**International Journal of Engineering Sciences & Emerging Technologies, October 2013.**
**ISSN: 22316604 Volume 6, Issue 2, pp: 142-153 ©IJESET**

# IMPACT OF CYBER CRIME: ISSUES AND CHALLENGES

Sumanjit Das and Tapaswini Nayak
Asst-Prof. Dept of Computer Science and Engineering,
Centurion University of Technology and Management, Bhubaneswar, Odisha, India

***ABSTRACT***
*The facilities of computer technology have not come out without drawbacks. Though it makes the life so speedy and fast, but hurled under the eclipse of threat from the deadliest type of criminality termed as 'Cyber crime' without computers, entire businesses and government operations would almost cease to function. This proliferation of cheap, powerful, user-friendly computers has enabled more and more people to use them and, more importantly, rely on them as part of their normal way of life. As businesses, government agencies, and individuals continue to rely on them more and more, so do the criminals 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 various areas like Soci-eco-political, consumer trust, teenager etc.with the future trends of cyber crimes are explained.*

***INDEX TERMS—****Cybercrime, Consumer trust, Soci-eco-poltical, Security.*

## I. INTRODUCTION

Cybercrime is a term used to broadly describe criminal activity in which computers or computer networks are a tool, a target, or a place of criminal activity and include everything from electronic cracking to denial of service attacks. It is also used to include traditional crimes in which computers or networks are used to enable the illicit activity. The Cyber crime can halt any railway where it is, it may misguide the planes on its flight by misguiding with wrong signals, it may cause any important military data to fall in the hands of foreign countries, and it may halt e-media and every system can collapse within a fraction of seconds.

The present study has been undertaken to touch some aspects, effect and prospects of this cyber-technology with special reference to threat poses of Cyber crime by India. Efforts have been made to analyze legal framework available for its control in India. To start with, it is, therefore, necessary to demarcate the dimensions of word 'crime'. Thus it is beyond doubt that 'crime' is a relative phenomenon, universal in nature and essentially all societies from ancient to modern have been evidently demonstrating its presence. Each society have been providing its own description of criminal behavior and conduct made punishable by express will of the political community ruling over the society and it was always influence by religious-social-political economical values prevailing in the given society. Thus from time immemorial the behavior that attracts '*penal liability*' influenced and characterized by overall outcome of these standards. Parenthetically, just as concept of crime [has undergone] change with the growth of Information Technology so the categories of criminals who engage in such crimes. So far Indian society is concerned, particularly during ancient period, the definition of crime flagged by religious interpretation. The period was known for complete ominance of religion. All political and social activities in general and 'Crime' in particular, considered to be happened due to the presence of super-natural power. The Demonological theory of crime causation was an outcome of this period.

Medieval period had evidenced the eras of renaissance and restoration, which delivered new, and a fresh look to 'crime'. The concepts like utilitarian, positive approach, analytical thinking, principles of natural justice, and thoughts of *lessie faire*, hedonistic philosophy, and pain and pleasure theory were

outcome of this period which helped to open new horizons for the study of crime. Latter period paved the way for scientific & industrial revolution and rational way of interpretation dominated the thinking.

***A Brief Survey***

The *2006 Computer Crime and Security Survey*, conducted by the Computer Security Institute in conjunction with the U.S. Federal Bureau of Investigation's International Computer Crime Squad [CSI/FBI 2006], showed an alarmingly high number of businesses reporting difficulties with computer and Internet fraud. Among the findings:

Of the organizations who acknowledged financial losses due to computer breaches, many could not quantify the losses.

