

# CYBER SECURITY AND ITS TRENDS

Shubham Nagare<sup>1</sup>sknagare666@gmail.com

Prof. Dushyant Bodkhey<sup>2</sup>dushyant.bodkhey@sinhgad.edu

Dr. Chandrani Singh<sup>3</sup>directormca\_siom@sinhgad.edu

Sinhgad Institute Of Management, Pune (India)

---

## **Abstract**

*Cyber security plays an important role in the field of information technology. information security has become one of the biggest challenges today. Whenever we think about cyber security, the first thing that comes to our mind is “Cyber Crimes” which are increasing tremendously day by day. Various governments and companies are taking many measures to prevent these cybercrimes. Apart from various measures, cyber security is still a big concern for many. This Research Paper focuses mainly on the challenges facing cyber security with the latest technologies. it also focuses on the latest information on cybersecurity techniques, ethics, and trends changing the face of cybersecurity.*

**Keywords:** Cyber Crime, cyber security, cybercrime, cyber ethics, social media, cloud security, android apps.

## **1. Introduction**

Today a person can send and receive any form of data be it email or audio or video at the click of a button, but have they ever wondered how secure their data is transmitted or sent to another person without any information leakage?? The answer lies in cyber security. The Internet is the fastest-growing infrastructure in everyday life today. In today's technical environment,

many of the latest technologies are changing the face of humanity. But due to these emerging technologies, we are not able to protect our private information in a very effective manner and that is why cyber-crimes are increasing day by day these days. Today, more than 60 percent of the total business transactions are done online, so this area required high quality of security for transparent and best transactions. Therefore, cyber security has become the latest issue. The scope of cyber security is not only limited to information security in the IT industry but also in various other areas like cyberspace etc. even the latest technologies like cloud computing, mobile computing, e-commerce, internet banking, etc. also require a high level of security. Since these technologies contain some important information about a person, their security has become a must. Strengthening cyber security and protecting critical information infrastructures are essential to the security and economic well-being of any nation. Increasing Internet security (and protecting Internet users) has become an integral part of the development of new services and government policy. The fight against cybercrime needs a comprehensive and safer approach. Since technical measures alone cannot prevent any criminal activity, it is essential that law enforcement agencies can

effectively investigate and prosecute cybercrime. Today, many countries and governments impose strict laws on cyber securities to prevent the loss of some important information. Every individual must also be trained in this cyber security and save themselves from these growing cybercrimes.

## **2. Problem Statement**

With computer information systems serving as the vital life blood of many organizations, managers must be aware of both the risks and the opportunities to minimize the risks to information systems. Over the past several years, experts and policymakers have expressed increasing concerns about protecting ICT systems from cyberattacks, and with the popularization of the Internet onto which most of these systems ride, there has grown interest in computer crime, ethics, and privacy particularly by unauthorized persons to access these systems. Usually the end goal is theft, disruption, damage, or other unlawful actions. Many experts expect the number and severity of cyberattacks to increase over the next several years.

“To Examine challenges of cyber security Presented on Information system”

With computer information systems serving as the vital life blood of many organizations, manager must be aware of both the risks and the opportunities to minimize the risk to information system over the past several years, experts and policymakers have expressed increasing concerns about

protecting ICT systems from cyberattacks, and with the popularization of the internet onto which most of these systems ride, there has grown interest in computer crime, ethics, and privacy particularly by unauthorized persons to access these systems. Usually the end goal is theft, disruption, damage or others unlawful actions. Many experts expect the number and severity of cyberattacks to increase over the next several years.

More Specifically, the following research questions need to be addressed:

- What is the current state of Information System being used?
- How to classify these cyber threats for easier identification and modeling?
- What are the current industry practices and researches in regards to cyber security modeling?
- How to come up with a unified model for development of secure information systems?

## **3. Objective**

The long-term goal of the research is to develop a formalized secure model for systems, that integrates from the hardware to the software to the human- computer interface. Ensuring cyber security requires efforts throughout an information system.

Cyber security is the body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access.

