingly dependent on computers, networks, and the information these are used to store and preserve, the risk of being subjected to cyber-crime is high. Some of the surveys conducted in the past have indicated as many as 80% of the companies' surveyed acknowledged financial losses due to computer breaches. The approximate number impacted was $450 million. Almost 10% reported financial fraud. Each week we hear of new attacks on the confidentiality, integrity, and availability of computer systems. This could range from the theft of personally identifiable information to denial of service attacks.

As the economy increases its reliance on the internet, it is exposed to all the threats posed by cyber-criminals. Stocks are traded via internet, bank transactions are performed via internet, purchases are made using credit card via internet. All instances of fraud in such transactions impact the financial state of the affected company and hence the economy.

The disruption of international financial markets could be one of the big impacts and remains a serious concern. The modern economy spans multiple countries and time zones. Such interdependence of the world's economic system means that a disruption in one region of the world will have ripple effects in other regions. Hence any disruption of these systems would send shock waves outside of the market which is the source of the problem.

Productivity is also at risk. Attacks from worms, viruses, etc take productive time away from the user. Machines could perform more slowly; servers might be in accessible, networks might be jammed, and so on. Such instances of attacks affect the overall productivity of the user and the organization. It has customer service impacts as well, where the external customer sees it as a negative aspect of the organization.

In addition, user concern over potential fraud prevents a substantial cross-section of online shoppers from transacting business. It is clear that a considerable portion of e-commerce revenue is lost due to shopper hesitation, doubt, and worry. These types of consumer trust issues could have serious repercussions and bear going into more detail.

2) Impact on Market Value

The economic impact of security breaches is of interest to companies trying to decide where to place their information security budget as well as for insurance companies' that provide cyber-risk

policies. For example, a ruling in favor of Ingram. Micro stated that "physical damage is not restricted to physical destruction or harm of computer circuitry but includes loss of use and functionality". This new and evolving view of damage becomes even more important as many firms rely on information systems in general and the Internet in particular to conduct their business. This precedent may force many insurance companies to compensate businesses for damage caused by hacker attacks and other security breaches. As the characteristics of security breaches change, companies continually reassess their IS environment for threats In the past, CIOs have relied on FUD—fear, uncertainty, and doubt—to promote IS security investments to upper management. Recently, some insurance companies created actuarial tables that they believe provide ways to measure losses from computer interruptions and hacker attacks. However, these estimates are questionable mostly due to the lack of historical data. Some industry insiders confess that the rates for such plans are mostly set by guesswork. As cited in: "These insurance products are so new, that the $64,000 question is: Are we charging the right premium for the exposure? Industry experts cite the need for improved return on security investment (ROSI) studies that could be used by insurance companies to create ? hacking insurance,with adjustable rates based on the level of security employed in the organization and by the organization to justify investments in security prevention strategies.

Depending on the size of the company, a comprehensive assessment of every aspect of the IS environment may be too costly and impractical. IS risk assessment provides a means for identifying threats to security and evaluating their severity. Risk assessment is a process of choosing controls based on the probabilities of loss. In IS, risk assessment addresses the questions of what is the impact of an IS security breach and how much will it cost the organization. However, assessing the financial loss from a potential IS security breach is a difficult step in the risk assessment process for the following reasons:

1. Many organizations are unable or unwilling to quantify their financial losses due to security breaches.
2. Lack of historical data. Many security breaches are unreported. Companies are reluctant to disclose these breaches due to management embarrassment, fear of future crimes, and fear of negative publicity. Companies are also wary of competitors exploiting these attacks to gain competitive advantage.
3. Additionally, companies maybe fearful of negative financial consequences resulting from public disclosure of a security breach. Previous research suggests that public news of an event that is generally seen as negative will cause a drop in the firm's stock price.