---- 65% detected computer viri;

---- 48% reported between one and five security incidents if the year

---- 42 % reported incidents that originated from sources within the organization;

---- 32% of the respondents experienced incidents of unauthorized use of their computer systems during the last year;

---- 47% reported theft of laptop computers and mobile devices; in the area of e-commerce:

All of the respondents experienced some sort of website incidents:

- 9% said they had experienced theft of proprietary information;
- 6% reported website defacement;
- 9% were victims of financial fraud.
- 3% were victims of sabotage

Losses due to computer security breaches totaled over US$ 52 million in 2006, a figure that is down 30% from the over US$ 141 million reported in 2004.. It must be noted, however that these figures relate just to the 313 respondents that advised the CSI / FBI survey of their results, and not all companies in the US. It was distributed to 5,000 companies in January 2006 for response, showing a return rate of 6%.

## II. CATEGORIES OF CYBER CRIME

### Data Crime

*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 [3].

*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 [4]. 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.

*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 [5].

## Network Crime

*Network Interferences*

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

*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 [6].

## Access Crime

*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 [7].

*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 [8].

## Related Crimes

*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" [9, 10].

*Computer-Related Forgery and Fraud*

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

*Content-Related Crimes*

Cyber sex, unsolicited commercial communications, cyber defamation and cyber threats are included under content-related offenses. 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 [11]-**

1. Research study has found that one in five online consumers in the US have been victims of cybercrime in the last two years.
2. 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.

i. 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.

ii. 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.

iii. 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.

iv. Reported cases of cases of spam, hacking and fraud have multiplied 50-fold from 2004 to 2007, it claims [12].

3. One recent report ranked India in 2008 as the fourteenth country in the world hosting phishing websites [13]. Additionally, the booming of call centers in India has generated a niche for cyber criminal activity in harvesting data, the report maintained.

4.The words of Prasun Sonwalkar [14] 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 [15] 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 [16].

The major cyber crimes reported, in India, are denial of services, defacement of websites, SPAM, computer virus and worms, pornography, cyber squatting, cyber stalking and phishing. [l]Given the fact that nearly $ 120 million worth of mobiles are being lost or stolen in the country every year, the users have to protect information, contact details and telephone numbers as these could be misused. Nearly 69 per cent of information theft is carried out by current and ex-employees and 31 per cent by hackers. India has to go a long way in protecting the vital information. [3 The Hindu, Saturday, Oct 27, 2007].

Symantec shares the numbers from its first systematic survey carried out on the Indian Net Security scene: The country has the highest ratio in the world (76 per cent) of outgoing spam or junk mail, to legitimate e-mail traffic. India's home PC owners are the most targeted sector of its 37.7 million Internet users: Over 86 percent of all attacks, mostly via 'bots' were aimed at lay surfers with Mumbai and Delhi emerging as the top two cities for such vulnerability.

Many of the African countries are lack of the cyber policies and laws (many articles and news are available at [17] 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 India, US, Europe, Asia and Africa to show the horrible situation of cyber crimes.

## III. TYPES OF CYBER CRIME

### Theft of Telecommunications Services

The "phone phreakers" of three decades ago set a precedent for what has become a major criminal industry. By gaining access to an organization's telephone switchboard (PBX) individuals or criminal organizations can obtain access to dial-in/dial-out circuits and then make their own calls or sell call time to third parties (Gold 1999). Offenders may gain access to the switchboard by impersonating a technician, by fraudulently obtaining an employee's access code, or by using software available on the internet. Some sophisticated offenders loop between PBX systems to evade detection. Additional

forms of service theft include capturing "calling card" details and on-selling calls charged to the calling card account, and counterfeiting or illicit reprogramming of stored value telephone cards [2].

## Communications in furtherance of criminal

## On spiracies

Just as legitimate organizations in the private and public sectors rely upon information systems for communications and record keeping, so too are the activities of criminal organizations enhanced by technology. There is evidence of telecommunications equipment being used to facilitate organized drug trafficking, gambling, prostitution, money laundering, child pornography and trade in weapons (in those jurisdictions where such activities are illegal). The use of encryption technology may place criminal communications beyond the reach of law enforcement. The use of computer networks to produce and distribute child pornography has become the subject of increasing attention. Today, these materials can be imported across national borders at the speed of light (Grant, David and Grabosky 1997). The more overt manifestations of internet child pornography entail a modest degree of organization, as required by the infrastructure of IRC and WWW, but the activity appears largely confined to individuals.

