Page 146 - 160 **DOI:** *https://doij.org/10.10000/IJLMH.114816*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 6 | Issue 3

2023

Cyber-Crime and Their Impacts

KUSHAGRA VIKRAM[1] AND PRERNA TIWARY[2]

ABSTRACT

There is a need for an understanding of cybercrimes and their impact on society, along with their future trends, in the current manuscript. It is the goal of the present manuscript to provide an understanding of cybercrimes and their impact on society, along with their future trends in the coming years. I would like to provide a brief overview of cybercrimes and the impact they have on society as well as their future direction in this manuscript. In the present manuscript, we present a concise overview of the state of cybercrime, along with an understanding of its impact on society and its future prospects. As part of the current manuscript, we provide an understanding of cybercrimes and their impact on society, as well as how they will unfold in the future. A description of cybercrimes and their impact on society, together with their future trends, is provided in the current manuscript. This paper provides a comprehensive understanding of cybercrime and its impact on society, as well as their future trends, through the presentation of the existing manuscript. I am currently working on a manuscript that is focusing on cybercrimes and their impact on society, as well as their future trends. It provides an insight into the following: cybercrimes and how they affect society as well as their potential future trends, as well as the impact they have on society as a whole. Despite the fact that cybercrimes have been a ubiquitous part of society for a long time, it is challenging to understand their impact on society, as well as their likely future trends.

Keywords: *Data Theft, Network Crime.*

I. INTRODUCTION

The term cybercrime can be defined as an act committed or omitted in violation of a law that prohibits or mandates it and for which a penalty will be imposed if convicted. Other words represent cybercrime as “criminal activities directly related to the use of computers, including but not limited to breaking into another's computer system or database, tampering with or theft of skenyatored or online data, or sabotage of devices and Data". [1]. The internet space or cyberspace is growing very fast and so is cybercrime. Some of the types of cyber criminals are mentioned below.

Individuals who aim to cause losses to satisfy antisocial or fun reasons are known as crackers.

[1] Author is an Assistant Professor at Jharkhand Rai University, Ranchi, India.
[2] Author is an Assistant Professor at Jharkhand Rai University, Ranchi, India.

 [ISSN 2581-5369]

There are numerous individuals who make and distribute computer viruses. Individuals who are hackers usually seek to learn about other people's computer systems in order to gain a competitive edge or to build a reputation as an expert. They may also be interested in acquiring a more powerful computer or gaining the respect of their peers. A prankster is someone who indulges in performing tricks on others, though they do not intend any long-term harm. Career criminals, these people earn some or all of the proceeds of crime despite being malcontents, drug addicts, and irrational, incompetent people: they work, earn, and steal money, and then change their minds to repeat the process. In some cases, they collude with others or work in organized gangs such as the Mafia. The biggest organized crime threats come from groups in Russia, Italy and Asia. "The FBI reported in 1995 that there were over 30 Russian gangs operating in the United States. According to the FBI, many of these unsavory alliances use advanced computer technology and encrypted communications to evade capture. Cyberterrorism, this crime can take many different forms. Sometimes a clever hacker breaks into a government website; other times, a horde of like-minded Internet users overwhelm a website with traffic to cause it to crash. No matter how innocent it may appear to be, it is still prohibited to engage in criminal negligence when you are dependent on drugs, drink, competition, or attention from others. Cyberbulls, any harassment that takes place online is considered cyberbullying. Cyberbullying can take many different forms, including abusive forum posts, name-calling in chat rooms, creating fictitious profiles on websites, and harsh email communications.

Attackers who utilise salamis, these assaults are carried out in order to commit financial crimes. The trick here is to make the change so minor that it would go completely undiscovered in a single instance, such as when a bank employee uploads a software into the bank's servers that automatically deducts a small sum from each customer's account.

