Library Progress International
Vol.44 No.3, Jul-Dec 2024: P. 28909-28913

Print version ISSN 0970 1052
Online version ISSN 2320 317X

Original Article

Available online at www.bpasjournals.com

Cybersecurity Challenges and Emerging Trends in Contemporary Technologies

P Sridhar [1],Attada venkat [2],Lanke Haritha [3]

[1]M.A; LL.M (Torts &Crimes); LL.M (Business Laws); (PhD in Law)
Research Scholar, Pratibha Awardee
sridharpininty@gmail.com ;
Dr BR Ambedkhar College of Law, Andhra University, Visakhapatnam,
venkatdemudu@gmail.com
[2]BA,LLM Research Scholar, Dr BR Ambedkhar College of Law, Andhra University, Visakhapatnam,
haritha.lanka@gmail.com;
[3]LLM, Research Scholar, Dr BR Ambedkhar College of Law, Andhra University, Visakhapatnam,

How to cite this article: P Sridhar ,Attada venkat ,Lanke Haritha (2024) Cybersecurity Challenges and Emerging Trends in Contemporary Technologies. *Library Progress International,* 44(3) 28909-28913

ABSTRACT

Cybersecurity is crucial in information technology, and protecting information is becoming a major challenge today. The most common thing that comes to our mind when discussing cybersecurity is how cyber crimes are increasing in this digital world. As much as governments and companies have taken steps to address these threats, cyber security continues to be a major issue. This paper primarily addresses the challenges faced by cybersecurity with emerging technologies, while also exploring recent developments in cybersecurity techniques, ethics, and the trends that are transforming the landscape of cybersecurity.

Keywords: cyber security, cyber crime, cyber ethics, social media, cloud computing, android apps.

1. INTRODUCTION

Nowadays man can send and receive any type of data(like e-mail, audio, video, etc) but did he ever think that his/her data which they are transmitting/sending is secure or sending/receiving in some internal format something without any leakage of information is fundamental question1. The solution is cyber security. In everyday life today Internet is the fastest-growing infrastructure. Being in the technical era today we have the latest technology that has emerged which is changing how people look. But with these new technological advances, it is tough for us to secure our private details very well and so we see that in today's world cyber crimes have grown a lot2. Since over 60% of all business transactions now take place online, this industry needs a high level of security to provide the most transparent and effective transactions. Cybersecurity has so emerged as a contemporary concern. Cybersecurity covers a wide range of areas, including cyberspace and other domains, in addition to protecting data in the IT sector3.

Even the newest technology, such as online banking, cloud computing, mobile computing, and e-commerce, require a high level of security. These technologies include some very sensitive personal data, thus maintaining their security has become essential. For the sake of both national security and economic prosperity,

1 https://www.chegg.com/homework-help/questions-and-answers/cyber-security-overview-today-man-able-send-receive-form-data-may-e-mail-audio-video-click-q81428391

2 https://www.academia.edu/40910470/A_STUDY_OF_CYBER_SECURITY_CHALLENGES_AND_ITS_EMERGNING_TRENDS_ON_LATEST_TECHNOLOGIES

3 https://arxiv.org/pdf/1402.1842

important information infrastructures must be safeguarded and cyber security must be improved4.Government policy and the creation of new services now depend on making the Internet safer and safeguarding its users. A thorough and safer strategy is required to combat cybercrime. Law enforcement agencies should be given the authority to properly investigate and prosecute cybercrime. Strict rules about cyber security are being imposed by numerous governments and countries nowadays.