## Telecommunications Piracy

Digital technology permits perfect reproduction and easy dissemination of print, graphics, sound, and multimedia combinations. The temptation to reproduce copyrighted material for personal use, for sale at a lower price, or indeed, for free distribution, has proven irresistible to many. This has caused considerable concern to owners of copyrighted material. Each year, it has been estimated that losses of between US$15 and US$17 billion are sustained by industry by reason of copyright infringement (United States, Information Infrastructure Task Force 1995, 131).When creators of a work, in whatever medium, are unable to profit from their creations, there can be a chilling effect on creative effort generally, in addition to financial loss.

## Dissemination of Offensive Materials

Content considered by some to be objectionable exists in abundance in cyberspace. This includes, among much else, sexually explicit materials, racist propaganda, and instructions for the fabrication of incendiary and explosive devices. Telecommunications systems can also be used for harassing, threatening or intrusive communications, from the traditional obscene telephone call to its contemporary manifestation in "cyber-stalking", in which persistent messages are sent to an unwilling recipient.

## Electronic Money Laundering and Tax Evasion

For some time now, electronic funds transfers have assisted in concealing and in moving the proceeds of crime. Emerging technologies will greatly assist in concealing the origin of ill-gotten gains. Legitimately derived income may also be more easily concealed from taxation authorities. Large financial institutions will no longer be the only ones with the ability to achieve electronic funds transfers transiting numerous jurisdictions at the speed of light. The development of informal banking institutions and parallel banking systems may permit central bank supervision to be bypassed, but can also facilitate the evasion of cash transaction reporting requirements in those nations which have them. Traditional underground banks, which have flourished in Asian countries for centuries, will enjoy even greater capacity through the use of telecommunications.

## Electronic Vandalism, Terrorism and Extortion

As never before, western industrial society is dependent upon complex data processing and telecommunications systems. Damage to, or interference with, any of these systems can lead to catastrophic consequences. Whether motivated by curiosity or vindictiveness electronic intruders cause inconvenience at best, and have the potential for inflicting massive harm (Hundley and Anderson 1995, Schwartau 1994).

## Sales and Investment Fraud

As electronic commerce becomes more prevalent, the application of digital technology to fraudulent endeavors will be that much greater. The use of the telephone for fraudulent sales pitches, deceptive charitable solicitations, or bogus investment overtures is increasingly common. Cyberspace now abounds with a wide variety of investment opportunities, from traditional securities such as stocks and bonds, to more exotic opportunities such as coconut farming, the sale and leaseback of automatic teller machines, and worldwide telephone lotteries (Cella and Stark 1997 837-844). Indeed, the digital age has been accompanied by unprecedented opportunities for misinformation. Fraudsters now enjoy direct access to millions of prospective victims around the world, instantaneously and at minimal cost.

### Illegal Interception of Telecommunications

Developments in telecommunications provide new opportunities for electronic eavesdropping. From activities as time-honored as surveillance of an unfaithful spouse, to the newest forms of political and industrial espionage, telecommunications interception has increasing applications. Here again, technological developments create new vulnerabilities. The electromagnetic signals emitted by a computer may themselves be intercepted. Cables may act as broadcast antennas. Existing law does not prevent the remote monitoring of computer radiation.

### Electronic Funds Transfer Fraud

Electronic funds transfer systems have begun to proliferate, and so has the risk that such transactions may be intercepted and diverted. Valid credit card numbers can be intercepted electronically, as well as physically; the digital information stored on a card can be counterfeited. Just as an armed robber might steal an automobile to facilitate a quick getaway, so too can one steal telecommunications services and use them for purposes of vandalism, fraud, or in furtherance of a criminal conspiracy.[1] Computer-related crime may be compound in nature, combining two or more of the generic forms outlined above.