Types of cybercrime Cybercrimes may generally be divided into the following categories:

Data theft: This involves stealing sensitive information, such as personal information, financial data, or intellectual property, through unauthorized access to computer systems or networks. Hackers can use various methods to gain access to the data, such as malware, phishing, or social engineering techniques. Data manipulation it involves unauthorized changes or alterations to data, such as modifying financial records, changing medical records, or tampering with election results. This can have serious consequences for individuals, organizations, and even governments. Data destruction it involves intentionally deleting or destroying data, either to prevent others from accessing it or to cause harm. This can include deleting important files, crashing computer systems, or corrupting data backups. Ransomware attacks it involves

 [ISSN 2581-5369]

encrypting a victim's data and demanding a ransom payment in exchange for the decryption key. If the ransom is not paid, the attacker may threaten to delete or publish the data. Insider threats it involves employees, contractors, or other individuals with authorized access to data using their privileges to steal or manipulate data for personal gain or to harm an organization. Botnets it involves using networks of infected computers to perform malicious activities, such as stealing data or launching DDoS attacks.

Network crimes, also known as cybercrimes, are criminal activities that are committed using computer networks or the internet. These types of crimes typically involve the unauthorized access, manipulation, or destruction of network infrastructure, computer systems, or data. Network crimes can cause significant damage to individuals, organizations, and even entire governments. Hacking which involves gaining unauthorized access to computer systems or networks, often through exploiting vulnerabilities in the system. Once inside, hackers can steal sensitive data, install malware, or cause damage to the system. Phishing which involves sending fraudulent emails or messages that appear to be from a reputable source in order to trick people into providing sensitive information, such as login credentials or credit card numbers. Distributed Denial of Service (DDoS) attacks which involves overwhelming a website or network with traffic in order to make it unavailable to users. Malware which refers to a range of malicious software programs, including viruses, worms, and Trojans, that are designed to infiltrate computer systems or networks in order to steal data or cause damage. Ransomware it involves encrypting a victim's data and demanding a ransom payment in exchange for the decryption key. If the ransom is not paid, the attacker may threaten to delete or publish the data.

Botnets which involve using networks of infected computers to perform malicious activities, such as stealing data or launching DDoS attacks. Insider threats which involve employees, contractors, or other individuals with authorized access to computer systems or networks using their privileges to steal or manipulate data for personal gain or to harm an organization. Network crimes can have serious consequences, including financial losses, reputation damage, and even legal action. It is essential for individuals and organizations to take steps to protect themselves from these threats, such as using strong passwords, keeping software up-to-date, and regularly backing up data.

Access crime refers to criminal activities that involve unauthorized access to computer systems, networks, or data. These types of crimes can have serious consequences for individuals, businesses, and governments. Hacking involving gaining unauthorized access to computer systems or networks, often through exploiting vulnerabilities in the system. Once inside, hackers can steal sensitive data, install malware, or cause damage to the system. Identity theft

 [ISSN 2581-5369]

involving stealing someone's personal information, such as their name, address, Social Security number, or credit card number, in order to gain unauthorized access to computer systems, networks, or data. Password cracking involving using software to guess or crack passwords in order to gain access to computer systems or networks. Social engineering involving using deception or manipulation to trick people into providing sensitive information or access to computer systems or networks. Insider threats which involve employees, contractors, or other individuals with authorized access to computer systems or networks using their privileges to steal or manipulate data for personal gain or to harm an organization. Physical access which includes gaining physical access to a computer system or network, such as by stealing a laptop or using an unsecured network port. Access crimes can have serious consequences, including financial losses, reputation damage, and legal action. It is essential for individuals and organizations to take steps to protect themselves from these threats, such as using strong passwords, implementing multi-factor authentication, and limiting access to sensitive data and systems to only those who need it. Additionally, regular security training for employees can help prevent social engineering attacks and insider threats

Aiding and Complicity in Cybercrimes, in which most allegations of assisting and abetting against a person have three components. The first is that the crime was perpetrated by another individual. Second, the accused person knew about the offence or the perpetrators' intentions. Finally, the person gave the principal some kind of support. In legal terminology, an accessory is often described as a person who helps another or others commit a crime. A person accused of being an accessory or aiding and abetting usually had knowledge of the crime before or after it occurred. a person who provides assistance to those doing the crime while being aware of it before it happens. its referred to as a "accessory before the fact" in legal terminology. He or she could offer support in the form of suggestions, deeds, or money. An "accessory after the fact" is a person who is not aware of the crime before it occurs but assists in its investigation and prosecution.

