**SIES GRADUATE SCHOOL OF TECHNOLOGY**

SRI CHANDRASEKARENDRA SARASWATHY VIDYAPURAM

PLOT 1-C D & E, SECTOR V, NERUL

NAVI MUMBAI-400706

A PROJECT REPORT

ON

“**Effects of Cyber Crime”**

PREPARED FOR

**BUSINESS COMMUNICATION AND ETHICS**

**SUBJECT INCHARGE**

**DR. VIJAY SONGIRE**

PREPARED BY

G. SAIPRASAD 114A1012

APARNA PATURI 116A1057

SUNIL PILLAI 116A1058

PRATHIKSHA POOJARY 116A1059

OMKAR POYEKAR 116A1060

**CERTIFICATE**

This is to certify that the project titled “**EFFECTS OF CYBER CRIME”** is carried out by following students of T.E in COMPUTER ENGINEERING.

G. SAIPRASAD 114A1012

APARNA PATURI 116A1057

SUNIL PILLAI 116A1058

PRATHIKSHA POOJARY 116A1059

OMKAR POYEKAR 116A1060

The project report is submitted in partial fulfilment of term work under the subject entitled of Third year of COMPUTER ENGINEERING from University of Mumbai during the academic year 2018- 19.

|  |  |  |
| --- | --- | --- |
| DR. VIJAY SONGIRE |  | DR. RIZWANA SHAIKH |
| **Subject In-charge** |  | **Head of Department** |
|  |  |  |
|  |  |  |

# **ACKNOWLEDGEMENT**

It is great pleasure to present this report on project named“**EFFECTS OF CYBER CRIME”** undertaken by third year engineering students (CE department) as a part of curriculum under the subject entitled **‘Business communication and ethics’**.

It pleasures that we find ourselves penning down these lines to express our sincere thanks to the people who helped us along the way in completing our project. We find inadequate words to express our sincere gratitude towards them.

First and foremost, we would like to express our gratitude towards our project guide Dr. Vijay Songire sir for placing complete faith and confidence in our ability to carry out this project and for providing us his time, inspiration, encouragement, help and valuable guidance. Without the sincere and honest guidance of our respected sir we would not have been to reach the present stage.

# **ABSTRACT**

This study was conducted to illustrate the relationship between cybercrime and its effects. In this study we’ve seen that right from the introduction of the first computer, people have been curious to exploit the various functionalities of the system. However, standalone systems couldn’t cause a lot of damage. The real problem started with the introduction of the internet. The introduction of Internet and its commercial availability led to increase in cases of cybercrime. We also see that as computer systems and internet became more affordable, more people could exploit it. In this study, we explore the different possible causes of cybercrime. We also study the effects and damage that such activities have caused. As cybercrime emerged into a growing problem, various preventive measures were introduced to reduce cybercriminal activity. In this study we also see the various laws that were put in place to curb cybercriminal activity. We also provide some possible solutions to reduce cybercrime.

**Table of Contents**

[**ACKNOWLEDGEMENT ………………………………………………. iii**](#_gjdgxs)

[**ABSTRACT ……………………………………………………………... iv**](#_30j0zll)

**1.** [**INTRODUCTION**](https://docs.google.com/document/d/1nGODF3s_YAqVm8cgKaoZVVocMcP7tXuW7_0sbpPuU2Q/edit#heading=h.1fob9te) **…………………………………………………….. 1**