Risk assessment can be performed using traditional accounting based measures such as the Return on Investment (ROI) approach. However, ROI cannot easily be applied to security investments. To justify investment in IS security, CIOs will need to (1) present evidence that the costs of a potential IS security problem outweigh the capital investment necessary to acquire such a system and, (2) prove the expectation that the IS security system's return on investment will equal or exceed that of competing capital investment opportunities. This is difficult to accomplish since if the security measures work—the number of security incidents are low and there are no measurable returns. Accounting-based measures such as ROI are also limited by the lack of time and resources necessary to conduct an accurate assessment of financial loss. Instead, companies ' IT resources are devoted to understanding the latest technologies and preventing future security threats. In addition, potential intangible losses such as ? loss of competitive advantage" that result from the breach and loss of reputation are not included because intangible costs are not directly measurable.

Therefore, there is a need for a different approach to assess the risk of security breaches. One such approach is to measure the impact of a breach on the market value of a firm. A market value approach captures the capital market's expectations of losses resulting from the security breach. This approach is justifiable because often companies are impacted more by the public relations exposure

than by the attack itself. Moreover, managers aim to maximize a firm‘s market value by investing in projects that either increase shareholder value or minimize the risk of loss of shareholder value. Therefore, in this study we elected to use market value as a measure of the economic impact of security breach announcements on companies. In the following section we define a security breach as an unexpected event and discuss the characteristics of DOS attacks.

3) Impact on Consumer trust

Since cyber-attackers intrude into others‘ space and try and break the logic of the page, the end customer visiting the concerned page will be frustrated and discouraged to use the said site on a long term basis. The site in question is termed as the fraudulent, while the criminal masterminding the hidden attack is not recognized as the root cause. This makes the customer lose confidence in the said site and in the internet and its strengths.

According to reports sponsored by the Better Business Bureau Online, over 80% of online shoppers cited security as a primary worry when conducting business over the Internet. About 75% of online shoppers terminate an online transaction when asked for the credit card information. The perception that the Internet is rife with credit card fraud and security hazards is growing. This has been a serious problem for e-commerce.

Complicating the matter, consumer perceptions of fraud assess the state to be worse than it actually is. Consumer perception can be just as powerful - or damaging - as fact. Hence user’s concerns over fraud prevent many online shoppers from transacting business. Concern over the credibility of an e-business in terms of being unsafe or cluttered makes a shopper reluctant to transact business. Even the slightest perception of security risk or amateurish commerce seriously jeopardizes potential business.

4) Areas Ripe for Exploitation: National Security

Modern military of most of the countries depends heavily on advanced computers. Information Warfare, or IW, including network attack, exploitation, and defense, isn't a new national security challenge, but since 9/11 it has gained some additional importance. IW appeals because it can be low-cost, highly effective and provide deniability to the attacker. It can easily spread malware, causing networks to crash and spread misinformation. Since the emphasis is more on non-information warfare, information warfare is definitely ripe for exploration. The Internet has 90 percent junk and 10 percent good security systems. When intruders find systems that are easy to break into, they simply hack into the system. Terrorists and criminals use information technology to plan and execute their criminal activities. The increase in international interaction and the wide spread usage of IT has facilitated the growth of crime and terrorism. Because of the advanced communication technology people need not be in one country to organize such crime. Hence terrorists and criminals can find security loopholes in the system and can function from unusual locales instead of their country of residence.

Most of such crimes have been originating in developing countries. The wide spread corruption in these countries fuel these security hacks. The internet has helped fund such crimes by means of fraudulent bank transactions, money transfer etc. Greater encryption technology is helping these criminal activities.

A REVIEW OF CYBERCRIME

Understanding cyber law enforcement gives insight into how the problem is being addressed and thus a better understanding of the problem. Finally, it is important to have an idea of the true extent of the problem by examining the levels of cybercrime among businesses and individuals. This information will demonstrate the need for research into this growing problem.

Cybercrime Legislation

The widespread use of computers and the internet has led to new and expanded forms of crime, resulting in the need for new legislation. These new types of crime have left governments and law enforcement agencies with many questions. How does one define what cyber activities are legal and what activities are illegal? How does one enforce cyber laws when the relationship between the victim and the offender is often purely virtual? The internet allows people to interact with each other across borders, so whose jurisdiction is it? The Federal Government and the various state governments have all attempted to address these issues. This paper will briefly address some federal and state laws that have been created to deal with cybercrimes.