Computer-Related Forgery and Fraud, Computer-related offences include both computer forgery and computer-related fraud. Content-Related Crimes: These violations include cybersex, unsolicited commercial messages, cyber defamation, and cyber threats. Millions of millions of dollars are spent annually by victims of these attacks, which is a considerable sum that might transform underdeveloped or developing nations into developed nations. The material offered by a US base news agency can considerably mark several of the cybercrime-related facts. Regarding online identity theft, phishing and malware, data breaches and data loss, RSA, the security subsidiary of EMC, has published its Quarterly Security Statistical Review.

 [ISSN 2581-5369]

The analysis discovered that while online sites are infected on average every 4.5 seconds, just 23% of individuals globally will fall for spear phishing attempts. Consumers are becoming more concerned about their online safety, according to the review. According to the Identity Theft Resource Centre's 2009 Consumer Awareness Study in the US, 85% of respondents were concerned about the security of transferring information over the Internet, while 59% said that the protection of the data they submit to websites needs to be strengthened. According to a recent survey, India was the fourteenth-ranked nation hosting phishing websites in the globe in 2008 [2]. The research also claimed that the expansion of contact centres in India has created a market for data harvesting by cybercriminals.

According to Prasun Sonwalkar [3], "India is swiftly developing as a major hub of cybercrime since recession is driving computer-literate criminals to electronic frauds." This quote highlights the issue of cybercrime in India. The report, "Crime Online: Cyber Crime and Illegal Innovation," claims that cybercrime is a "leap in cybercrime" in India in recent years and is a "cause of special worry" in Brazil, China, Russia, and India. Computer spam is the term for unsolicited commercial e-mail that is disseminated online and may contain viruses and other harmful software. According to Warner, the UAB Spam Data Mine has examined millions of spam emails so far this year and related 69,117 different hosting domains to the hundreds of thousands of promoted Web sites in the spam. 48,552 (or 70%) of the total domains analysed had Internet domains or addresses that ended in the ".cn" country code for China. Nevertheless, 48,331 (or 70%) of the websites were hosted on Chinese machines [4]. A large number of African nations lack cyber laws and policies (many articles and news are available at [5] in this support). As a result, a cybercriminal may escape even after being apprehended. Cyber laws and rules are essentially non-existent in nations like Kenya, Nigeria, Tunisia, Tanzania, etc.

II. IMPACTS OF CYBERCRIME

On a blog entry from October 2005, Lunda Wright, a legal scholar at Rhodes University with a focus on digital forensic law, presents an intriguing study conclusion. It claims that the number of cybercriminals being prosecuted has grown. The crackdown on online piracy of works of music and movies has been tougher. There are innovative legal actions and litigation methods. In businesses and the government, there is a rising reliance on the expertise of computer forensic specialists. The level of intergovernmental cooperation has increased [17]. Major online fraud and theft are being carried out by organised crime gangs. Trends point to the involvement of organised crime in white-collar crime. Criminals are increasingly using the internet to commit crimes as they abandon more traditional techniques. Online stock fraud has brought in millions

 [ISSN 2581-5369]

of dollars every year for crooks, costing investors money, making it a profitable field for such crime.

Police agencies around the country confirm that they have been receiving more reports of these crimes in recent years. This is consistent with the general national trend brought on by rising computer use, internet commerce, and technologically advanced criminals. In 2004, cybercrime brought in more money than drug trafficking, and as digital use increases in underdeveloped nations, this trend is expected to continue. Denial-of-service assaults won't be the new trend in the future, according to Scott Borg, head of the U.S. Cyber Consequences Unit, an organisation funded by the U.S. Department of Homeland Security. In comparison to the potential for future attacks, worms and viruses are seen as "not quite mature."