**2. HISTORY OF CYBER CRIME ……………………………………… 2**

2.1 Rise of Cyber-crime ……………………………………………………… 2

2.2 Incentives and Motivation Behind These Attacks ………………………. 5

2.3 Parallel Evolution Of Defense …………………………………………… 6

2.4 What Is Learnt ? ………………………………………………………….. 7

**3. CAUSES OF CYBER CRIME …………………………………………. 8**

3.1 Economically Motivated Cyber Crime ………………………………….. 8

3.2 Personally Motivated Cyber Crime ……………………………………… 8

3.3 Ideologically Motivated Cyber Crime ……………………………………. 9

3.4 Negligence …………………………………………………………………9

3.5 Lack of Evidence ……………………………………………………… 10

**4. EFFECTS OF CYBER CRIME…………………………………………… 11**

4.1 Loss of Revenue …………………………………………………………….. 11

4.2 Wasted Time ……………………………………………………………….. 12

4.3 Damaged Reputations ………………………………………………………. 12

4.4 Influence of Cyber Terrorism ……………………………………………….. 12

4.5 Impact on Government and Society ……………………………………….. 13

**5. LAWS OF CYBER CRIME ……………………………………………… 14**

5.1 Amendment Act 2008 ……………………………………………………… 14

5.2 ITA Structure ………………………………………………………………. 15

5.3 Applicability ………………………………………………………………... 16

**6. SOLUTIONS TO REDUCE CYBER CRIME ………………………….. 17**

6.1 Diffusion …………………………………………………………………… 17

6.2 Investigation ……………………………………………………………….. 18

6.3 Legislation ………………………………………………………………….. 18

6.4 Penalties …………………………………………………………………… 19

6.5 Awareness…………………………………………………………………… 20

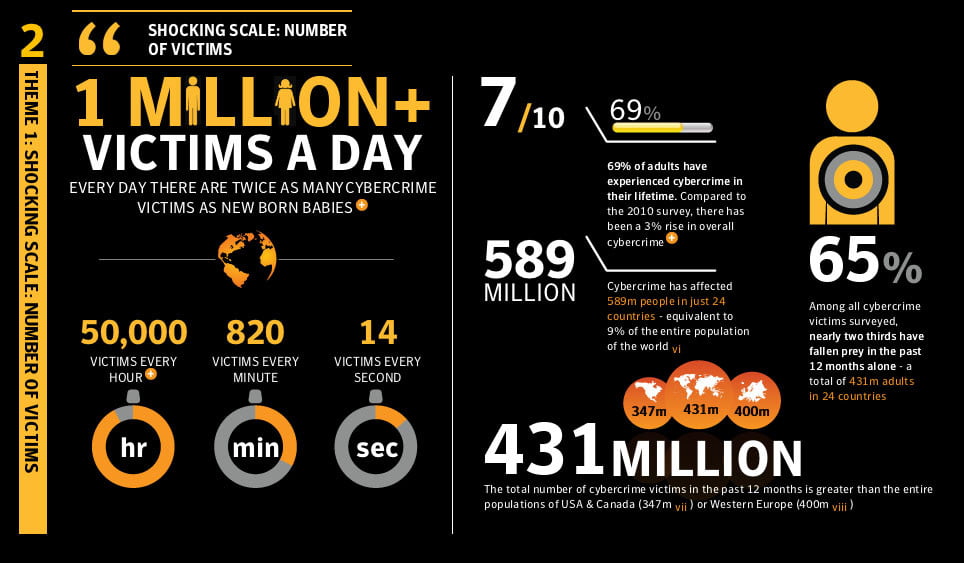
**7. CONCLUSION ……………………………………………………………. 21**

**METHODOLOGY …………………………………………………………….. 22**

**BIBLIOGRAPHY**……………………………………………………………………………….. 22

CHAPTER 1: INTRODUCTION

Cyber-crime is one of the fastest growing areas of criminality. Many criminals are exploiting the speed, convenience, and anonymity that modern technologies offer to commit a diverse range of crimes, including attacks against computer data and systems, identity theft and Internet auction fraud. The global nature of the Internet allows criminals to commit almost any illegal activity anywhere in the world, which makes it essential for all countries to adapt their domestic anti cybercrime controls to cover crimes carried out in cyberspace. We read about it in newspapers very often. Cyber-crime is formally defined as "A criminal activity committed on the internet. This describes everything from electronic cracking to denial of service attacks that cause electronic commerce sites to lose money ". Finally, this research will present some possible solutions to curb cybercrime.

****

CHAPTER 2. HISTORY OF CYBER CRIME

## 2.1 RISE OF CYBER-CRIME:

The early computer devices like ENAIC- Electronic Numerical Integrator and Computer, BINAC-Binary Automatic Computer, UNIVAC- Universal Automatic Computer, and other punch card tabulation machines had some major security advantages. They were standalone systems, huge and very expensive, and not many people knew what a computer actually was. Commercial computers like PDP-1(Programmed Data Processor) got introduced around 1960s with a business model of renting out the machine to companies and individuals. This renting was done on a time-sharing basis. This made the data and programs stored in it vulnerable, and hence opened the doors to *Hacking*. The first hackers’ group came from the Massachusetts Institute of Technology (MIT) in 1961, after MIT got its first PDP-1.

During the 1970s, while computers were introduced slowly, the telephone system was well established by that time. There was a group of people, called *phreaks* who were curious about the idea of making free phone calls and looked into various methods of doing it. One of the first phreaks was Stewart Nelson from MIT who wrote software to generate tones that helped in accessing the phone company’s long-distance service and making free calls. The phreaks created a blue box device that was programmed to generate a 2600-hertz signal, allowing them to perform functions like stacking a trunk line, and kicking off the operator line that helped in making free long-distance calls. Steve Jobs and Steve Wozniak (future founders of Apple Computer) were known to be involved in the production and distribution of such devices.