Particularly, the study has the following sub-objectives

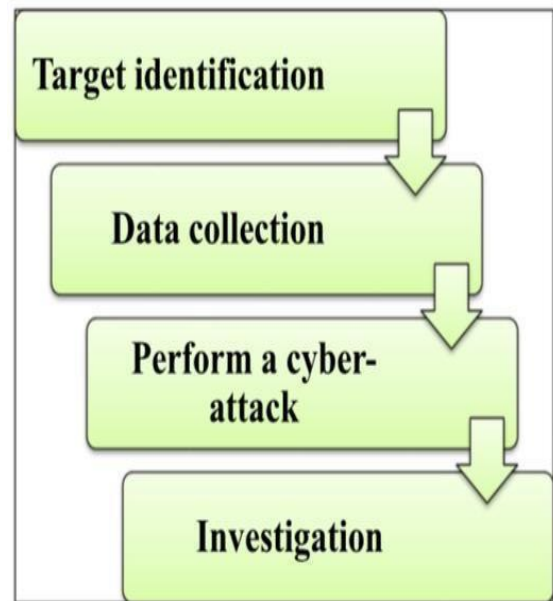
- To provide a comprehensive review of state of security of most information system.
- To develop a cyber-classification method of the threats for easier identification and modeling.
- To review current industry practices and researches in regards to cyber security modeling.

#### 4. Cyber Crime

Cybercrime is a time period for any unlawful pastime that makes use of a laptop as its number one method of fee and robbery. The U.S. Department of Justice expands the definition of cyber-crime to encompass any unlawful pastime that makes use of a laptop for the garage of evidence. The developing listing of cyber-crimes consists of crimes which have been made viable via way of means of computers, which include community intrusions and the dissemination of laptop viruses, in addition to laptop-primarily based totally versions of existing crimes such as identification robbery, stalking, bullying and terrorism that have come to be as essential hassle to human beings.

Usually in not unusual place man's language cyber-crime can be described as crime dedicated to the usage of a laptop and the net to thief a person's identification or promote contraband or stalk sufferers or disrupt operations with malevolent programs. As every day era is gambling a main function in

a person's existence the cyber-crimes will also grow at the side of the technological advances.



**Fig.1 – Steps of Cyber Attack**

#### 5. Cyber Security

Cyber safety is a crucial problem within the infrastructure of each organization and company. In short, an organization or company primarily based totally on cyber safety can reap excessive fame and endless successes, due to the fact this achievement is the end result of the organization's functionality to defend non-public and consumer records towards a competitor.

Organizations and competition of clients and people are abusive. An organization or company have to first and essential offer this safety withinside the first-rate manner to set up and increase itself. Cyber-safety consists of sensible measures to defend statistics, networks and records towards inner or outside threats. Cyber-safety experts defend networks, servers, intranets, and laptop systems. Cyber-safety guarantees that

handiest legal people have access to that information for higher protection, so it's essential to recognize the kinds of cyber safety. Demonstrates the exceptional kinds of cyber protection.

## **6. Cyber Security Trends**

Here we mentioned some of the trends that are having a huge impact on cyber security.

### **6.1 Servers:**

The hazard of assaults on net packages to extract facts or to distribute malicious code persists. Cyber criminals distribute their malicious code through valid net servers they've compromised. But facts-stealing assaults, lots of which get the eye of the media, also are a huge hazard. Now, we want an extra emphasis on defensive net servers and net packages. Web servers are particularly the excellent platform for those cyber criminals to thief the facts.

Hence one need to usually use more secure browsers are a number of the expected developments in cyber security.

### **6.2 Cloud computing services:**

These days all small, medium and massive corporations are slowly adopting cloud offerings. In different phrases the arena is slowly shifting closer to the clouds. This brand new fashion provides a large project for cyber safety, as site visitors can pass round conventional factors of inspection. Additionally, because the range of packages to be had inside the cloud grows, coverage controls for net packages and cloud offerings may also want to conform to be able to save

you the lack of treasured information. Though cloud offerings are growing their very own fashions nonetheless a variety of problems are being added up approximately their safety. Cloud might also additionally offer giant possibilities however it has to constantly be referred to because the cloud evolves in order its safety issues increase.

### **6.3 Mobile Networks:**

Today we are able to connect to anyone in any part of the world. But for these mobile network's security is a very big concern.

Firewalls and other security mechanisms are getting more permeable as people use more devices such as tablets, phones, PCs, and other devices, all of which require additional security beyond that provided by the programmes they use. We must always think about the security issues of these mobile networks. Further mobile networks are highly prone to these cyber-crimes a lot of care must be taken in case of their security issues.