(A) Economic impact

Over 74 million Americans were victims of cybercrime in 2010, according to the 2011 Norton Cybercrime Report. Direct financial damages from these illicit activities totaled $32 billion. 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 mindset that engaging in online commerce entails the risk of cybercrime. [6]. The likelihood of being a victim of cybercrime is great because modern consumers are so reliant on computers, networks, and the information they store and maintain. Up to 80% of the organisations examined, according to some previous polls, reported suffering financial losses as a result of computer intrusions. $450 million was the impacted amount roughly. Almost 10% of people [3] reported financial fraud. We learn of fresh attempts to compromise the availability, confidentiality, and integrity of computer systems every week. This could include denial-of-service attacks or the theft of personally identifiable information. The economy is more vulnerable to cybercriminals' attacks as a result of its growing reliance on the internet. Online trading of stocks, online bank transactions, and online credit card purchases are all commonplace. Every occurrence of fraud in such transactions has an effect on the economy and the financial health of the afflicted organisation. One of the significant effects that still warrants great worry is the potential disruption of global financial markets. The global and multi-time zone nature of the modern economy. A disturbance in one section of the world will have an impact on other regions due to the interconnection of the global economic system. Since the market is the root of the problem, any interruption of these processes would have an impact elsewhere. Also under danger is productivity. Worm, virus, and other attacks prevent the user from being productive. Machines may operate more slowly; servers may not be reachable; networks may be congested; and so on. Such assaults have an impact on both the user's and the

 [ISSN 2581-5369]

organization's overall productivity. Additionally, it affects customer service because the outside client perceives it as a flaw in the company. In addition, a sizable portion of online customers refrain from making purchases due to user worry over possible fraud. It is evident that consumer uncertainty, doubt, and concern account for a sizeable amount of lost e-commerce income. These kinds of consumer trust concerns merit more discussion since they may have major consequences.

(B) Impact on market value

Companies striving to allocate their information security budgets and insurance providers of cyber-risk policies are both interested in the economic effects of security breaches [7]. A decision in favour of Ingram Micro, for instance, noted that "physical damage is not restricted to physical destruction or harm of computer circuitry but includes loss of use and functionality" [8]. As more businesses rely on information technology in general and the Internet in particular to do business, this new and growing concept of harm becomes even more crucial. This precedent may require several insurance providers to pay out claims for losses brought on by cyber attacks and other security lapses. Companies regularly reevaluate the dangers to their IS environment as the features of security breaches evolve [9]. FUD—fear, uncertainty, and doubt—has historically been used by CIOs to sell IS security investments to upper management. Recently, a few insurance firms developed actuarial tables that, in their opinion, allow for the measurement of losses due to computer outages and hacker assaults. These figures, however, are in doubt primarily because there is a dearth of historical information [7]. The pricing for these programmes are mostly determined by guessing, according to some industry insiders [10]. According to [7] The $64,000 query is: Are we charging the correct premium for the exposure given the novelty of these insurance products? Improved return on security investment (ROSI) studies are required, according to industry experts. These studies could be used by insurance providers to develop "hacking insurance" with variable premiums based on the organization's level of security [10] and by the organisation to support investments in security prevention strategies. A thorough analysis of every component of the IS environment may be too expensive and unfeasible, depending on the scale of the business. Identification and assessment of security threats are made possible through IS risk assessment. A method of selecting controls based on the likelihood of loss is known as risk assessment.

The effect of an IS security breach and the cost to the organisation are concerns that are addressed by risk assessment in IS [9]. For the following reasons, calculating the financial damage from a prospective IS security breach is a challenging stage in the risk assessment procedure.

 [ISSN 2581-5369]

i. Many businesses find it difficult or impossible to estimate the financial losses brought on by security breaches [11].
ii. A lack of previous data. Unreported security breaches frequently occur. Companies are hesitant to reveal these violations because they are concerned about management humiliation, potential criminal activity, and bad press [23, 24]. Companies are also concerned that rivals may use these assaults as a means of gaining an edge over them [11].
iii. In addition, businesses can be concerned about the adverse financial effects of disclosing a security breach to the public. According to earlier studies, a public announcement of an event that is often viewed negatively would result in a decrease in the firm's stock price [12].