With the introduction of Altair 8800, the first affordable PC in around the 1970s it became possible for people to own computers and learn to program. This soon led to curiosity about hacking. At the same time, the emergence of other computers like the Radio Shack’s TRS-80 and the IBM PC brought even more powerful computing to people who were eager to find new ways to explore the system. But since these systems were standalone, it limited the potential of damage that could be done once the machine was compromised. However, with the introduction of networking concepts, real gates to hacking were opened. The early networking model consisted of a powerful 6 mainframe to which many terminals are connected to allow users to share files and run programs. This allowed hackers to access files.

Today’s technology has tremendously improved with regards to networking, and has gone way beyond the previous mainframe model with new concepts such as peer to peer communication. The Ethernet enabled providers to create compatible products that link computers easily and inexpensively. Interoperability (the ability of computer systems or software to exchange and make use of information) is a key consideration from any business perspective to foster a healthy ecosystem and improve economic growth. Unfortunately, these open standards also made it easier for the hackers to break into systems. This was done by reverse engineering the widely available protocols.

As computers became increasingly cheaper and started getting mainstream, efforts were made to get seamless interaction between them. *ARPAnet* was one such effort. While designing the ARPAnet, security was not a big issue for research scientists because they thought that the small number of nodes on the network would limit the scope of the threat posed by any security breaches. However, in 1988, Robert T. Morris, who was a graduate student at Cornell University launched a self-replicating worm on the government's ARPAnet. This was done to test its effect on UNIX systems. The worm quickly spread all across the United States, infected thousands of computers, clogged government and university systems and brought the Internet to a standstill. This was when internet users realized how big the problem actually was.

In the early 1990s, as Internet access became cheaper, the number of attacks increased and cyber-crime was now crossing international boundaries. Among the first cyber-crime case to make international headlines, hackers in West Germany were apprehended and subsequently arrested for breaking into U.S. government and corporate computers, and for selling operating system source code to the Soviet KGB. In another event, Russian cracker Vladimir Levin, 7 siphoned $10 million from Citibank and transferred the money to bank accounts around the world. Around the same time the first electronic bulletin board systems (BBSs) were introduced which allowed the phreakers and hackers to gossip about trade tips, share stolen computer passwords and credit card numbers, and distribute pirated software.

With the launch of rich browsers like Netscape Navigator and Microsoft Internet Explorer, during the mid-90s accessing the information on the Web became easy. Hackers now started moving their “how to” information and hacking programs from BBSs to new hacker Web sites. As information and easy-to-use tools become widely available to anyone with Net access, the number of attacks also increased drastically. There were reports by the General Accounting Office that the Defense Department computers sustained 250,000 attacks by hackers in 1995 alone.

In the late 1990, Hackers pierced security in Microsoft's Windows operating system to illustrate its weaknesses. Trojan horse virus was released in 1998 by hacking group ‘Cult of the Dead Cow’ which on a machine running Windows 95 or Windows 98, allowed unauthorized remote access of the machine. Spamming attack was also seen during this time. An example of which is the attack on the Federal Bureau of Labor Statistics in 1998, which was inundated for days with hundreds of thousands of fake information requests. The website was brought down that frustrated the economists and investors as they depended on it to retrieve the latest economic data. In addition, Internet portals like Yahoo and AOL were also target of spam attacks. Yahoo was hit by hackers claiming a "logic bomb" will go off in the PCs of Yahoo!'s users on Christmas Day 1997. AOL was a target when AOHell was released which caused the mail box of AOL users to be flooded with multi-megabyte mail bombs and chat rooms to be disrupted with spam messages.

The worms and viruses released in the twenty first century possess a higher impact in terms of financial damage and loss of productivity. An example is the “Love Letter” worm that caught on in May 2000 caused companies $960 million in clean-up costs and $7.7 billion in lost productivity. Nimda and Code Red virus in 2001 ushered new threats that the viruses are capable of spreading across the Internet without any user interaction and then automatically launching further attacks such as denial-of-service (DoS) attack. Microsoft was a target of DNS attack, which took the users to corrupted links and prevented millions of users from reaching Microsoft Web pages for two days. In January 2002, the Slammer worm that spread across the Internet caused short-term Internet outages. In 2004, Mydoom virus caused $43.9 billion in economic damage in 215 countries, according to a report by mi2g Intelligence Unit (mi2g.net), a digital risk firm. This virus is considered as the worst virus to ever hit our networks.

