# A Study of Cyber Security and Its Challenges

**Vedula Snigdha[1], ShriyaRungta[2], SachinHarne[3]**

*Graduates Students[1],PhD Student[2]*
*Department of Computer Science & Engineering, Rungta college of Engineering and Technology, Bhilai , India, 490023*

***Abstract***- *Cyber Security plays an important role in the field of information technology .Securing the information have become one of the biggest challenges in the present day. When ever we think about the cyber security the first thing that comes to our mind is 'cyber crimes' which are increasing immensely day by day. Various Governments and companies are taking many measures in order to prevent these cyber crimes. Besides various measures cyber security is still a very big concern to many. This paper mainly focuses on challenges faced by cyber security on the latest technologies. It also focuses on latest about the cyber security techniques, ethics and the trends changing the face of cyber security.*

***Key words***- *Cyber Crime, Media Gadgets, Social Networking, Cyber Threats, Cyber Terrorism, Radicalization, Cyber Ethics.*

## I- INTRODUCTION

We live in a world where our lives are constantly dependent on the media, from weather forecasts to entertainment. Media gadgets surround us everywhere; from the cell phones clinging to our bodies to the digital screens in our homes, offices, and streets; we are provided with a steady stream of information all day. Our brains are constantly fed by the media, thereby forming and shaping our minds. In this agonizing unknown brainwashing we are becoming victim to our greatest foe i.e. Terrorism. Researchers have found an astonishing relationship between Terrorism and Media. They have a symbiotic relationship; terrorism provides media with the blood, gore and all the sensational material that the media uses to sell itself. Unfortunately, for us, this is exactly what the terrorists want. They want us to see all that bloodshed and cruelty, to scare us, to drive us with fear.

Today man is able to send and receive any form of data may be an e-mail or an audio or video just by the click of a button but did he ever think how securely his data id being transmitted or sent to the other person safely without any leakage of information?? The answer lies in cyber security. Today Internet is the fastest growing infrastructure in every day life. In today's technical environment many latest technologies are changing the face of the man kind. But due to these emerging technologies we are unable to safeguard our private information in a very effective way and hence these days cyber crimes are increasing day by day.

## 1. CYBER CRIME

Cyber crime is a term for any illegal activity that uses a computer as its primary means of commission and theft. The U.S. Department of Justice expands the definition of cyber crime to include any illegal activity that uses a computer for the storage of evidence. The growing list of cyber crimes includes crimes that have been made possible by computers, such as network intrusions and the dissemination of computer viruses, as well as computer-based variations of existing crimes, such as identity theft, stalking, bullying and terrorism which have become as major problem to people and nations. Usually in common man's language cyber crime may be defined as crime committed using a computer and the internet to steel a person's identity or sell contraband or stalk victims or disrupt operations with malevolent programs. As day by day technology is playing in major role in a person's life the cyber crimes also will increase along with the technological advances.

## 2. CYBER SECURITY

Privacy and security of the data will always be top security measures that any organization takes care. We are presently living in a world where all the information is maintained in a digital or a cyber form. Social networking sites provide a space where users feel safe as they interact with friends and family. In the case of home users, cyber-criminals would continue to target social media sites to steal personal data. Not only social networking but also during bank transactions a person must take all the required security measures.

| Incidents | Jan-June 2012 | Jan-June 2013 | % Increase/ (decrease) |
|---|---|---|---|
| Fraud | 2439 | 2490 | 2 |
| Intrusion | 2203 | 1726 | (22) |
| Spam | 291 | 614 | 111 |
| Malicious code | 353 | 442 | 25 |
| Cyber Harassment | 173 | 233 | 35 |
| Content related | 10 | 42 | 320 |
| Intrusion Attempts | 55 | 24 | (56) |
| Denial of services | 12 | 10 | (17) |
| Vulnerability reports | 45 | 11 | (76) |
| Total | 5581 | 5592 | |

The above Comparison of Cyber Security Incidents reported to Cyber999 in Malaysia from January–June 2012 and 2013 clearly exhibits the cyber security threats. As crime is increasing even the security measures are also increasing. According to the survey of U.S. technology and healthcare executives nationwide, Silicon Valley Bank found that companies believe cyber attacks are a serious threat to both their data and their business continuity.

## 3.TRENDS CHANGING CYBER SECURITY

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

### 3.1 Web servers:

The threat of attacks on web applications to extract data or to distribute malicious code persists. Cyber criminals distribute their malicious code via legitimate web servers they've compromised. But data-stealing attacks, many of which get the attention of media, are also a big threat. Now, we need a greater emphasis on protecting web servers and web applications. Web servers are especially the best platform for these cyber criminals to steal the data. Hence one must always use a safer browser especially during important transactions in order not to fall as a prey for these crimes.

### 3.2 Cloud computing and its services

These days all small, medium and large companies are slowly adopting cloud services. In other words the world is slowly moving towards the clouds. This latest trend presents a big.