2. CYBERCRIME

Cybercrime refers to any illicit action where the primary tool for commission and theft is a computer5. The concept of cybercrime has been broadened by the U.S. Department of Justice to encompass any illicit behavior that makes use of a computer to save evidence6. The increasing number of cybercrimes includes both computer-based versions of pre-existing crimes like identity theft, stalking, bullying, and terrorism, which have become serious issues for individuals and countries, as well as crimes that have been made possible by computers, like network intrusions and the spread of computer viruses. We can observe that technological development is inversely proportional to cyber crimes7. In simple terms "Cyber Crimes" are the offences committed in cyberspace with the aid of electronic devices like computers and smartphones etc. Here the notable thing is there will be no question of the physical presence of the criminal. The criminals used to do criminal activities from countries due to loopholes in the existing cybercrime laws. The anonymity of the criminal is beneficial to the offender to escape from liability. In some circumstances without the involvement of the person also cyber crime can be committed. Eg: Software Piracy.

3. CYBER SECURITY

The two most important security precautions that each organization takes are data security and privacy. Nowadays, every piece of information is kept in a digital or cyber format in our environment. Social networking site users interact with friends and family in a safe setting. In the case of home users, cybercriminals would still target social networking sites in an attempt to acquire personal data. In addition to social networking, one must take all necessary security precautions when transacting with banks.

3.1 The Cyber Security Skills Crunch

In 2024, the shortage of professionals possessing the skills and expertise needed to protect businesses from cyber-attacks will continue to be a problem. According to a study, the majority of cyber security professionals (54 percent) say that the impact of the skills shortage on their organization has gotten worse over the last two years. We may anticipate that efforts to address this issue will involve increasing funding for programs that promote training, development, and upskilling as well as maintaining the salary increases given to individuals who possess the requisite abilities8.

4. TRENDS CHANGING CYBER SECURITY

The following are some of the trends that are having a huge impact on cyber security.

4.1 Web servers:

Malicious code or data extraction attacks against web applications are still a possibility. Via hacked legal web servers, cybercriminals spread their harmful code. However, there's also a serious threat from data-stealing hacks, many of which attract media attention. We have to seriously focus on web application security9. In particular, web servers provide these cyber criminals with the most effective platform for data theft. Therefore, to avoid becoming a victim of these crimes, one must always use a safer browser, particularly during critical transactions10.

---

4 https://www.studocu.com/en-us/document/university-of-the-people/english-composition/learning-journal-unit-3/24167554

5 https://arxiv.org/pdf/1402.1842

6 .https://www.chegg.com/homework-help/questions-and-answers/cyber-security-overview-today-man-able-send-receive-form-data-may-e-mail-audio-video-click-q81428391

7 https://www.researchgate.net/profile/Nikhita-Reddy-Gade/publication/260126665_A_Study_Of_Cyber_Security_Challenges_And_Its_Emerging_Trends_On_Latest_Technologies/links/54107d0d0cf2d8daaad3d18e/A-Study-Of-Cyber-Security-Challenges-And-Its-Emerging-Trends-On-Latest-Technologies.pdf

8 https://www.forbes.com/sites/bernardmarr/2023/10/11/the-10-biggest-cyber-security-trends-in-2024-everyone-must-be-ready-for-now

9https://www.bing.com/ck/a?!&&p=0aff3031dee8b944JmltdHM9MTcyNTY2NzIwMCZpZ3VpZD0zNWIyOGIzMi1jMjJmLTY3YWEtMDdiOS05ZmM2YzNlMDY2MTYmaW5zaWQ9NTI5MA&ptn=3&ver=2&hsh=3&fclid=35b28b32-c22f-67aa-07b9-9fc6c3e06616&psq=%22Now%2c+we+need+a+greater+emphasis+on+protecting+web+servers+and+web+applications.%22&u=a1aHR0cHM6Ly9hcnhpdi5vcmcvcGRmLzE0MDIuMTg0Mg&ntb=1

10 https://www.coursehero.com/file/77143833/Assignment-1Roll-11docx

4.2 Online cloud storage and related services:

These days, cloud services are being gradually adopted by all sizes of businesses, small and large. The ability of traffic to evade conventional points of inspection makes this most recent trend extremely challenging for cyber security. To prevent the loss of important data, policy controls for web apps and cloud services will also need to change as the number of applications available in the cloud increases. Even though cloud services are creating their models, many security-related concerns are still being raised. Although the cloud may offer a plethora of benefits, it is important to remember that as the cloud develops, so do security risks11.

