

# Cyber Security Challenges and its Emerging Trends on Latest Technologies

Shruti C Karbhari<sup>1</sup> and Sonali Singh<sup>2</sup>

Asst. Professor and HOD, Department of Computer Science<sup>1</sup>

Student TYBSC, Department of Computer Science<sup>2</sup>

Anjuman Islam Janjira, Degree College of Science, Murud-Janjira, Raigad, Maharashtra, India

**Abstract:** *Cyber Security plays a very important role within the field of data technology. Securing the data became one amongst the most important challenges within the gift day. Whenever we predict concerning the cyber security the primary factor that involves our mind is 'cyber crimes' that square measure increasing vastly day by day. Numerous Governments and corporations square measure taking several measures so as to forestall these cybercrimes. Besides numerous measures cyber security remains a awfully huge concern to several. This paper principally focuses on challenges moon-faced by cyber security on the newest technologies .It additionally focuses on latest concerning the cyber security techniques, ethics and therefore the trends dynamic the face of cyber security.*

**Keywords:** Cyber Security, Cybercrime, Cyber Ethics, Social Media, Cloud Computing, Automaton Apps

## I. INTRODUCTION

Nowadays man is ready to send associated receive as sociatey type of information is also an e-mail or an audio or video simply by the clicking of a however ton but did he ever assume however firmly his information id being transmitted or sent to the opposite person safely with none escape of information?? The solution lies in cyber security. Nowadays net is that the quickest growing infrastructure in on a daily basis life. In today's technical setting several latest technologies square measure dynamic the face of the person kind. however thanks to these rising technologies we tend to square measure unable to safeguard our personal info in an exceedingly} very effective method and therefore of late cybercrimes square measure increasing day by day. Nowadays quite sixty % of total business transactions square measure done on-line, thus this field needed a top quality of security for clear and best transactions. Therefore cyber security has become a contemporary issue. The scope of cyber security isn't simply restricted to securing the data in IT business however additionally to varied alternative fields like cyber house etc. Even the newest technologies like cloud computing, mobile computing, E-commerce, internet banking etc additionally desires high level of security. Since these technologies hold some vital info concerning someone their security has become a requirement factor. Enhancing cyber security and protective essential info infrastructures square measure essential to every nation's security and economic successfulness. Creating the web safer (and protective net users) has become integral to the event of recent services still as governmental policy. The fight against cybercrime desires a comprehensive and a safer approach. Provided that technical measures alone cannot stop any crime, it's essential that enforcement agencies square measure allowed to research and prosecute cybercrime effectively. Nowadays several nations and governments square measure imposing strict laws on cyber securities so as to forestall the loss of some vital info. Each individual should even be trained on this cyber security and save themselves from these increasing cyber crimes

## II. CYBER CRIME

Cyber crime may be a term for any criminal activity that uses a laptop as its primary suggests that of commission and stealing. The U.S. Department of Justice expands the definition of cyber crime to incorporate any criminal activity that uses a laptop for the storage of proof. The growing list of cyber crimes includes crimes that are created attainable by computers, like network intrusions and therefore the dissemination of laptop viruses, still as computer-based variations of existing crimes, such as fraud, stalking, bullying and terrorism which became as major downside to folks and nations. Sometimes in common man's language cyber crime is also outlined as crime committed employing a laptop and therefore the net to steel

a person's identity or sell contraband or stalk victims or disrupt operations with malevolent programs. As day by day technology is taking part in in major role in an exceedingly person's life the cyber crimes additionally can increase alongside the technological advances

### **III. CYBER SECURITY**

Privacy and security of the information can continuously be prime security measures that any organization takes care. We tend to square measure presently living in an exceedingly world wherever all the data is maintained in an exceedingly digital or a cyber type. Social networking sites offer an area wherever users feel safe as they move with friends and family. Within the case of home users, cyber-criminals would still target social media sites to steal personal information. Not solely social networking however additionally throughout bank transactions someone should take all the desired security measures. technology and health care executives nationwide, {silicon valley Silicon Valley geographical square measure geographic area geographical region geographic region} Bank found that corporations believe cyber attacks are a significant threat to each their information and their business continuity.