2.2 INCENTIVES AND MOTIVATION BEHIND THESE ATTACKS:

If we examine the early attacks, one would see that early hackers were basically programmers who programmed for fun. This curiosity could be interpreted as the beginning or essence of hacking. Some people hacked in an attempt to gain personal fame. Movies such as Wargames and Iain Softley’s Hackers motivated few others as they saw the character of a hacker as a brilliant guy that breaks the law for noble purposes.

Today’s sophisticated attacks possess a greater damage potential. Various hacker groups make threatening claims about breaking into Pentagon network to steal military software and selling it to terrorists if their demands are not met. Such cases are on a rise. This is a clear indication that cyber-criminal activity is changing. The scope and intention of the attackers has increased beyond control. Hackers are no longer enthusiastic programmers but people with malicious intentions having monetary interests and selfish motives. Today, we see a strong link between the attackers and terrorist organizations who envision cyber-crime as a potential mode to carry out their motive – i.e. to spread terror.

2.3 PARALLEL EVOLUTION OF DEFENSE:

Preventive measures were developed to defend against the attacks as soon as cyber-criminal activity was discovered and reported. For example, phone companies started the use of ESS (Electronic Switching System) to counterattack phreaks. ESS made phreaking extremely difficult by sending a computer-generated artificial ring in which the voice is not connected directly to the called person’s line unless it is picked up. The installation of ESS in almost all major cities made blue boxing harder.

The Federal Government also stepped up to stop cyber-criminal activity and enforced a national crackdown on hackers. In the wake of an increasing number of break-ins to government and corporate computers, Congress passed the ‘Computer Fraud and Abuse Act’ in 1986, which made breaking into computer systems a crime. Also, the ‘Comprehensive Crime Control Act’ passed in the same year gave Secret Service jurisdiction over credit card and computer fraud (Section Current Law and Policy speaks in detail on this). In addition, the Computer Emergency Response Team was formed by U.S. defense agencies with the mission to investigate the growing volume of attacks on computer networks. Simultaneously, intelligence services such as FBI stepped up and started investigation of hunting down cyber-crackers. In one of the first 10 arrests of hackers, the FBI busted the Milwaukee-based 414s after members were accused of 60 computer break-ins ranging from Memorial Sloan-Kettering Cancer Center to Los Alamos National Laboratory which helps develop nuclear weapons.

The invention of IPv6 protocol that supported built-in authentication, integration, confidentiality and access control at the IP layer also helped in preventing cybercrime to a huge extent. Also, more and more people started using antivirus products from companies like Norton and MacAfee for home computers. Realizing the series of attacks that exploited security in Windows Operating System and other Microsoft products, Bill Gates outlined his vision for *Trustworthy computing*. This led to more secure products in the current Microsoft releases. Software companies also made efforts to release advisories and patches as soon as vulnerability is discovered in a released product. Security is an important aspect today in the software development where security reviews are held, threat modeling is done to do an in-depth risk analysis of various potential threats.

## 2.4 WHAT IS LEARNT?

It is safe to assume that soon after the first computer networks were built, some people started looking for ways to exploit the system, thus giving birth to cyber-crime. However, cyber-crime did not become a problem overnight. This problem kept growing as computing became easier, cheaper and more easily accessible. As technology advances, vulnerabilities are discovered, and then defenses against those vulnerability can be researched. Whenever new products are released, new security holes are soon discovered and this cycle never ends. With the countless examples of the devastation caused by cyber-attack and the rise of terrorism in the last few years, Cyber-crime has become a serious threat for countries and organizations.

CHAPTER 3: CAUSES OF CYBER CRIME

According to the credit-checking firm Experian, online theft increased 300 percent in 2010 and 2012 just one of the areas of online crime that has increased in recent years. Cybercrime including all from identity theft and hacking to virus distribution and computer fraud is a complicated area of criminology and one that is receiving more consideration as computers are prevalent in our lives and handle more of our personal information. Like different areas of crime, its causes are sometimes difficult to establish, but certain patterns in cybercrime are rising.

3.1 Economically Motivated Cyber Crime

As is the case with several crimes committed outside the Internet, money is a main motivator for many cyber criminals. Especially because the dangers of criminality are lesser apparent when you're hiding behind a network, the perception of low risk and very high financial accolade prompts many cyber criminals to participate in malware, phishing, identity theft, fraudulent money request attacks. Businessweek estimates that cybercrimes targeting online banking accounts only, for example, pull in almost 700 million dollars per year globally.