Traditional accounting-based metrics, such as the Return on Investment (ROI) method, may be used for risk assessment [13]. ROI, however, cannot be simply applied to investments in security. CIOs will need to (1) show proof that the costs of a potential IS security issue outweigh the capital investment required to acquire such a system and (2) prove the expectation that the IS security system's return on investment will be equal to or greater than that of competing capital investment opportunities in order to justify investment in IS security. This is challenging to do since, even if the security precautions are effective, there won't be many security events and no observable results. The lack of time and resources required to make an accurate assessment of financial loss also places restrictions on accounting-based metrics like ROI. Instead, organisations' IT resources are used to comprehend cutting-edge technology and stop upcoming security risks [14]. Additionally, because intangible costs are not easily quantifiable, possible intangible damages from the breach, such as "loss of competitive advantage" and "loss of reputation" [15], are not included. As a result, a new strategy is required to evaluate the risk of security breaches. Measuring the effect of a breach on a company's market value is one such strategy. The capital market's estimates of losses brought on by the security breach are captured via a market value method. This strategy is acceptable since public relations exposure frequently has a greater negative impact on businesses than the actual attack [16]. Additionally, managers engage in initiatives that either raise shareholder value or reduce the risk of loss of shareholder value in order to maximise a firm's market value. So, in this study, we choose to utilise market value as a proxy for the financial impact that security breach disclosures have on businesses.

(C) Impact of Consumer Trust

The end user accessing the relevant website will be irritated and deterred from using the stated site frequently since cyber attackers invade others' space and attempt to undermine the logic of

 [ISSN 2581-5369]

the page. The website in issue is referred to as bogus, but the criminal who planned the covert assault is not acknowledged as the main culprit. The client becomes less confident in the mentioned website, the internet, and its benefits as a result. Over 80% of online customers named security as their top concern when doing business online, according to surveys sponsored by the Better Business Bureau Online. When prompted for their credit card number during an online transaction, almost 75% of consumers give up. The idea that security risks and credit card theft are rampant on the Internet is spreading. This has been a significant issue for e-commerce. Consumer perceptions of fraud make the situation more complicated since they make the situation appear worse than it is. Consumer impression has equal power to reality and can be just as harmful. Because of this, many online buyers refrain from making purchases due to consumer fears about fraud. A customer is hesitant to make a purchase because they are concerned that an online business is hazardous or cluttered. Potential revenue is gravely jeopardised by even the smallest perception of a security risk or incompetent behaviour in the marketplace.

(D) Impact on National Security

The majority of nations' modern militaries rely largely on cutting-edge technology. IW, which includes network assault, exploitation, and defence, is not a new threat to national security, but it has taken on more significance in the wake of 9/11. IW has appeal since it may be inexpensive, very effective, and provide the attacker some level of denial. It may quickly propagate malware, bringing down networks and disseminating false information. Information warfare is undoubtedly ready for investigation because non-information warfare is being emphasised more. On the Internet, 90% of the content is garbage, and just 10% is secure [17]. When hackers come across systems that are simple to compromise, they just hack into the system. Information technology is used by terrorists and criminals to organise and carry out their illicit actions. The expansion of crime and terrorism has been aided by the increase in global interaction and the widespread use of IT. People no longer need to reside in a single nation to plan such crimes because to advancements in communication technologies. Terrorists and criminals can thereby exploit security flaws in the system and operate from remote locations rather than their own countries. The majority of these crimes have their roots in poorer nations. These security breaches are made possible by the pervasive corruption in these nations. Through fraudulent bank transactions, money transfers, and other methods, the internet has contributed to the funding of these crimes. Technology with greater encryption is assisting these illicit operations.