Federal Law

In order to combat the growing cybercrime problem, the United States government has established laws to deal with many cybercrimes including, but not limited to, computer intrusions, cyber-terrorism, and copyright infringements. These crimes encompass three domains of victims the government, the business, and the individual. The purpose of these laws is to help define what computer activity is and is not illegal. This section will provide a brief overview of Federal law concerning three specific types of cybercrime: computer intrusions, terrorism, and copyright infringement.

The Federal government has developed laws to deal with many cybercrime issues including computer intrusions. Individuals, businesses, and the government can all be victimized by cyber intrusions. The federal law that deals with computer intrusions, which includes crimes such as hacking, viruses, and malware, comes primarily from Title Cybercrime 8 18 U.S. Code § 1030 (Brenner, 2004).This law defines computer intrusions as an illegal computer activity. In order to fall under this federal law, the computer being intruded must fall under federal jurisdiction, which means that the computer must be used by either a financial institution or government agency or be used in interstate or foreign commerce (Brenner, 2004). This helps alleviate questions of jurisdiction by defining the types of computers that fall under federal jurisdiction. Federal jurisdiction for prosecuting computer intrusions against computers used by the government and financial institutions comes from Title 18 U.S. Code § 1030.

Another cybercrime issue that has been addressed by Federal law is cyber- terrorism. Federal cybercrime law dealing with terrorism is based primarily in Title 18 U.S. Code§ 2331. Terrorists can use computers to perform acts which might be harmful or intimidate individuals and when this is the case, the Federal government has jurisdiction. Terrorism is an important issue facing governments today and under United States Federal law, cyber-terrorism falls under the jurisdiction of the Federal government. The United States government has also developed laws to deal with issues of copyright infringement. Federal copyright law can be found in several statutes. Title 18 U.S. Code § 2319, makes it “a crime for someone willfully to infringe a copyright (a) for purposes of commercial advantage or private financial gain.” (Brenner, 2004). Computers have made it easier to engage in acts that violate copyright law, such as illegally downloading music and software. This law makes acts that violate copyright law illegal and

gives the Federal government jurisdiction for the investigation and prosecution of this crime.

State Law

Each state has its own cybercrime legislation defining what is and is not considered a cybercrime, making it difficult to comprehensively review current state level laws dealing with cybercrime. State governments have developed different laws to deal with many cybercrime issues including, but not limited to, computer intrusions and computer fraud. This section will provide a brief overview of state laws dealing with these two types of cybercrimes.

One cybercrime issue that states have addressed is cyber intrusions that occur on computers that are not used by the government or financial institutions. Both businesses and individuals can be potential targets for cyber intrusions. Lawmakers realize the dangers of computer intrusions, they do not agree on what constitutes computer intrusions. Brenner defines simple 'Hacking' as, "unauthorized access to a computer or computer system" (2004). However, according to the Arizona Revised Statutes § 13-2316 this is called computer tampering and involves, "Accessing, altering, damaging or destroying any computer, computer system or network." Each state has made decisions about what to include in legislation aimed at defining and combating cybercrime.

Another cybercrime issue that states have needed to address is computer fraud, which can affect both businesses and individuals. Like computer intrusions, lawmakers have differed on how they define and classify computer fraud. A few states make this type of fraud its own crime (Brenner, 2004). These states view computer fraud as its own type of offense separate from other types of fraud and other computer crimes. Other states, according to Brenner "simply include using a computer to commit fraud in their basic aggravated hacking statute." (2004) These states include various cybercrimes under one statute or offense category. Various states have taken different positions on how to define and classify cyber fraud.

In conclusion, the development and growth of cybercrimes in recent years have necessitated the various individual state governments in the United States to create laws addressing issues related to cyber intrusion and fraud. These types of crime fall under individual state government's jurisdiction to investigate and prosecute. While the laws between states differ, legislators in every state recognize cybercrime legislation as an important issue which needs to be addressed.