3.2 Personally Motivated Cyber Crime

Cyber criminals are also human beings and what they do including their crimes is often the cause of personal emotions and revenge. From the unhappy employee installing a virus on office computers to a jealous boyfriend hacking into a girlfriend's social media handle or a teenager taking down a website just to prove that he could do it, many cybercrimes are actually crimes of passion committed over the Internet. Most of these crimes, however, can still have very serious impacts and cause adequate property damage.

3.3 Ideologically Motivated Cyber Crime

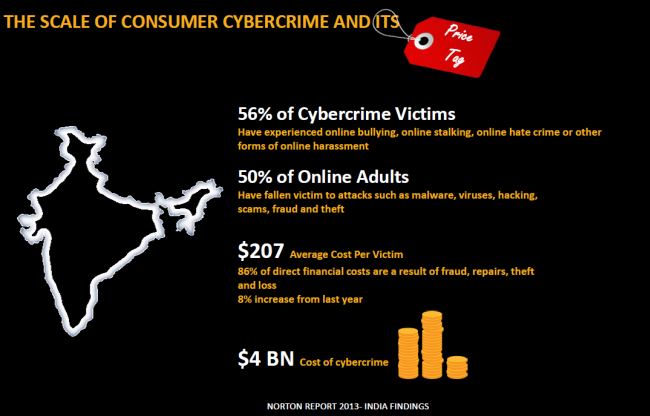
After companies like Visa, MasterCard and PayPal refused to let account and card holders make additions to the controversial non-profit WikiLeaks, the "hacktivist" group Anonymous coordinated a sequence of bot attacks on the company servers, rendering them unreachable to Internet users. These types of attacks are conducted for perceived ethical, ideological or moral reasons, destroying or disabling computer equipment and networks to express grudges against individuals, corporations, organizations or also national governments.

3.4 Negligence:

Sometimes simple negligence can give rise to criminal actions, such as saving a password on an official computer, using official information in a public place and even saving data without protecting it. The cybercriminal can take advantage of such negligence and use it to attain, manipulate and forge information. Negligence is very closely related with human conduct. It is therefore very probable that while securing the computer system there might be any negligence, which in turn provides a Cyber Criminal to obtain access and control over the system.

3.5 Lack of Evidence:

One cause of rise in cybercrime is the lack of evidence to bind the criminal by law. There are plenty ways to hide the trail of a cybercrime and little to actually identify the criminal. Consider a pedophile who baits his victim through email or social network platforms. The police can trace the information to the criminal, but until solid physical evidence is found, the trail cannot be used in a court of law. Loss of evidence is the most common & obvious problem as all the data are routinely deleted. Further collection of data outside the territorial extent also halts this system of Crime Investigation.



CHAPTER 4: EFFECTS OF CYBER CRIME

4.1 Loss of Revenue

One of the main consequences of cybercrime on a company is a loss of revenue/income. This loss may be caused by an outside person who acquires sensitive financial information, using it to extract funds from an organization. It can also come about when a business's e-commerce site becomes compromised--while terminal, expensive income is lost when consumers are unable to utilize the site.



4.2 Wasted Time

Another major consequence of cybercrime is the time that is wasted when Information Technology personnel must dedicate maximum part of their day handling such incidences. Rather than working on productive and creative measures for an organization, many Information. Technology staff members spend a great percentage of their time handling security breaches and other problems related with cybercrime.

4.3 Damaged Reputations

In situations where customer records are compromised by a security contravene associated with cybercrime, a company's reputation can take a major batter. Customers whose credit cards or other monetary data become grabbed by hackers or other infiltrators drop assurance in an office and often begin taking their business elsewhere.

4.4 Influence of Cyber Terrorism

Cyber-terrorism can have a serious large-scale influence on significant numbers of people. It can weaken countries' economy greatly, thereby stripping its resources and making it more vulnerable to military attack. Cyber-terror also affects internet-based businesses. Like brick and mortar retailers and service providers, most websites that produce income (whether by advertising, monetary exchange for goods or paid services) could stand to lose money in the event of downtime created by cyber criminals. As internet-businesses have increasing economic importance to countries, what is normally cybercrime becomes more political and therefore "terror" related.

