Hemraj Saini, Yerra Shankar Rao, T.C.Panda / International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com
Vol. 2, Issue 2,Mar-Apr 2012, pp.202-209

Cyber-Crimes and their Impacts: A Review

[1]Hemraj Saini
Associate Professor & Head, Department of Computer Science & Engineering
Alwar Institute of Engineering & Technology, MIA, Alwar-301030
Yerra Shankar Rao
PhD Student, Department of Mathematics
Shiksha 'O' Anusandhan University, Bhubaneswar-751030
T.C.Panda
Principal
Orissa Engineering College, Bhubaneswar-752050

Abstract
In the current era 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. Therefore, the current manuscript provides the understanding of cyber crimes and their impacts over society with the future trends of cyber crimes.
Keywords: Cyber Attacks, Cyber Crimes, Potential Economic Impact, Consumer trust, National Security.

I. Introduction
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." [1]. The Internet space or cyber space is growing very fast and as the cyber crimes. Some of the kinds of Cyber-criminals are mentioned as below.

- 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.
- 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.
- Pranksters: These individuals perpetrate tricks on others. They generally do not intend any particular or long-lasting harm.
- 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" [2].
- 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.

- 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.
- 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.

In general cyber crimes can be categorized as follows-

1.1. 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 [3].

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 [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.

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 [5].

1.2. 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 [6].

1.3. 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 [7].

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 [8].

1.4. 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" [9, 10].

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.

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]-

- 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 [12].
- 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.
- 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].

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 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.

II. 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 [32].

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.

2.1. 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! [18].

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 [14]. 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.

2.2. 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 [19]. 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" [20]. 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 [21]. 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 [19]. Some industry insiders confess that the rates for such plans are mostly set by guesswork [22]. As cited in [19]: "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 [22] 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 [21]. 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 [23].
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 [24], and fear of negative publicity [23]. Companies are also wary of competitors exploiting these attacks to gain competitive advantage [23].
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 [25].

Risk assessment can be performed using traditional accounting based measures such as the Return on Investment (ROI) approach [26]. 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 [27]. In addition, potential intangible losses such as "loss of competitive advantage" that result from the breach and loss of reputation [28] 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 [29]. 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.

2.3. 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 users' 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.

2.4. 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 [32]. 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.

III. Future Trends

One of the biggest concerns is what if there is a hack into the critical systems in government, companies, financial institutions etc. This could lead to malware in critical systems leading to data loss, misuse or even killing the critical systems. Since the communication flow is easy via the internet, the crime organizations might merge and cooperate even more than they are currently.

It is feared that due to enhanced mobility, funds and people could transfer easily. The Internet is increasingly likely to be used for money laundering. As the Internet becomes the medium through which more and more international trade takes place, the opportunities for laundering money through over-invoicing and under-invoicing are likely to grow. Online auctions offer similar opportunities to move money through apparently legitimate purchases, but paying much more than goods are worth. Online gambling also makes it possible to move money especially to offshore financial centers.

Recruitment into crime agencies over internet will be easier than before. Secret messages can be transferred over the internet to a large group of people very easily without being conspicuous.

Because much of the information technology companies are privately owned, the focus would be on making customer happy as opposed to worry about the transnational crime. In addition, legitimate civil liberties could be argued in favor of not monitoring the information technology. All of these things make it more difficult to deal with cyber-crime.

Some of the future trends predicted by Stephen Northcutt & Friends [33] are briefly summarized in the followed text.

Improved Social Engineering Attacks will be the trend for the coming era. Attackers will increasingly make use of social-engineering tactics to bypass technological security controls, fine-tuning their techniques to exploit natural human predispositions. This will bring us closer to merging the line between external and internal threat agents, because social engineering will allow external attackers to quickly gain an internal vantage point despite traditional perimeter security measures.

Social Media will provide the platform for the cyber crimes. More organizations will adopt social media as a core aspect of their marketing strategy. They will struggle to balance the need to be active as part of on-line social communities while balancing compliance and litigation risks associated with such activities. Similarly, organizations will have a hard time controlling online social networking activities of their users. Attackers will continue to take advantage of the still-evolving understanding of online social networking safety practices to defraud people and organizations. Security vendors will position their products as solving all these problems; some of them will stand out by allowing organizations to granularly control and monitor on-line social networking activities, while being mindful of users' privacy expectations.