National Levels of Cybercrime

The development of the internet has led to the development of new types of crimes and new ways to commit crimes, but how prevalent is internet crime in today's world? The Bureau of Justice Statistics (BJS), a department of the U.S. Department of Justice, has conducted a national survey of businesses to determine, "the prevalence of computer security incidents." (Rantala, 2008) The 2005 National Computer Security Survey provides a good measure of the level of business cybercrime victimization in the United States. The Internet Crime Complaint Center (IC3), a partnership between the FBI and the National White Collar Crime Center publishes annual reports for the nation, as well as annual reports for each state, which detail the type, number, and characteristics of complaints received by the IC3 (The FBI, 2010). Information from the 2010 IC3 report provides a good measure of the level of individual cybercrime victimization in the United States. The national reports of the Bureau of Justice Statistics and the Internet Crime Complaint Center provide information on national computer crime levels.

Business Cyber Victimization

In 2005, the Bureau of Justice Statistics conducted the National Computer Security Survey which sampled 7,818 businesses, from thirty-six different industries, to determine the pervasiveness of cybercrime incidents (Rantala, 2008). It is important to understand the extent of cybercrime victimizations among U.S. businesses so businesses and law enforcement agencies can work together to protect our economy. Cybercrime incidents included crimes such as cyber-attacks which include viruses and denial of service attacks, cyber-thefts which includes crimes such as fraud and theft of intellectual property, and other incidents such as spyware and hacking (Rantala, 2008). Of the 7,818 businesses surveyed "67% detected at least one cybercrime in 2005." (Rantala, 2008) Many U.S. businesses, both small and large, are being victimized by computer crimes.

This survey also found that there were more than 22 million cybercrime incidents which resulted in a total financial loss of $867 million (Rantala, 2008). This is a large sum of money that businesses are losing as a result of computer crimes. The large financial loss from cybercrimes poses a threat not only to businesses, but also to local, national, and global economies. The National Computer Security Survey found that there are high rates of computer victimization among business and that these crimes are causing businesses to lose millions of dollars.

The National Computer Security Survey also asked businesses about the identity, if known, of the perpetrator. The study found that about 75% of cyber thefts, which include crimes such as fraud, embezzlement, and theft of intellectual property, were perpetrated by insiders in the business (Rantala, 2008). This suggests that companies need to improve their internal computer security and monitor their employees to reduce their victimization from cyber-thefts. However, 70% of cyber-attacks perpetrated against businesses were committed by individuals outside of the company (Rantala, 2008). This suggests that companies should focus on increasing their external computer security from cyber-attacks committed by outsiders.

In sum, cybercrime victimization is very prevalent among businesses both large and small. This victimization is perpetrated by both insiders and outsiders and results in large financial losses for businesses. Cybercrime victimization is very prevalent among businesses, as well as among individuals.

Individual Cyber Victimization

Victims of cybercrime can report incidents of cybercrime victimization to the Internet Crime Complaint Center (IC3). The IC3 then takes these complaints and funnels them to the appropriate federal agencies for investigation (The FBI, 2010). This makes it easy for victims because they can report to one agency that can then send these reports to the appropriate organization for investigation rather than trying to figure out which agency investigates this type of incident. Every year the Internet Crime Complaint Center publishes a report detailing the number and type of incidents reported as well as the characteristics of the victims and perpetrators (The FBI, 2010). Although these reports only provide information about incidents reported to the IC3, the information in these reports still provide a valuable look into the prevalence of internet crime and victimization in the United States.