4.5 Impact on Government and Society

Cybercrime has been increasing its convolution and financial expenses since corporations have begun to use computers in the course of doing business. As technology increases between governments that are caught up in international business, criminals have realized that this is a cost-efficient method of making money. This investigation and testing manual are meant to provide as a basic model on the lessons learned to set up governments, and their prosecutors, for combating cybercrime. To research deeply into computer technology requires both long learning and technical expertise. Therefore, as in most of the crimes that are technological in nature, or have technical aspects to them, such as bank hoax or murder investigations that necessitate the analysis of blood and spatter techniques, gunshots that require extensive ballistics investigation, experts are advisable for use as an aid in directing your investigations, to act as a special aide in preparing for trial, and as an expert to testify in that trial. However, experts are not absolutely required, principally in identifying basic components that make up a cybercrime, and on how to show the elements of that case. All of us know that computer crimes can run from the simple to the mega sophisticated. This does not mean they are not solvable, and understandable to the judiciary throughout any trial. The complication in these crimes should not be feared. All that is required is for you to comprehend the basic concepts explained in this manual, follow its simple set of laws and use the facts you have acquired. You will then be able to effectively investigate, organize and put on any case.

CHAPTER 5: LAWS OF CYBERCRIME

The Information Technology Act, 2000 (also known as ITA-2000, or the IT Act) is an Act of the [Indian Parliament](https://en.wikipedia.org/wiki/Indian_Parliament) (No 21 of 2000) notified on 17 October 2000. It is the primary law in [India](https://en.wikipedia.org/wiki/India) dealing with [cybercrime](https://en.wikipedia.org/wiki/Cybercrime) and [electronic commerc](https://en.wikipedia.org/wiki/Electronic_commerce)e. It is based on the United Nations Model Law on Electronic Commerce 1996 (UNCITRAL Model) recommended by the General Assembly of United Nations by a resolution dated 30 January 1997.

The Act essentially deals with the following issues:

* Legal Recognition of Electronic Documents
* Legal Recognition of Digital Signatures
* Offenses and Contraventions
* Justice Dispensation Systems for cybercrimes.

5.1 Amendment Act 2008

Being the first legislation in the nation on technology, computers and ecommerce and e-communication, the Act was the subject of extensive debates, elaborate reviews and detailed criticisms, with one arm of the industry criticizing some sections of the Act to be draconian and other stating it is too diluted and lenient. There were some conspicuous omissions too resulting in the investigators relying more and more on the time-tested (one and half century-old) Indian Penal Code even in technology-based cases with the I.T. Act also being referred in the process and the reliance more on IPC rather on the ITA. 3 Thus the need for an amendment – a detailed one – was felt for the I.T. Act almost from the year 2003- 04 itself. Major industry bodies were consulted and advisory groups were formed to go into the perceived lacunae in the I.T. Act and comparing it with similar legislations in other nations and to suggest recommendations. Such recommendations were analyzed and subsequently taken up as a comprehensive Amendment Act and after considerable administrative procedures, the consolidated amendment called the Information Technology Amendment Act 2008 was placed in the Parliament and passed without much debate, towards the end of 2008 (by which time the Mumbai terrorist attack of 26 November 2008 had taken place). This Amendment Act got the President assent on 5 Feb 2009 and was made effective from 27 October 2009.

Some of the notable features of the ITAA are as follows:

* Focusing on data privacy
* Focusing on Information Security
* Defining cyber café
* Making digital signature technology neutral
* Defining reasonable security practices to be followed by corporate
* Redefining the role of intermediaries
* Recognizing the role of Indian Computer Emergency Response Team
* Inclusion of some additional cybercrimes like child pornography and cyber terrorism Authorizing an Inspector to investigate cyber offences (as against the DSP earlier)

5.2 ITA Structure

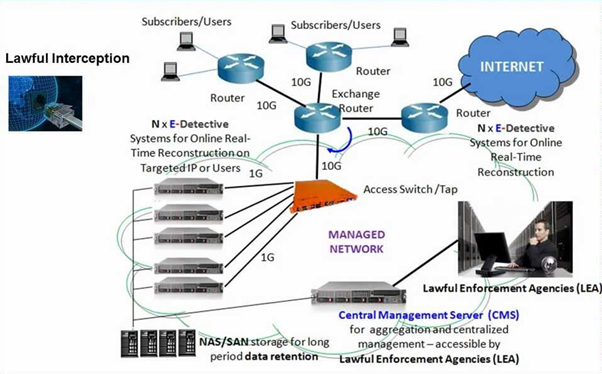
The Act totally has 13 chapters and 90 sections (the last four sections namely sections 91 to 94 in the ITA 2000 dealt with the amendments to the four Acts namely the Indian Penal Code 1860, The Indian Evidence Act 1872, The Bankers’ Books Evidence Act 1891 and the Reserve Bank of India Act 1934). The Act begins with preliminary and definitions and from there on the chapters that follow deal with authentication of electronic records, digital signatures, electronic signatures etc. Elaborate procedures for certifying authorities (for digital certificates as per IT Act -2000 and since replaced by electronic signatures in the ITAA -2008) have been spelt out. The civil offence of data theft and the process of adjudication and appellate procedures have been described. Then the Act goes on to define and describe some of the well-known cybercrimes and lays down the punishments therefore. Then the concept of due diligence, role of intermediaries and some miscellaneous provisions have been described. Rules and procedures mentioned in the Act have also been laid down in a phased manner, with the latest one on the definition of private and sensitive personal data and the role of intermediaries, due diligence etc., being defined as recently as April 2011.