4.3 Targeted attacks and APTs:

Cybercrime malware has reached a whole new level with APT (Advanced Persistent Threat). For many years, network security tools like intrusion prevention systems and web filtering have been crucial in spotting these kinds of focused attacks (usually after the first penetration). To identify assaults, network security must interact with other security services as attackers become more brazen and use less specific tactics. Therefore, we need to enhance our security protocols to stop new risks from emerging in the future 12.

4.4 Wireless Networks:

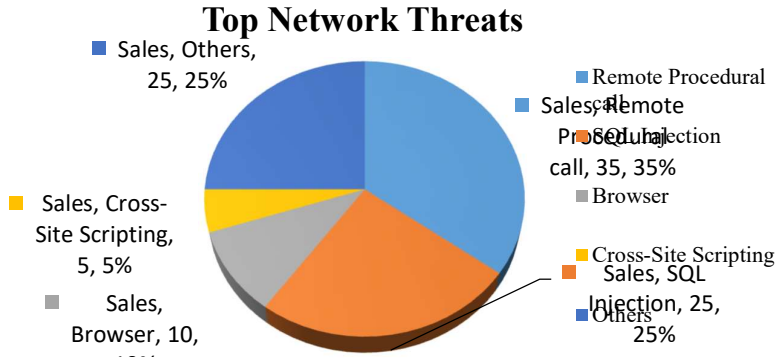
We can now communicate with anyone, anywhere in the globe. The security issue is the main task for mobile networks. As more people use devices like tablets, phones, PCs, and other gadgets, firewalls and other security measures are becoming more vulnerable. These devices also call for additional security protections on top of those offered by the programs they use. We need to be aware of these mobile networks' security concerns at all times13.

4.5 The New Internet Protocol, or IPv6:

The previous IPv4 protocol, which served as the foundation for both the Internet as a whole and our networks specifically, is being replaced by the new IPv6 system. It takes more than merely migrating IPv4 capabilities to secure IPv6. Although IPv6 comprehensively replaces IPv4, increasing the number of IP addresses available, there are several extremely important protocol modifications that security policies must take into account. Therefore, it is always preferable to upgrade to IPv6 as soon as feasible to lower the risks associated with cybercrime14.

4.6 Encryption of the code:

Encryption is the process of encoding messages (or information) in such a way that eavesdroppers or hackers cannot read it. In an encryption scheme, the message or information is encrypted using an encryption algorithm, turning it into an unreadable cipher text. This is usually done with the use of an encryption key, which specifies how the message is to be encoded. Encryption at the very beginning level protects data privacy and its integrity. However, more use of encryption brings more challenges in cyber security. Encryption is also used to protect data in transit, for example, data being transferred via networks (e.g. the Internet, e-commerce), mobile telephones, wireless microphones, wireless intercoms, etc. Hence by encrypting the code, one can know if there is any leakage of information15.



[11] https://www.coursehero.com/file/95700416/cloud-computingdocx

[12] https://www.coursehero.com/file/77143833/Assignment-1Roll-11docx

[13] https://arxiv.org/pdf/1402.1842

[14] https://www.coursehero.com/file/p283bqld/networks-Further-mobile-networks-are-highly-prone-to-these-cyber-crimes-a-lot-of

[15] https://www.science.edu/Enscitech/Encryption.html

5. CYBER SECURITY AND ROLE OF SOCIAL MEDIA

In an increasingly interconnected world, as we become more social, businesses need to come up with innovative solutions to safeguard personal data. Social media is a major contributor to personal cyber dangers and plays a significant role in cyber security. Employee use of social media is rapidly increasing, and with it, the danger of cyber attacks. Considering that the majority of them use social media or social networking sites virtually daily, this has made them a prime target for cybercriminals looking to steal important data and access personal accounts.16In a world where consumers readily divulge personal information, businesses must make sure they can recognize hazards, act quickly to address them and prevent breaches of any kind. These social media platforms draw users in, so hackers exploit them as bait to obtain the data and information they need.