The IC3 tracks the number of complaints that it receives each year, providing a picture of the rate of cybercrime victimization in the U.S. In 2000, when the Internet Crime Complaint Center first opened it received about 17,000 complaints. In 2010, the number of complaints per year had risen to over 300,000 (The FBI). This is a 1,664.7% increase over a ten year period. There are many possibilities for this increase. For one thing it is possible that more people know about the Internet Crime Complaint Center today and therefore use the service more than in 2000. This increase could also be the result of

increases in levels of cybercrime over the decade. Or it could be a combination of both. During 2010, the top ten crimes reported to the IC3 were: "the non-delivery of payment or merchandise, FBI-related scams, identity theft, computer crimes, miscellaneous fraud, advance fee fraud, spam, auction fraud, credit card fraud, and overpayment fraud" (The FBI). This information can provide law enforcement agencies with an idea of what types of computer crime they should focus their efforts.

According to the IC3, in 2010 "most complainants were in the U.S., male, between 40 and 49, and a resident of California, Florida, Texas, and New York." (The FBI) These characteristics suggest that there may be certain types of people or geographic areas that are more at risk for victimization. Men, between 40 and 49, may be more at risk for victimization because they are more likely to be involved in business and therefore provide an attractive target. In 2010, males reported more incidents of victimization than females (The FBI). According to the IC3, in 2010 "men reported greater dollar losses than women (at a ratio of $1.25 to every $1.00)." (The FBI) Not only are males more likely to report incidents of computer victimization, but males also report higher levels of monetary loss from victimization than females.

The Internet Crime Complaint Center also provides information on demographic characteristics of perpetrators when complainants knew the offender. In 2010, known offenders were mostly male "more than half resided in California, Florida, New York, Texas, the District of Columbia, or Washington." (The FBI) California, Florida, New York, and Texas are also the same states where most complainants resided. This overlap between victims and offenders can partially be explained by the fact that these states have the largest populations in the United States. Not only are males more likely to report an incident of cybercrime victimization, but males are more likely to be the perpetrators in cases where the perpetrator is known. Almost fifty percent of perpetrators reported to the IC3 are residing in the United States (The FBI, 2010). According to the Internet Crime Complaint Center?s 2010 report, in cases where the perpetrator is known and resides in a foreign country, most offenders came from "the United Kingdom, Nigeria, and Canada". This information can help governments work together to better combat the problem of cybercrime.

In conclusion, the internet has changed the way the world does business and how individuals run their lives. However, the advent of this new technology has resulted in a new way for offenders to commit crimes. But how prevalent is internet crime in our society today? The number of cybercrime incidents reported Internet Crime Complaint Center has drastically increased over the last decade (The FBI, 2010). This suggests that not only is cybercrime a major issue facing businesses, but it also poses a major problem for individuals as well. The increasing number of cybercrime incidents among businesses and individuals suggests that cybercrime will be an important field of study as we move into the future.

A REVIEW OF THEORIES:- Now that we have reviewed several aspects of computer crime including current legislation, law enforcement, and the prevalence of computer crime, this paper will review crime theories that have been applied to the study of cybercrime. Over the past two hundred years many theories have been developed in an attempt to explain why crimes occur. Some of these theories, like self-control theory and routine activity theory, have been applied to the study of cybercrime. These theories focus on the individual level characteristics in individuals or the situations they are in that increase the chances of a crime occurring. The study of cybercrime will become more and more important as we look for solutions to this growing problem. This section will review the different theories and their empirical studies which have been applied to the study of cybercrime.

In criminology the two main schools of thought are the classical school and the positivist

school. Classical theorists believe that people are rational and that they commit crimes through their own free will in order to satisfy their own self- interest (Cullen & Agnew, 2006). According to classical theorists people will not participate in crime if they know what the punishment will be, they know that it will be delivered rapidly, and they know that punishment is certain because when this occurs the consequences from committing the crime outweigh the benefits an individual would have received from a crime (Cullen & Agnew, 2006). People rationally choose to participate in criminal acts; in order to prevent these acts from occurring people need to know that consequences will outweigh the benefits. If people believe that the consequences outweigh the benefits then they will freely choose not to participate in the criminal behavior. On the other hand the positive school of criminology believes that individuals participate in crime because of forces beyond individual control and relies on the scientific method to prove its theories (Cullen & Agnew, 2006). Individuals should not be held solely responsible for their actions because not everyone is rational. Outside factors can play an important part in determining one's participation in crime.