5.3 Applicability

The Act extends to the whole of India and except as otherwise provided, it applies to also any offence or contravention there under committed outside India by any person. There are some specific exclusions to the Act (i.e. where it is not applicable) as detailed in the First Schedule, stated below:

1. negotiable instrument (Other than a cheque) as defined in section 13 of the Negotiable Instruments Act, 1881;
2. a power-of-attorney as defined in section 1A of the Powers-of-Attorney Act, 1882;
3. a trust as defined in section 3 of the Indian Trusts Act, 1882
4. a will as defined in clause (h) of section 2 of the Indian Succession Act, 1925 including any other testamentary disposition
5. any contract for the sale or conveyance of immovable property or any interest in such property;
6. any such class of documents or transactions as may be notified by the Central Government

CHAPTER 6: SOLUTIONS TO REDUCE CYBER CRIME

****

6.1 Diffusion

The broad diffusion of cyber-criminal activities is a compelling issue in computer crimes detection and prosecution. According to a research, technical expertise and accessibility no longer act as barriers to entry into cybercrime. Indeed, hacking is much less complex than it was a few years ago, as hacking communities have greatly spread their knowledge through the Internet. Experienced hackers have hugely contributed to information sharing. Beginners could benefit from the already existing information in the internet on hacking.

Moreover, hacking is not as expensive as before. Before the advent of such technology, in order to spam or scam one needed a dedicated server, skills in server management, network configuration, and maintenance, knowledge of Internet service provider standards. By comparison, an e-mail software as a service is a scalable, inexpensive, bulk, and transactional email sending service for marketing purposes and could be easily set up for spam. Even though cloud computing could be helpful for a cybercriminal as a way to leverage his attack like brute-forcing a password, improve the reach of a [botnet](https://en.wikipedia.org/wiki/Botnet), or facilitating a spamming campaign.

6.2 Investigation

A computer can be a source of [evidence](https://en.wikipedia.org/wiki/Evidence). Even where a computer is not directly used for criminal purposes, it may contain records of criminal investigators in the form of a [log-file](https://en.wikipedia.org/wiki/Logfile). In most countries[Internet Service Providers](https://en.wikipedia.org/wiki/Internet_Service_Providers) are required, to keep their log-files for a predetermined amount of time. For example; a European wide [Data Retention Directive](https://en.wikipedia.org/wiki/Data_Retention_Directive) states that all [email](https://en.wikipedia.org/wiki/E-mail) traffic should be retained for a minimum of 12 months.

There are many ways for cybercrime to take place, and investigations tend to start with tracking [IP Address](https://en.wikipedia.org/wiki/IP_Address), however it is not necessarily the right choice to solve a case. Different types of high-level crime may also include elements of low-level crime, and vice versa, making cybercrime investigators an indispensable part of modern law-enforcement. The detective work involved in solving cybercrime is constantly improving whether it be at small police units or at large organizations as the hackers find new ways to perform cyber-criminal activities

### 

### 6.3 Legislation

Due to easily exploitable laws, cyber criminals use developing countries where the laws aren’t robust in order to evade detection and prosecution from law enforcement. In developing countries, laws against cybercrime are weak or sometimes non-existent. These weak laws allow cyber criminals to strike from unknown locations and remain undetected. Even when identified, these criminals avoid being punished or transferred to a country, such as the [United States](https://en.wikipedia.org/wiki/United_States), that has developed laws that allow prosecution.

While this proves difficult in some cases, certain investigation agencies, have used deception and tricks to catch criminals. For example, two Russian hackers had been escaping the FBI for some time. The FBI set up a fake computing company based in Seattle, Washington to lure the two Russian men into the United States by offering them work with this company. Upon completion of the interview, the culprits were arrested outside of the building. Clever ploys like this are sometimes necessary to catch cyber criminals when the legislation doesn’t help.