## IV. IMPACT OF CYBER CRIME

### Crime as an Evil Factor of Society

Despite crimeless society is myth, crime is omnipresent phenomenon, and it is non-separable part of social existence, one may get irritate by the question, *'Why there is too much ado about crime?'*No one can deny that crime is a social phenomenon, it is omnipresent, and there is nothing new in crime as it is one of the characteristic features of the all societies existed so far, may it be civilized or uncivilized, and it is one of the basic instincts of all human behavior! However, it should bear in mind that the social concern for high crime rate is not because of its nature, but due to potential disturbance it causes to the society. In addition, some individuals are victims of crime in a more specific sense. The victims of crime may lose anything that has value. Safety, peace, money, and property are perhaps basic values, because they contribute to the satisfaction of many wishes.

### Impact of Cyber Crime over Socio-Eco-Political Riders

Conceptually, crime is a dynamic and relative phenomenon and subjected to the relative socio-political & economical changes occurring in existing system of society. Therefore, neither all-time suitable comprehensive definition encompassing all aspects of ‘crime’ is possible at any moment of time nor can a single definition be made applicable to different society. With its dynamicity, it is influenced by the changes occurring in the correlated phenomenon and value system generated by these changes. As evident in present scenario where money is more valuable than values, a definite hike in the corruption related offences are observed where social morality is low which influence the commission of crime attached less social stigma than ever before. Incidentally economic crime is on its peak. This clearly reflects that crime has its interdependency with other social phenomenon, economic systems and political machineries. Also, the population is one of the important factors influencing incidences of crimes. A positive correlation between the growth in incidences of crime and the population of the country has been observed. Besides population, the other factors influencing the crime are such as situation at a particular place, rate of urbanization, migration of population from

neighboring places, unemployment, income inequality, [computer literacy in case of Cyber crime] etc.[2] At the same time, the economic structure of give society is also influence the economic crimes. As every controlling systems for crime has much to do with the political system which prescribe norms, make rules, create preventive measure, the political structure and system also influence the crime in given society. This clearly demonstrates that every definition of crime has correlation with the socio-economical and political factors.

## Impact of Cyber Crime over Teenager

These days a worst fear in teenager's eyes is Cyber Bullying. It is become common over past five years, generally from the age below eighteen are more susceptible and feared from Cyber Bullying as per inspection. It is becoming an alarming trend in our society. As per inspection of data, the worst fear of cyber crime is on teenagers female. Cyber Bullying is a fear when person receives threats, negative comments or negative pictures or comments from other person.

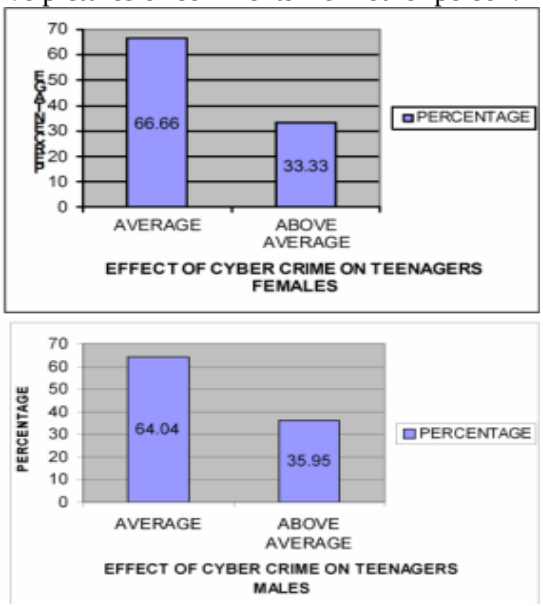


**Fig: 1** Effect of cybercrime

This is all done through core technologies described above mainly via online. Cyber Bulling can be done through chatting, instant messaging etc. Where website like Facebook, Orkut, Twitter user are more affected from Cyber Bullying. In my analysis generally feared person can reach a limit of depression, humiliation and threatens. Through this analysis we come to analyze that if person Bulled online he or she may be depressed up to the level of self harming.