AREAS FOR FUTURE RESEARCH:- One area that merits future research is the expansion of these studies to more varied samples. Most of the empirical studies reviewed by this paper surveyed college students about their involvement in cybercrime and cybercrime victimization. Using college students can provide an important look into the phenomenon because most college students regularly use computers and the internet. This regular computer use, as well as students computer skills, means that college students have the access and ability to commit cybercrimes and they may be at higher risk for being victimized online. College students are an important demographic in the study of cybercrime, however they do not represent the whole picture. College students are a self-selected group of individuals therefore future research needs to be conducted among other groups to determine if findings from studies on college students can truly be generalized to the entire population.

A second area for future research is the study of business cyber victimization. There have been very few research studies examining cybercrimes and business. The Bureau of Justice Statistics conducted the National Security Survey which measured the prevalence of business cybercrime victimization (Rantala, 2008). However, this survey did not examine issues of why some businesses experienced cybercrime victimization, leaving scholars with future research possibilities. For example, researchers could examine whether certain business practices, such as online banking, make some business more attractive to offenders? Most current cybercrime research has studied what makes certain individuals more at risk for cybercrime victimization. However, if researchers expand their research to the study of business victimization, it would be possible to learn what makes certain businesses more susceptible to cybercrime victimization and point to possible practices that might reduce a business likelihood of being victimized.

The nature of the internet makes it difficult for parents to monitor their children's behavior and as a result they are not able to correct the behavior. Does this result in children developing further characteristics of low self-control? Researchers could explore the influence of the internet on effective parenting. There are still several areas of cybercrime research to which self-control can be applied.
Scholars need to conduct more research into this area to examine whether routine activity theory can be applied to the study of cybercrime and what answers this application can offer us. Some scholars say that routine activity theory can be applied to the study of cybercrime, others disagree.

Researchers have also begun to use routine activity theory to study cyber victimization. Their application of routine activity theory has shown that this theory holds promise for explaining cyber victimization. These studies found that an individual's routine activities, such as the number of social networking sites he or she uses and an individual's use of online communication, increases his or her

likelihood of victimization for both violent and nonviolent cybercrimes.

CONCLUSION

Computers and the internet have become common place in today's society. This new technology has resulted in the development of a new form of crime, cybercrime. This paper has provided a background to the cybercrime problem. It has reviewed current legislation on cybercrime, current law enforcement responses to cybercrime, and classified different forms of cybercrime. Both the Federal government and the various state governments have developed legislation which defines cybercrimes, establishes jurisdiction, and provides the legal base for prosecuting such crimes. This paper has also reviewed various cybercrimes and classified these crimes into three general categories, crimes against the computer, crimes where the computer is the tool used to commit the crime, and crimes where the computer is just incidental to the crime (Brenner, 2004). Furthermore, this paper has examined the current level of cyber victimization for both businesses and individuals. Cyber victimization affects many individuals and businesses in the United States and this problem seems to have increased as the use of computers and the internet has increased over the last decade. This paper has provided a look at what we know about cybercrime and victimization a little more than a decade into the new century. As the use of computers and the internet becomes further engrained into our society this problem will continue to face legislators and law enforcement officials. The fluidity of technology will make it difficult to develop programs and policies to help protect people. Cybercrime research will be an important area of study for future criminologist as we move farther into the digital age, who knows, there may be a day in the far future when the number of cybercrimes committed outweighs the number of traditional crimes committed. This manuscript put its eye not only on the understanding of the cyber crimes but also explains the impacts over the different levels of the society. This will help to the community to secure all the online information critical organizations which are not safe due to such cyber crimes. The understanding of the behavior of cyber criminals and impacts of cyber crimes on society will help to find out the sufficient means to overcome the situation.