- 98% of corporations square measure maintaining or increasing their cyber security resources and of these, [ \*fr1 ] square measure increasing resources dedicated to on-line attacks this year
- The majority of corporations square measure making ready for once, not if, cyber attacks occur
- Only third square measure utterly assured within the security of their info and even less assured concerning the safety measures of their business partners.

There will be new attacks on automaton OS primarily based devices, however it'll not air large scale. The actual fact tablets share an equivalent OS as good phones suggests that they'll be presently targeted by an equivalent malware as those platforms. the amount of malware specimens for Macs would still grow, although abundant but within the case of PCs. Windows eight can enable users to develop applications for just about any device (PCs, tablets and good phones) running Windows eight, thus it'll be attainable to develop malicious applications like those for automaton, therefore these square measure a number of the expected trends in cyber security.

#### **3.1 Cloud Computing and its Services**

These days all little, medium and huge corporations square measure slowly adopting cloud services. In alternative words the globe is slowly moving towards the clouds. This latest trend presents an enormous challenge for cyber security, as traffic will go around ancient points of review to boot, because the range of applications obtainable within the cloud grows, policy controls for internet applications and cloud services also will ought to evolve so as to forestall the loss of valuable info. although cloud services square measure developing their own models still a great deal of problems square measure being said concerning their security. Cloud could offer vast opportunities however it should be noted that because the cloud evolves thus as its security considerations increase.

#### **3.2 APT's and Targeted Attacks**

APT (Advanced Persistent Threat) may be a whole new level of cyber crime ware. For years network security capabilities like internet filtering or IPS have compete a key half in distinguishing such targeted attacks (mostly once the initial compromise). As attackers grow bolder and use additional imprecise techniques, network security should integrate with alternative security services so as to discover attacks. Therefore one should improve our security techniques so as to forestall additional threats coming back within the future.

#### **3.3 Mobile Networks**

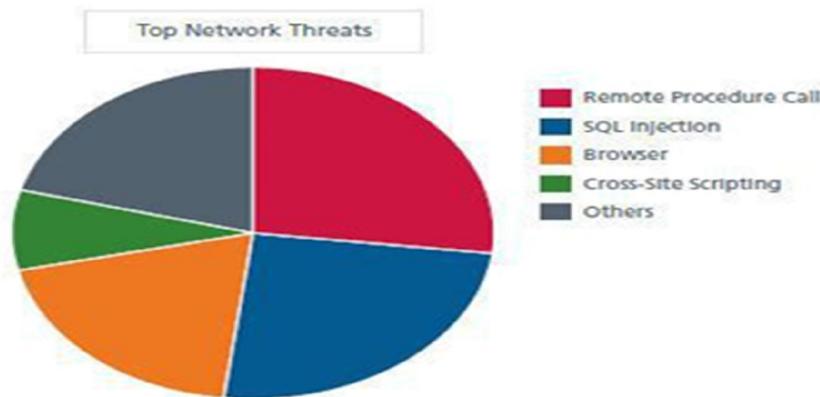
Today we tend to square measure able to hook up with anyone in any a part of the globe. Except for these mobile networks security may be a terribly huge concern of late firewalls and alternative security measures are getting porous as folks square measure exploitation devices like tablets, phones, PC's etc all of that once more need additional securities except those gift within the applications used. We tend to should always admit the safety problems with these mobile networks. Additional mobile networks square measure extremely liable to these cyber crimes a great deal of care should be taken just in case of their security problems.

### 3.4 Mobile Networks

Today we tend to square measure able to hook up with anyone in any a part of the globe. Except for these mobile networks security may be a terribly huge concern of late firewalls and alternative security measures are getting porous as folks square measure exploitation devices like tablets, phones, PC's etc. all of that once more need additional securities except those gift within the applications used. we tend to should always admit the safety problems with these mobile networks. Additional mobile networks square measure extremely liable to these cyber crimes a great deal of care should be taken just in case of their security problems. Extremely liable to these cyber crimes a great deal of care should be taken just in case of their security problems.to be thought-about in security policy. Therefore it's continuously higher to modify to IPv6 as presently as attainable so as to scale back the risks concerning cyber crime.