### **6.4 IPv6 protocol:**

IPv6 is a completely new Internet protocol that will replace IPv4 (the previous version), which has served as the backbone of our modern networks and the Internet at large. Protecting IPv6 isn't always only a query of porting IPv4 capabilities. While IPv6 is a wholesale alternative in making extra IP addresses available, there are a few very essential modifications to the protocol which want to be taken into consideration in protection policy. Hence, it's usually better to

exchange to IPv6 as quickly as viable with the intention to lessen the dangers concerning cyber-crime.

## **6.5. Social Media**

Companies must develop innovative ways to protect personal information as we become more social in an increasingly connected world. It has not been tampered with. Social media has a significant impact on cyber security and will play a significant part in personal cyber dangers. Social media adoption among personnel is skyrocketing and so is the threat of attack. Since social media or social networking sites are almost used by most of them every day it has become a huge platform for the cyber criminals for hacking private information and stealing valuable data.

Companies must ensure they're secure in a world where we're willing to hand over our personal information. Just as quick in identifying threats, responding in real time, and avoiding a breach of any kind.

Because these social media sites draw individuals readily, hackers utilize them as bait to obtain the information and data they seek. As a result, users must take necessary precautions, particularly while dealing with social media, to avoid losing their data. The ability of individuals to share information with an audience of millions is at the heart of the particular challenge that social media presents to businesses. In addition to giving anyone the power to disseminate commercially sensitive information, social media Companies must ensure that they have

the same power to spread false information, which can be just as devastating, in a world where we're willing to give over our personal information. Through social media can be used for cyber-crimes these companies cannot afford to stop using social media as it plays an important role in publicity of a company. Instead, they must have solutions that will notify them of the threat in order to fix it before any real damage is done. Companies, on the other hand, should be aware of this and recognize the significance of data analysis in particular. In social conversations and provide appropriate security solutions in order to stay away from risks. One must handle social media by using certain policies and right technologies.

## **7. Security Techniques to be taken**

### **7.1 Access control and password security:**

The concept of user name and password has been a fundamental way of protecting our information. This could be one of the first cyber security measures taken.

### **7.2 Authentication of data:**

The documents that we receive must always be authenticated before downloading, that is it should Verify that it came from a reputable and trustworthy source and that it has not been tampered with. Anti-virus software installed on the devices is frequently used to authenticate these papers. Thus a good antivirus software is also essential to protect the devices from viruses.

### **7.3 Malware scanners:**

This is software program that commonly

scans all of the documents and files gift withinside the gadget for malicious code or dangerous viruses. Viruses, worms, and Trojan horses are examples of malicious software programs which might be frequently grouped collectively and known as malware.

#### **7.4 Firewalls:**

A firewall is a piece of software or hardware that helps block hackers, viruses, and worms from accessing your computer via the Internet. All messages entering or leaving the internet pass through the firewall present, where Each message is examined and those that do not fulfill the established security standards are blocked. As a result, firewalls are critical in detecting malware.

#### **7.5 Anti-virus software:**

Antivirus software is a computer application that detects, stops, and eliminates harmful software programmes such as viruses and worms. Most antivirus products have an auto-update capability that allows them to download new virus profiles so that they may be checked for as soon as they are discovered. Anti-virus software is a must-have for every computer system.

### **8. Conclusion**

Cyber security is a broad topic that is becoming increasingly important as the world becomes increasingly interconnected, with networks being used to carry out fundamental transactions.

With each New Year that goes, digital

malfeasance and data security continue to swerve in different directions. The most recent and problematic innovations, as well as new digital apparatuses and dangers that emerge on a daily basis, are putting organizations to the test in terms of how they protect their systems, as well as how they require new stages and knowledge to do so. There is no perfect solution to digital violations other than to do our best to keep them to a minimum so that we can live in a world free of them.

### **9. References**

CIO Asia, September 3rd, H1 2013: Cyber protection in Malaysia with the aid of using Avanthi Kumar.

Aghajani, G., Ghadimi, N., 2018 Multi-objective energy control in a micro- grid. Energy Rep. 4, 218–225.

An assessment of paradigm shift barriers and prospects. Energy Rep. 4

Al-Ghamdi, M.I., 2021. Effects of knowledge of cyber security on prevention of attacks. Mater.

Al Shaer, D., et al., 2020. Hydroxamate siderophores: Natural occurrence

Alghamdi, M.I., 2021. Determining the impact of cyber security awareness on employee behavior: A case of Saudi Arabia. Mater.

Alghamdie, M.I., 2021. A novel study of preventing cyber security threats Mater.