 [ISSN 2581-5369]

III. FUTURE TRENDS

One of the main worries is what would happen if important systems in the government, businesses, financial institutions, etc. were compromised. Malware in vital systems might result from this, which could cause data loss, exploitation, or even the death of the important systems. Due to the ease of contact provided by the internet, the criminal organisations may combine and work together much more than they already do. It is thought that increased mobility would make it simpler for individuals and money to move around. Money laundering on the Internet is more and more likely. The potential for money laundering through over- and under-invoicing is projected to increase as more and more international transaction is conducted through the Internet. Similar chances to shift money through ostensibly legal transactions while overpaying are provided by online auctions. Additionally, online gaming enables the transfer of funds, particularly to offshore financial hubs. Internet recruitment will make it simpler than ever to join criminal organisations. Internet technology makes it relatively simple to send covert communications to a huge number of recipients.

Since many IT businesses are privately held, ensuring client satisfaction would take precedence over worrying about international criminality. In addition, the case for not monitoring information technology might be made on the grounds of fundamental civil liberties. Dealing with cybercrime is made more challenging by all of these factors. The text that follows provides a quick summary of some of the future trends projected by Stephen Northcutt & Friends [18]. More effective social engineering The future will be marked by attacks. Attackers will increasingly employ social engineering strategies to get beyond technology security measures, honing their approaches to take advantage of innate human tendencies. Because social engineering will enable external attackers to easily gain an internal vantage point despite conventional perimeter security measures, this will bring us closer to blending the line between external and internal threat agents.

Cybercrimes will have a forum thanks to social media. More businesses will incorporate social media as a key component of their marketing plans. They will struggle to strike a balance between the urge to participate actively in online social groups and the compliance and legal risks involved with such actions. Organisations will also struggle to manage their consumers' online social networking activity. Attackers will continue to scam people and organisations by abusing the still-evolving awareness of online social networking safety practises. Security providers will advertise their solutions as resolving each of these issues; some of them will stand out by enabling businesses to monitor and regulate online social networking activity at the

 [ISSN 2581-5369]

individual user level while still respecting users' privacy expectations. No matter how technology advances, attackers know they can always hack employees because they are the weakest link. These human attacks will only get more frequent and sophisticated in the years 2012 and 2013. The easiest route will always be used by cybercriminals. Management and organisations will finally begin taking action to secure the human.

Without delivering a grim warning that some worm would devour all the iPhones and turn the Androids into bricks, it is a sensitive matter for those reliant on iPhones for their day-to-day functioning. However, spyware-containing apps seem to be the main problem. Even the pre-installed apps on the phone are likely to call home; however, third-party apps almost always do. By enrolling its clients in Asurion roadside assistance without even asking them, AT&T has shown that they cannot be trusted. And it is really important. In the near future, memory scraping will become more widespread. This has been around for a while, but recently it has been more active in its pursuit of data including credit card information, passwords, PINs, and keys. They are successful because they get past the PCI, GLBA, HIPAA, and other security regulations that demand that data be encrypted both in transit and at rest. On the system, data in transit is decrypted and frequently kept in memory for the duration of a process, or at the very least during a decryption routine. A process may continue to be resident even after it has finished. This depends on how well it cleans up. Even while the data is encrypted on the hard drive, it's more than likely still in clear text in the RAM. During web sessions, browsers are infamous for leaving things hanging around in memory. In order to decode everything from session data to encrypted files, the RAM Scraping virus also targets encryption keys in memory. Regarding the increasing security problem, RAM scraping is becoming more prevalent as attackers turn their attention away from server-side assaults and towards client-side attacks. Browsers are frequently misconfigured, allowing malware to enter a user's machine and steal passwords and credit card information. They are mostly an inconvenience since the account must be credited and altered whenever a customer or the fraud department notices fraudulent activities. These transactions must be written down by the banks as a result, which may pile up very rapidly. Due to its aggressive rate and polymorphic traits, AV products are unable to keep up with this kind of malware. Every week, we find a tonne of new malware, partially reverse it, and give the information to AV manufacturers to be incorporated as a new signature. The threat of RAM scraping malware that targets Point Of Sale (POS) systems is the other new element. The usage of wireless technology will increase, expanding to include more protocols with specific goals that cater to the requirements of various technologies. While Wi-Fi technology will continue to develop, other protocols, such as ZigBee, Wireless HART, and Z-Wave, as