Humans are the weakest link, regardless of how technology changes attackers know they can always hack employees. In the year 2012 and 2013 these human attacks will only grow in sophistication and numbers. Cyber attackers will always take the path of least resistance. Organizations and management will finally start doing something about it to secure the human.

It’s the sensitive issue for the people relying on iPhones for their day today working that without issuing a dire warning that some worm will eat all the iPhones and convert the Androids to bricks. However, the biggest issue seems to be apps with spyware. Even the apps that come loaded on the phone are likely to phone home, it is a sure thing with 3rd party apps. AT&T has proved they cannot be trusted by signing their customers up for Asurion road side assistance without even asking them. And it matters big time.

Memory Scraping Will Become More Common in the coming time. This has been around for a long time, but is more aggressively targeting data such as credit card records, passwords, PIN's, keys, as of late. The reason they are successful is that they get around PCI/GLBA/HIPAA/ETC security requirements that data must be encrypted while in transit and at rest. Data in transit is decrypted on the system and often stored in memory during the lifetime of a process, or at least during a decryption routine. Depending on how a process cleans up after itself, it may stay resident even after the fact. The data is encrypted on the hard disk, but again, the RAM likely maintains the clear-

text version of the data. Browsers are notorious for leaving things sitting around in memory during web sessions. The RAM Scraping malware also targets encryption keys in memory to decrypt anything for session data to encrypted files. As far as the emerging security threat part, we are seeing RAM scraping more commonly now as attackers focus on client-side attacks, shifting away from server-side attacks. Browsers are often misconfigured, allowing malware to get onto a user's system, stealing credit card data and passwords. They are mostly an annoyance where if a customer or fraud department detects fraudulent transactions, the account must be credited and changed. This requires the banks to write-off these transactions, which can add up quickly. AV products can't keep up with the aggressive rate and polymorphic characteristics of this type of malware. We discover a ton of new malware every week, reverse it to some extent, and send the details to AV vendors to be added as a new signature. The other emerging component is the threat of RAM scraping malware targeting Point Of Sale (POS) systems.

Wireless adoption will continue, branching out into a larger number of purpose-focused protocols that fit the needs of individual technology. Wi-Fi technology will continue to grow, but other protocols will also emerge with widespread adoption suiting the needs of embedded technology with a variety of focus areas including ZigBee, WirelessHART and Z-Wave, as well as proprietary protocols. With this growing alternate wireless adoption, we're already seeing some of the past mistakes from earlier failed protocols repeated. Based on this exposure, and the trend of Wi-Fi failure and improvement, we'll see history repeating itself where vendors are quick to the market to capitalize on new opportunities, failing to critically examine the lessons from earlier wireless technologies.

More Cloud Computing Issues will be at the eye of the cyber attackers. While there are many possible benefits to Cloud Computing, the honeymoon will end. Many organizations will soon discover that they do not have the flexibility they need for their businesses, and many others will discover that any security issues (from audit to compromise) are far more complex in the cloud. Many security professionals will come to terms with security risks of cloud computing. They will do so under pressure from the businesses they support, as companies will continue to migrate to cloud platforms. The infosec community will better understand cloud environments, while the technologies implementing cloud platforms will reach an acceptable level of maturity. Security professionals will continue to apply extra scrutiny to scenarios that involve processing sensitive or regulated data in shared cloud environments.

Security Continues to become part of Virtual Infrastructure. As more and more organizations add virtualization technologies into their environment, particularly server and desktop virtualization, security will be more embedded in the native technologies, and less of an "add-on" after the implementation is complete. For server virtualization, new firewalls and monitoring capabilities are being integrated into some of the leading platforms now. For desktop virtualization, native integration with remote access technologies and client-side sandbox capabilities are common. Vendors will continue to push the envelope and offer new tools to enhance virtual environments, but virtualization platforms will evolve to easily allow existing security technologies to interoperate more natively, as well. In addition, security architecture design will be a "must have" element of virtual infrastructure planning and deployment, not a "nice to have".

IV. Conclusion

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.

The way to overcome these crimes can broadly be classified into three categories: Cyber Laws (referred as Cyber laws), Education and Policy making. All the above ways to handle cyber crimes either are having very less significant work or having nothing in many of the countries. This lack of work requires to improve the existing work or to set new paradigms for controlling the cyber attacks.

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.