## Impact of Cyber Crime over Private Industry

Having to use three attributes to describe cybercrime I would use the words intrusive, silent and dangerous. Just the silent mode of this type of crimes is a major problem in combating the threat, in fact, very often the companies realize that they have been victims of frauds or attacks until long after the event occurred. The consequences are disarming and retrieve the situation is sometimes impossible, precisely the time gap between the criminal event and its discovery provides an advantage to those who commit crimes often unbridgeable that makes impossible any action of persecution. But we are assuming that the event is discovered by the victims and this is not always true, many companies are in fact over the years are victims of cybercrime, but they are not aware, a cancer that destroys from within.

According the report "Second Annual Cost of Cyber Crime Study – Benchmark Study of U.S. Companies" published by the Ponemon Institute, a study is based on a representative sample of 50 larger-sized organizations in various industry sectors, despite the high level of awareness of the cyber threat the impact of cybercrime has serious financial consequences for businesses and government institutions. The report shows that the median annualized cost of cybercrime for 50 organizations is $5.9 million per year, with a range of $1.5 million to $36.5 million each year per company. The total cost is increased if compared to the first study of the previous year.

The following chart demonstrate that virtually all companies experienced attacks moved using malware, very interesting also the data related to the action made by the insider and the damages caused by social engineering attacks. The conclusion is that industries fall victim to cybercrime, but to different degrees and with different economic impact. Defense, utilities and energy, and financial service companies experience higher costs than organizations in retail, hospitality and consumer products.

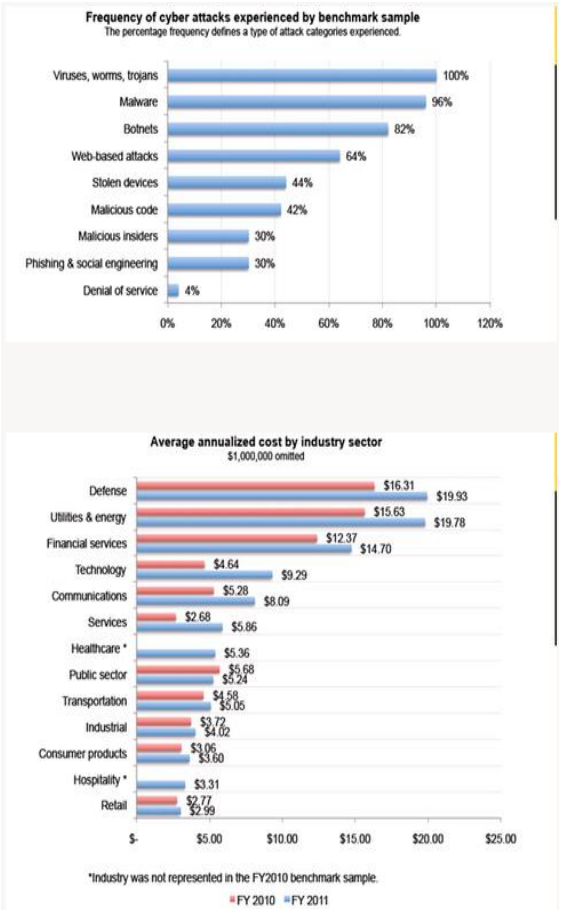


**Fig: 2** Average cost for cyber crime by Industry Sector

The data provided give a clear situation regarding the impact of the cybercrime on the business of large size companies, however a significant impact is observed on the small business where the companies face the cyber threats with fewer resources and accepting the risks related to exposure. In this market segment cybercrime is very fierce and daily it tries to elude helpless companies that often fail to meet the cyber threat, the related damages are devastating causing in many situations the end of the business. In this sector is desirable for governments to support small businesses in harmony with a cyber strategy defined at the national level. Leave helpless the social fabric made up of small businesses has definitely a direct impact also on the business of large firms.