REFERENCES

[1.] Wow Essay (2009), Top Lycos Networks, Available at: http://www.wowessays.com/ dbase/ab2/ nyr90.shtml, Visited: 28/01/2012.
[2.] Bowen, Mace (2009), Computer Crime, Available at: http://www.guru.net/, Visited: 28/01/2012.
[3.] CAPEC (2010), CAPEC-117: Data Interception Attacks, Available at: http://capec.mitre.org/ data/ definitions/ 117.html, Visited: 28/01/2012.
[4.]Oracle (2003), Security Overviews, Available at: http://docs.oracle.com/cd/B13789_01/ network.101/ b10777/overview.htm, Visited: 28/01/2012.
[5.]Computer Hope (2012), Data Theft, Available at: http://www.computerhope.com/jargon/d/ datathef.htm, Visited: 28/01/2012.
[6.] DSL Reports (2011), Network Sabotage, Available at: http://www.dslreports.com /forum/ r26182468-Network-Sabotage-or-incompetent-managers-trying-to-, Visited: 28/01/2012.
[7.] IMDb (2012), Unauthorized Attacks, Available at: http://www.imdb.com/title/tt0373414/, Visited: 28/01/2012
[8.] Virus Glossary (2006), Virus Dissemination, Available at: http://www.virtualpune.com/citizen-centre/html/cyber_crime_glossary.shtml, Visited: 28/01/2012
[9.] Leagal Info (2009), Crime Overview Aiding And Abetting Or Accessory, Available at:

http://www.legalinfo.com/content/criminal-law/crime-overview-aiding-and-abetting-or-accessory.html, Visited: 28/01/2012
[10.] Shantosh Rout (2008), Network Interferences, Available at: http://www.santoshraut.com/forensic/ cybercrime.htm, Visited: 28/01/2012
[11.] By Jessica Stanicon (2009), Available at: http://www.dynamicbusiness.com/articles/articles-news/one-in- five-victims-of-cybercrime3907.html, Visited: 28/01/2012.
[12.] Prasun Sonwalkar (2009), India emerging as centre for cybercrime: UK study, Available at: http://www.livemint.com/2009/08/20000730/India-emerging-as-centre-for-c.html, Visited: 10/31/09
[13.] India emerging as major cyber crime centre (2009), Available at: http://wegathernews.com/203/india- emerging-as-major-cyber-crime-centre/, Visited: 10/31/09
[14.] PTI Contents (2009), India: A major hub for cybercrime, Available at: http://business.rediff.com/slide- show/2009/aug/20/slide-show-1-india-major-hub-for-cybercrime.htm, Visited: 28/01/2012.
[15.] Crime Desk (2009), Million Online Crimes in the Year: Cyber Crime Squad Established, Available at:http://www.thelondondailynews.com/million-online-crimes-year-cyber-crime-squad-established-p-3117.html, Visited: 28/01/2012.
[16.] Newswise (2009), China Linked to 70 Percent of World's Spam, Says Computer Forensics Expert, Available at: http://www.newswise.com/articles/view/553655/, Visited: 28/01/2012.
[17.] Cyberlawtimes (2009), Available at: http://www.cyberlawtimes.com/forums/index.php?board=52.0, Visited: 10/31/09
[18.] Kevin G. Coleman (2011), Cyber Intelligence: The Huge Economic Impact of Cyber Crime, Available at:http://gov.aol.com/2011/09/19/cyber-intelligence-the-huge-economic-impact-of-cyber-crime/, Visited: 28/01/2012
[19.] Gordon, L. A. et al., 2003, A Framework for Using Insurance for Cyber-Risk Management, Communications of the ACM, 46(3): 81-85.
[20.] D. Ariz. (April 19, 2000), American Guarantee & Liability Insurance Co. v. Ingram Micro, Inc. Civ. 99-185 TUC ACM, 2000 U.S. Dist. Lexis 7299.
[21.] Kelly, B. J., 1999, Preserve, Protect, and Defend, Journal of Business Strategy, 20(5): 22-26.
[22.] Berinato, S. (2002), Enron IT: A take of Excess and Chaos, CIO.com, March 5 http://www.cio.com/executive/edit/030502_enron.html, Visited: 28/01/2012
[23.] Power, R., 2001, 2001 CSI/FBI Computer Crime and Security Survey, Computer Security Issues and Trends, 7(1): 1-18.
[24.] Hoffer, J. A., and D. W. Straub, 1989, The 9 to 5 Underground: Are You Policing Computer Crimes?, Sloan Management Review (Summer 1989): 35-43
[25.] Sprecher, R., and M. Pertl, 1988, Intra-Industry Effects of the MGM Grand Fire, Quarterly Journal of Business and Economics, 27: 96-16.
[26.] Baskerville, R., 1991, Risk Analysis: An Interpretive Feasibility Tool in Justifying Information Systems Security, European Journal of Information Systems, 1(2): 121-130.
[27.]Lyman, J., 2002, In Search of the World's Costliest Computer Virus, http://www. newsfactor.com/perl/story/16407.html. 2002.
[28.] D'Amico, A., 2000, What Does a Computer Security Breach Really Cost?, The Sans Institute
[29.] Hancock, B., 2002, Security Crisis Management—The Basics, Computers & Security, 21(5): 397-401.
[30.] Cyber Trust and Crime Prevention, Mid-Term Review, November 2005 – January 2009, Available at: http://www.bis.gov.uk/assets/bispartners/foresight/docs/cyber/ctcp_midterm_ review.pdf, Visited: 28/01/2012