 [ISSN 2581-5369]

well as proprietary protocols, will also become widely used and meet the needs of embedded technology. Some of the past errors from prior failed protocols are now being replicated as a result of the increased acceptance of alternative wireless technologies. We'll see history repeating itself as manufacturers rush to the market to take advantage of new prospects without carefully considering the lessons from past wireless technologies, based on this exposure and the trajectory of Wi-Fi failure and improvement. The focus of cyber attackers will shift to more Cloud Computing issues. Even though cloud computing has a lot of potential advantages, the honeymoon phase will pass. Many organisations will quickly realise that the flexibility they want for their operations is not available, and many others will find that any security concerns (from audit to breach) are far more difficult to resolve in the cloud. The security dangers of cloud computing will be accepted by many security experts. As more businesses move to cloud platforms, they will be forced to comply by the firms they serve. The infosec community will have a greater understanding of cloud settings, and the technology used to construct cloud platforms will be developed to a satisfactory degree.

Security is still included into virtual infrastructure. Security will become increasingly integrated into the original technology and less of a "add-on" after the deployment as more organisations use virtualization technologies into their environments, notably server and desktop virtualization. New firewalls and monitoring tools are now being included into some of the top platforms for server virtualization. Native integration with remote access technologies and client-side sandbox features are typical for desktop virtualization. While vendors continue to push the boundaries and provide innovative solutions to improve virtual environments, virtualization platforms will advance to make it simpler for current security technologies to interact more naturally. Additionally, security architecture design will be a "must have" rather than a "nice to have" component in planning and deploying virtual infrastructure.

IV. Conclusion

This article focuses not only on comprehending cybercrimes but also on explaining how they affect society at various levels. This will assist the community in protecting all of the important online information held by organisations that are not secure as a result of such cybercrimes. Finding the necessary measures to resolve the issue will be aided by knowledge about the actions of cybercriminals and the effects they have on society.

The methods for combating these crimes may be roughly categorised into three categories: education, policymaking, and cyberlaws. In many nations, none of the aforementioned strategies for combating cybercrime are being used at all or are being used very ineffectively.

 [ISSN 2581-5369]

Due to a shortage of effort, new paradigms for preventing cyberattacks must be established or the present work must be improved.

*****

 [ISSN 2581-5369]

V. REFERENCES

1. Wow Essay (2009), Top Lycos Networks, Available at: http://www.wowessays.com/ dbase/ab2/ nyr90.shtml, Visited: 28/01/2012.
2. 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
3. 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.
4. 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.
5. Cyberlawtimes (2009), Available at: http://www.cyberlawtimes.com/forums/index.php?board =52.0, Visited: 10/31/09
6. 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
7. Gordon, L. A. et al., 2003, A Framework for Using Insurance for Cyber-Risk Management, Communications of the ACM, 46(3): 81-85.
8. 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.
9. Kelly, B. J., 1999, Preserve, Protect, and Defend, Journal of Business Strategy, 20(5): 22-26.
10. 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
11. Power, R., 2001, 2001 CSI/FBI Computer Crime and Security Survey, Computer Security Issues and Trends, 7(1): 1-18.
12. Sprecher, R., and M. Pertl, 1988, Intra-Industry Effects of the MGM Grand Fire, Quarterly Journal of Business and Economics, 27: 96-16.
13. Baskerville, R., 1991, Risk Analysis: An Interpretive Feasibility Tool in Justifying Information Systems Security, European Journal of Information Systems, 1(2): 121-130.

 [ISSN 2581-5369]

14. Lyman, J., 2002, In Search of the World‘s Costliest Computer Virus, http://www.newsfactor.com/perl/story/16407.html. 2002.
15. D‘Amico, A., 2000, What Does a Computer Security Breach Really Cost?, The Sans Institute
16. Hancock, B., 2002, Security Crisis Management—The Basics, Computers & Security, 21(5): 397-401.
17. Nilkund Aseef, Pamela Davis, Manish Mittal, Khaled Sedky, Ahmed Tolba (2005), Cyber-Criminal Activity and Analysis, White Paper, Group 2.
18. 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.

*****