## Impact of Cyber Crime over Consumer Behavior

The information revolution, coupled with the strategic leveraging of the Internet, has exposed a number of relatively open societies to the dangers of cybercriminal and cyber terrorist acts, especially in commercial business transactions. With the development of e-commerce, this commercial dark side has become known as cybercrime and has taken on many forms that affect the perceptions of the way we shop online. Corporations should realize that these threats to their online businesses have strategic implications to their business future and take proper measures to ensure that these threats are eliminated or significantly reduced so that consumer confidence in the Internet as an alternative means of shopping is maintained. These counter measures, coined as cyber security, have been developed to ensure the safety of consumer privacy and information and allow for a carefree shopping

experience. There is need for the development of models that will allow corporations to study the effects of cybercrime on online consumer confidence and to counter through leveraging the benefits associated with the latest developments in cyber security. With these two facets of e-commerce impacting the online consumer, corporations must ensure that the security measures taken will ultimately prevail to assure that consumers will continue to use the Internet to satisfy their shopping needs.

## Emotional Impact of Cyber Crime

The first study to examine the emotional impact of cybercrime, it shows that victims' strongest reactions are feeling angry (58%), annoyed (51%) and cheated (40%), and in many cases, they blame themselves for being attacked. Only 3% don't think it will happen to them, and nearly 80% do not expect cybercriminals to be brought to justice— resulting in an ironic reluctance to take action and a sense of helplessness."We accept cybercrime because of a 'learned helplessness'," said Joseph LaBrie, PhD, associate professor of psychology at Loyola Marymount University. "It's like getting ripped off at a garage – if you don't know enough about cars, you don't argue with the mechanic.
People just accept a situation, even if it feels bad."Despite the emotional burden, the universal threat, and incidents of cybercrime, people still aren't changing their behaviors - with only half (51%) of adults saying they would change their behavior if they became a victim
Cybercrime victim Todd Vinson of Chicago explained, "I was emotionally and financially unprepared because I never thought I would be a victim of such a crime. I felt violated, as if someone had actually come inside my home to gather this information, and as if my entire family was exposed to this criminal act. Now I can't help but wonder if other information has been illegally acquired and just sitting in the wrong people's hands, waiting for an opportunity to be used."
The "human impact" aspect of the report delves further into the little crimes or white lies consumers perpetrate against friends, family, loved ones and businesses. Nearly half of respondents think it's legal to download a single music track, album or movie without paying. Twenty-four percent believe it's legal or perfectly okay to secretly view someone else's e-mails or browser history. Some of these behaviors, such as downloading files, open people up to additional security threats.

## Impact of Cyber Crime over Business

According to the FBI and the Department of Justice, cyber-crime is on the rise among American businesses, and it is costing them dearly. Cyber-crime includes a myriad of devious criminal practices designed to breach a company's computer security. The purpose of the electronic break and enter can be to steal the financial information of the business or its customers, to deny service to the company website or to install a virus that monitors a company's online activity in the future.

## The-Cost-Of-Protection

Companies that want to protect themselves from online thieves have to pull out their wallets to do it. There are costs in identifying risks, building new and safer operating procedures, and buying protective software and hardware. For businesses with complex or sensitive operations, this often involves hiring a cyber-security consultant to develop a customized solution. Not only are the upfront costs of protection expensive, but the systems must be tested and monitored regularly to ensure that they are still effective against emerging cyber-attacks. These costs are often passed on to the customer through higher prices of goods and services.