[31.] Nigel Jones, Director or the Cyber Security Knowledge Transfer Network, was featured in the daily telegraph (May 6, 2008), Cyber Security KTN,
[32.] Nilkund Aseef, Pamela Davis, Manish Mittal, Khaled Sedky, Ahmed Tolba (2005), Cyber-Criminal Activity and Analysis,White Paper, Group 2.
[33.] Stephen Northcutt et al. (2011), Security Predictions 2012 & 2013 - The Emerging Security Threat, Available at:http://www.sans.edu/research/security-laboratory/article/security-predict2011, Visited: 29/01/2012. Arizona Revised Statutes § 13-2316. Computer tampering; venue; forfeiture; classification. Retrieved February 15, 202, from http://www.azleg.state.az.us/ Format Document.asp?inDoc=/ars/13/02316.htm&Title=13&DocType=AR Brenner, S. (2004). U.S. cybercrime law: Defining offenses. Information Systems Frontiers, 6(2), 115-132.
[34]Buzzell, T., Foss, D., & Middleton, Z. (2006). Explaining use of online pornography: A test of self-control theory and opportunities for deviance. Journal of Criminal Justice and Popular Culture, 13(2), 96-116. Retrieved December 27, 2011, from http://www.albany.edu/scj/jcjpc/vol13is2/Buzzell.pdf
[35]Cohen, L., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. In F.
[36] Cullen & R. Agnew (Eds.), Criminological Theory Past to Present: Essential Readings (pp. 427-442). New York, NY: Oxford University Press.
[37]Deng, X., & Zhang, L. (1998). Correlates of self-control: An empirical test of self-control theory. Journal

Publish Research Article
International Level Multidisciplinary Research Journal
For All Subjects

Dear Sir/Mam,

We invite unpublished Research Paper,Summary of Research Project,Theses,Books and Book Review for publication,you will be pleased to know that our journals are

Associated and Indexed,India

- International Scientific Journal Consortium
- OPEN J-GATE

Associated and Indexed,USA

- EBSCO
- Index Copernicus
- Publication Index
- Academic Journal Database
- Contemporary Research Index
- Academic Paper Databse
- Digital Journals Database
- Current Index to Scholarly Journals
- Elite Scientific Journal Archive
- Directory Of Academic Resources
- Scholar Journal Index
- Recent Science Index
- Scientific Resources Database
- Directory Of Research Journal Indexing

Golden Research Thoughts
258/34 Raviwar Peth Solapur-413005,Maharashtra
Contact-9595359435
E-Mail-ayisrj@yahoo.in/ayisrj2011@gmail.com
Website : www.aygrt.isrj.org