### 3.5 coding of the code

Encryption is that the method of encryption messages (or information) in such some way that eavesdroppers or hackers cannot scan it. In associate coding theme, the message or info is encrypted exploitation associate coding rule, turning it into associate unclear cipher text. This is often sometimes through with the employment of associate coding key, that specifies however the message is to be encoded. Coding at a awfully starting level protects information privacy and its integrity. However additional use of coding brings additional challenges in cyber security. coding is additionally accustomed defend information in transit, as an example information being transferred via networks (e.g. the web, e-commerce), mobile telephones, wireless microphones, wireless intercoms etc. therefore by encrypting the code one will recognize if there's any escape of data. Hence the higher than square measure a number of the trends dynamic the face of cyber security within the world.



The top network threats square measure mentioned in below Fig -1.

## IV. ROLE OF SOCIAL MEDIA IN CYBER SECURITY

As we become more social in an increasingly connected world, companies must find new ways to protect personal information. Social media plays a huge role in cyber security and will contribute a lot to personal cyber threats. 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.

In a world where we're quick to give up our personal information, companies have to ensure they're just as quick in identifying threats, responding in real time, and avoiding a breach of any kind. Since people are easily attracted by these social media the hackers use them as a bait to get the information and the data they require. Hence people must take appropriate measures especially in dealing with social media in order to prevent the loss of their information.

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 also gives the same power to spread false information, which can be just being as damaging. The rapid spread of false information through social media is among the emerging risks identified in *Global Risks2013* report.



Though 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. However companies should understand this and recognise the importance of analysing the information especially 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.

V. CYBER SECURITY TECHNIQUES

5.1 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.

5.2 Authentication of Data

The documents that we receive must always be authenticated before downloading that is it should 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.

5.3 Malware Scanners

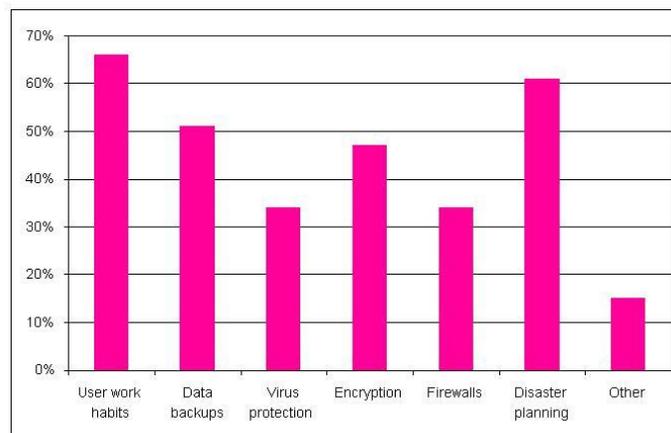
This is software that usually scans all the files and documents present in the system for malicious code or harmful viruses. Viruses, worms, and Trojan horses are examples of malicious software that are often grouped together and referred to as malware.

5.4 Firewalls

A firewall is a software program or piece of hardware that helps screen out hackers, viruses, and worms that try to reach your computer over the Internet. All messages entering or leaving the internet pass through the firewall present, which examines each message and blocks those that do not meet the specified security criteria. Hence firewalls play an important role in detecting the malware.

5.5 Anti-virus software

Antivirus software is a computer program that detects, prevents, and takes action to disarm or remove malicious software programs, such as viruses and worms. Most antivirus programs include an auto-update feature that enables the program to download profiles of new viruses so that it can check for the new viruses as soon as they are discovered. An anti virus software is a must and basic necessity for every system.



#### **VI. 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 be 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.

#### **VII. 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 corróns – Panda Labs.
- [5]. International Journal of Scientific & Engineering Research, Volume 4, Issue 9, September-2013 Page nos.68 – 71 ISSN 2229-5518, “Study of Cloud Computing in HealthCare Industry “ by G.Nikhita Reddy, G.J.Ugander Reddy
- [6]. IEEE Security and Privacy Magazine – IEEECS “Safety Critical Systems – Next Generation “July/ Aug 2013.
- [7]. CIO Asia, September 3<sup>rd</sup>, H1 2013: Cyber security in malasia by Avanthi Kumar.