## Lost-Sales

Cyber-crime isn't just for thieves anymore. A new subculture has emerged in the past few years: the cyber-activist. These are the online equivalents of protesters who chain themselves to buildings or trees. Their purpose is to shut down a company's online operations to send a message about the company's business practices. In the past two years, major corporations, such as PayPal and MasterCard, have been attacked in this way. In December 2010, the PayPal website was attacked by dozens of people claiming to be part of the group, Anonymous. They attempted to perpetrate a denial of service attack in retaliation for PayPal shutting down payment services to Wiki Leaks. More than a dozen hackers were arrested in that crime.

While PayPal did not experience a full shutdown, many other businesses aren't so lucky. A denial of service attack results in fewer sales as customers cannot access the company's online store. It can even

result in less revenue in the long-term if some customers decide to no longer do business with a company vulnerable to attack.

### Impact of Cyber Crime over Youth

Cyber communication is society's newest way to interact. Online social networking websites, text messages and emails provide users with an effective, quick way to communicate with people all over the world. Teens in particular spend hours online every day, on computers or personal electronic devices.

### Friendships

Family-rescource.com states that 48 percent of teens believe the Internet improves their friendships. With social networking sites becoming increasingly popular, youth are able to stay connected to real and online friends. Some teens believe cyber connections help them feel confident to be their true selves. Instant messaging programs, used by an estimated 13 million teens, allow conversations with friends to occur in real time. Online communication tools open the door for friendships with other teens near and far.

### Writing

While teens are frequently online, using cyber forms of communication doesn't require formal writing skills. Quite the opposite actually occurs; youths often use shorthand, abbreviations or slang when writing online. The National Commission on Writing states that 85 percent of teens use social networking communication, but 60 percent of them don't see this form of communication as "writing." Teens should be aware of the difference between formal and informal writing, and understand when the latter is not appropriate (in school).

### Cyber Bullying

Cyber bullying is a negative effect of online communication between youth. Victims of cyber bullying often experience rumors and lies spread on online social networks. Bullies may post inappropriate or embarrassing pictures of their victims. Another aspect of cyber bullying involves using mean text messages as harassment. The National Crime Prevention Council states that cyber bullying is a problem for almost half of American teens. In some extreme cases, teens have taken their own lives as a result of cyber bullying.

### Sexual Solicitation

Sexual solicitation is a growing concern for youth who use forms of cyber communication. It may occur in chat rooms or on social networking sites. Sexual solicitation occurs when an adult or peer tries to engage in an online sexual relationship. A teen may be asked to disclose personal information, view pornography or discuss something sexual online. About 70 percent of teens who are sexually solicited online are girls. Teens should be cautious in posting suggestive photos online and talking to strangers in chat rooms.

## V. FUTURE TRENDS IN CYBER CRIME

The pace at which cybercrime is growing is one of the most disturbing trends. Valerie McNiven, a U.S. Treasury Advisor, has proclaimed “Last year was the first year that proceeds from cybercrime were greater than proceeds from the sale of illegal drugs, and that was, I believe, over $105 billion." She further added that "cybercrime is moving at such a high speed that law enforcement cannot catch up with it.”iii It seems clear that the issue will only become worse in the next few years, now that professionals have realized the potential windfalls if exploited properly.

Recently, there has been significant discussion over the amalgamation of organized criminals and cybercrime. Such a pairing indeed forebodes an ill omen for the near term future. With most of the criminal groups operating out of Eastern Europe, Russia and Asia, where laws and enforcement are scanty, there seems little hope in containing and neutralizing the threat through traditional means. Phil Williams, a visiting scientist at CERT, summarized the issue succinctly. “The Internet provides both

channels and targets for crime and enables them to be exploited for considerable gain with a very low level of risk. For organized crime it is difficult to ask for more."

The result that can then be expected will be an increase in sophisticated phishing attacks and other means for identity theft that may be two pronged. For example, using call centers to notify "customers" ahead of time of some issue, and then following up with emails that request personal information. The aggregation of personal information in many third party data centers will prove to be valuable targets to infiltrate. It is not hard to imagine criminals using data mining techniques to find the most gullible consumers, or tailoring phishing emails for specific people based on their medical, financial or personal history. Identify theft will also move in more automated directions. For example, botnets will become vehicles not just for denial of service attacks and spam, but also as giant search platforms for finding personal information, like credit cards and social security numbers. Controllers of the botnets will then receive payment to run queries on their "database."