The executive order against cybercrime in United States allows the country to seize assets of convicted cyber criminals and block their economic activity within the United States. This is amongst the first solid legislation that combats cybercrime.

### 

### 6.4 Legislation

Penalties for computer-related crimes in some countries can range from a fine and a short period of jail time for a small offense such as unauthorized use of a computer up to computer tinkering which is a big crime and can to longer duration of imprisonment.

However, some [hackers](https://en.wikipedia.org/wiki/Hacker_(computer_security)) have been hired as [information security](https://en.wikipedia.org/wiki/Information_security) experts (also called as ethical hackers) by private companies due to their experience in committing computer crime, a phenomenon which theoretically could create [tenacious](https://en.wikipedia.org/wiki/Moral_hazard) spur. A possible comeback to this is for courts to ban accused hackers from using the Internet or computers, even after they have been released from prison, this punishment could be viewed as very severe or harsh as computers and the Internet become more and more important in everyday life.

However, subtle approaches have been developed that handle cyber criminals’ behavior without resorting to such strict actions. These methods involve restricting individuals to selected devices which are monitored by investigating officers.

### 

### 6.5 Awareness

### As technology advances and more people rely on the internet to store personal information such as banking or credit card credentials, criminals increasingly attempt to steal that information. Cybercrime is becoming a menace to people across the world. Creating awareness about how information can be safeguarded and the tactics criminals use to procure your details continue to grow in importance. According to a detective agency, there were huge complaints filed on cyber-criminal activities. With all the claims combined the total loss incurred by the victims was massive.

### But cybercrime is affecting at an individual level. There are one and a half million cyber-attacks annually, which means that there are over four thousand attacks a day, one seventy attacks every hour, or nearly three attacks every minute, with studies showing us that only sixteen percent of victims had asked the people who were carrying out the attacks to stop. Anybody who uses the internet for any reason can be a target or a criminal, which is why it is important to be aware of how one is being protected while one is online.

CONCLUSION

We have thus successfully studied the effects of Cyber Crime persisting in all parts of the world. We learnt a lot from this study about the various aspects of cybercrime i.e. it’s history, causes, effects, laws and in the end also on the basis of this study managed to provide some feasible solution to this problem. It is worldwide threat and is an undesirable by product of technology that has crept into the system along with the advent of internet and has brought something called cyberspace into the system. Its presence has exponentially risen in the past few years and is now felt more than ever. Though not all people are victims to cybercrimes, they are still at risk. Crimes by computer vary, and they don’t always occur behind the computer, but they executed by computer. Crimes done behind the computer are the 21st century’s problem. With the technology increasing, criminals don’t have to rob banks, nor do they have to be outside in order to commit any crime. They have everything they need on their lap. Their weapons aren’t guns anymore; they attack with mouse cursors and passwords. Thus, we would like to conclude by saying that yes, cybercrime is a global threat and has the capability to even fall robust networks and hence literally nobody’s information is safe. It will remain in the system as long there is technology. But yes, with the advent of recent threats such as these, methods and ways have also been devised to combat, prevent and hopefully to eliminate cybercrime once for all.

# METHODOLOGY

Analytical method has been used for research. Primary or secondary sources has been used for study purposes. MLA (Modern Language Association) has been used for documentation.

# BIBLIOGRAPHY

* “Consequences of Crime - Calling off Cyber Crime.” Google Sites, sites.google.com/site/callingoffcybercrime/consequences.
* Shabnam, Naznin, et al. “Underlying Causes of Cyber-Criminality and Victimization: An Empirical Study on Students.” Social Sciences, Science Publishing Group, 5 Mar. 2016, article.sciencepublishinggroup.com/html/10.11648.j.ss.20160501.11.html.
* “Causes of Cybercrime and Preventive Measures.” Krazytech, 20 Nov. 2017, krazytech.com/technical-papers/cyber-crime.
* “Cybercrime.” Wikipedia, Wikimedia Foundation, 24 Oct. 2018, en.wikipedia.org/wiki/Cybercrime.
* “Cybercrime Problems and Solutions Information Technology Essay.” UKEssays,[www.ukessays.com/essays/information-technology/cybercrime-problems-and-solutions-information-technology-essay.php](http://www.ukessays.com/essays/information-technology/cybercrime-problems-and-solutions-information-technology-essay.php).
* “Information Technology Act, 2000.” Wikipedia, Wikimedia Foundation, 17 Oct. 2018, en.wikipedia.org/wiki/Information\_Technology\_Act, \_2000.