## 4. CYBER SECURITY TECHNIQUES

### 4.1 Access control and password security

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

### 4.2 Authentication of data

The documents that we receive must always be authenticated be before downloading that is itshould be checked if it has originated from a trusted and a reliable source and that they are not altered. Authenticating of these documents is usually done by the anti virus software present in the devices. Thus a good anti virus software is also essential to protect the devices from viruses.

### 4.3 Malware scanners

This is software that usually scans all the files and documents present in the system for malicious code or harmful viruses. Viruses, worms, and Trojan horses are examples of malicious software that are often grouped together and referred to as malware.

## CYBER TERRORISM

Cyber terrorism is the use of the Internet to conduct violent acts that result in, or threaten, loss of life or significant bodily harm, in order to achieve political or ideological gains through threat or intimidation. It is also sometimes considered an act of Internet terrorism where terrorist activities, including acts of deliberate, large-scale disruption of computer networks, especially of personal computers attached to the Internet by means of tools such as computer viruses, computer worms, phishing, and other malicious software and hardware methods and programming scripts.

Cyber terrorism is a controversial term. Some authors opt for a very narrow definition, relating to deployment by known terrorist organizations of disruption attacks against information systems for the primary purpose of creating alarm, panic, or physical disruption. Other authors prefer a broader definition, which includes cybercrime. Participating in a cyber attack affects the terror threat perception, even if it isn't done with a violent approach. By some definitions, it might be difficult to distinguish which instances of online activities are cyber terrorism or cybercrime.

Cyber terrorism can be also defined as the intentional use of computers, networks, and public internet to cause destruction and harm for personal objectives. Experienced cyber terrorists, who are very skilled in terms of hacking can cause massive damage to government systems, hospital records, and national security programs, which might leave a country, community.

**Radicalization**

Online radicalization is the process by which people particularly youth adopt extreme political or religious views via internet. After the 9/11, the phenomenon of online radicalization plays a vital role in the promotion of religious polarization and terrorism in Pakistan. Online radicalization constitutes the polarized sectarian literatures and promotes the cause of religious extremist ideology. Political Scientists, researchers and policy makers are continuously neglecting the aspect of online radicalization in Pakistan. The differences are listed below. The process of radicalization is slow while the online radicalization is fast. The radicalization is expensive and has the less objectivity while online radicalization is cheap and has the more objectivity. There are the many obstacles in the way of radicalization and dissemination of radicalized ideology while in online radicalization the obstacles are few and limitless audiences are to be addressed via cyber technology.

The propagation of the radicalized ideology is slow via conventional means while in online radicalization the propagation of radicalized ideology is fast. For the propagation of religious ideology through conventional as well as via internet, huge funds are required and the market traders, shopkeepers are the main source of giving funds to the radicalized organizations. The researcher conducts a survey to check the validity of this hypothesis. A survey was conducted in Punjabi, Urdu and in English with a total 1000 respondents across the big markets and shops of the observed

## CYBER ETHICS

Cyber ethics are nothing but the code of the internet. When we practice these cyber ethics there are good chances of us using the internet in a proper and safer way. The below are a few of them:

- DO use the Internet to communicate and interact with other people**.** Email and instant messaging make it easy to stay in touch with friends and family members, communicate with work colleagues, and share ideas and information with people across town or halfway around the world
- Don’t be a bully on the Internet. Do not call people names, lie about them, send embarrassing pictures of them, or do anything else to try to hurt them.
- Internet is considered as world’s largest library with information on any topic in any subject area, so using this information in a correct and legal way is always essential.
- Do not operate others accounts using their passwords.
- Never try to send any kind of malware to other’s systems and make them corrupt.
- Never share your personal information to anyone as there is a good chance of others misusing it and finally you would end up in a trouble.
- When you’re online never pretend to the other person, and never try to create fake accounts on someone else as it would land you as well as the other person into trouble.
- Always adhere to copyrighted information and download games or videos only if they are permissible.

The above are a few cyber ethics one must follow while using the internet. We are always thought proper rules from out very early stages the same here we apply in cyber space.

## CONCLUSION

Computer security is a vast topic that is becoming more important because the world is becoming highly interconnected, with networks being used to carry out critical transactions. Cyber crime continues to diverge down different paths with each New Year that passes and so does the security of the information. The latest and disruptive technologies, along with the new cyber tools and threats that come to light each day, are challenging organizations with not only how they secure their infrastructure, but how they require new platforms and intelligence to do so. There is no perfect solution for cyber crimes but we should try our level best to minimize them in order to have a safe and secure future in cyber space

## REFERENCES

[1] *A Sophos Article 04.12v1.dNA, eight trends changing network security by James Lyne.*

[2] *Cyber Security: Understanding Cyber Crimes-SunitBelapure Nina Godbole.*

[3] *Computer Security Practices in Non Profit Organisations – A NetAction Report by Audrie Krause.*

[4] *A Look back on Cyber Security 2012 by Luis corrons – Panda Labs.*