With professional criminals managing the money laundering and organization of such schemes, it begs to ask where all the technical know-how will come from in order to perform cybercrime. Unfortunately, there are growing numbers of intelligent black-hats with university degrees spread around the globe, many of them operating in countries where legal employment does not pay as well and the chances of being caught are slim. But more troublesome is that it has become easier than ever before to be a hacker capable of inflicting great harm on networks and committing cybercrime. The Internet has created a repository of knowledge where anyone is able to learn the fundamentals of subverting computer systems, with numerous tutorials available that spell out in nearly layman's terms how to perform a buffer overflow or a man in the middle attack. Interestingly, the greatest problem is not those who will take the time to learn and find new exploits. In fact this group will probably remain a small, highly intelligent network of researchers and security groups focused solely on finding holes in software. In this, it is preordained, that even if someone is motivated to learn how exploits work, finding a new exploit takes a degree of investigation, skill and diligence that most are not willing to invest. The real threat comes from the profound ease at which anyone can run a program like "MetaSploit," a framework for running exploits against targets that allows new modules to be imported and run automatically. The attacker literally needs to know nothing about how computers work, besides how to operate one. In fact, for almost all attacks, the hard work is done by a small group of people, and then released into the public domain, allowing almost anyone to just run the attack. Botnets are no longer hand-crafted software made by one group who truly understood the fundamentals, but instead are open-source collaborative efforts that aim to make it as easy as possible to control remote computers, such as BotNET, eggheads and CSharpBot, all available from Source Forge.

Thus, the barrier to entry to the field is so low that it allows almost anyone to experiment and join the swelling ranks of cybercriminals. With the learning curve so low, it should prompt discussion on the need for a new paradigm of thought in how to preempt and deal with criminals, in a way that is no longer tied to traditional methods. For example, for someone to break into a house, not only do they need to plan the opportune moment, but they may also have to be aware of lock picking, security system evasion and possess a degree of gumption to overcome moral thresholds. In opposition, the ease of cybercrime seems inversely proportional to the lucrativeness that it bestows and moreover, these trends show signs of accelerating.

## VI. CONCLUSION

The future of the Internet is still up for grabs between criminals and normal users. Fears of a cyber apocalypse still abound, while the potential extent of damage that can be caused by wide scale fraud is nearly unbounded. These anxieties should be rationally tempered with the knowledge that the problems are being addressed, although perhaps not fast enough. The usefulness of the Internet has proved itself in numerous and myriad ways that will hopefully be enough to ensure it does not become a wasteland of criminal activity and a bastion for the malicious. The government still has an important role to play, but most of the prevention needs to be done by commercial entities producing software and those with the ability to stop fraud. Relying on consumer education programs will only affect a percentage of possible victims. The others need to be automatically protected through measures that

do not stress and require considerable participation. Security needs to be easy and effective if it is doing work. Whether cybercrime is still a pertinent issue ten years from now is unknowable in a sense, but if the Internet will continue to grow, it must be solved so that the realities of cybercrime will be proportional to real-world crimes, if not better.

## REFERENCES

[1.] Wow Essay (2009), Top Lycos Networks, Available at: http://www.wowessays.com/ dbase/ab2/ nyr90.shtml, Visited: 28/01/2012.
[2.] Crime in the Digital Age by Peter Grabosky and Russell Smith, Sydney: Federation Press, 1998
[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: 28/01/201
[8.] Virus Glossary (2006), Virus Dissemination, Available at: http://www.virtualpune.com/citizen-centre/html/cyber_crime_glossary.shtml, Visited: 28/01/2012
[9.] Legal 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.