Therefore, users need to take the necessary precautions, particularly when using social media, to ensure that their information is protected. One of the new threats noted in the Global Risks 2013 report is the quick dissemination of misleading information via social media. Even though social media might be used for cybercrimes, some businesses cannot afford to cease using it because it is crucial to their brand's visibility. To avoid problems, however, businesses should be aware of this, recognize how important it is to analyze information, particularly in social interactions, and offer suitable security solutions. Social media management requires the use of appropriate technologies and policies17.

6. TECHNIQUES OF CYBER SECURITY

6.1 Password security and access control:

The basic concept of a username and password has been a vital component of information security. This can be among the first actions to be taken in the context of cyber security.

6.2 Data authentication:

All documents we receive need to be verified before downloading; this means they need to be scrutinized to make sure they are legitimate and unaltered and that they come from a reputable source. The anti-virus software on the devices typically handles the authentication of these documents. Therefore, to safeguard the devices against viruses, effective anti-virus software is also necessary.

6.3 Scanners for malware:

This software typically checks all of the system's files and papers for dangerous viruses or malicious code. Malicious software is generally referred to as malware and includes programs like Trojan horses, worms, and viruses.

6.4 Protection against intrusions:

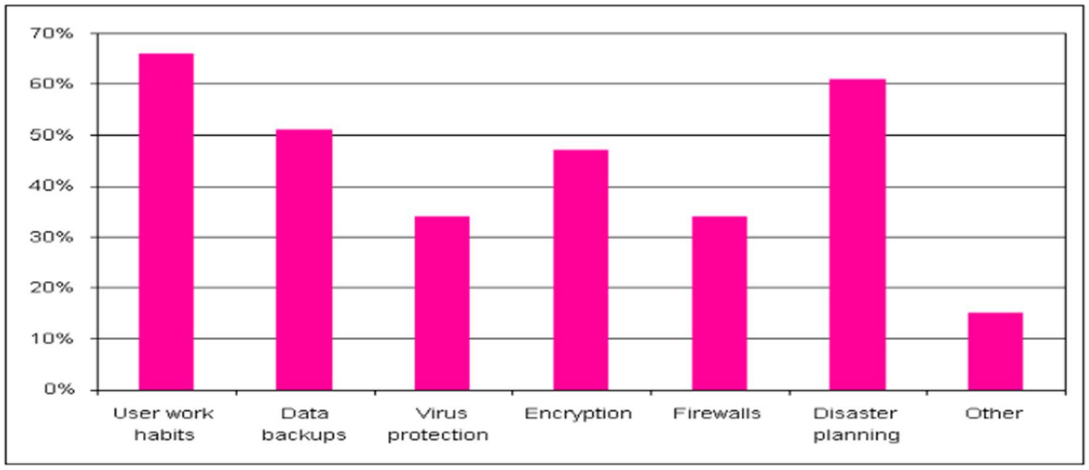
A firewall is a hardware device or program that helps prevent viruses, worms, and hackers from attacking your computer through the Internet. Every message that enters or exits the internet is filtered by the firewall, which checks each one and prevents those that don't fit the predetermined security requirements.

6.5 Software for antivirus:

Computer programs that detect, prevent, and take action are known as antivirus software.There are so many antiviruses available in the market. They are Kaspersky, AVG antivirus, Norton 360, etc, These antivirus software provide security to our computers by preventing malware from entering into a computer which may lead to the leakage of sensitive information. The following table explains the techniques of cyber security.

[16] https://www.chegg.com/homework-help/questions-and-answers/cyber-security-overview-world-re-quick-give-personal-information-companies-ensure-re-quick-q81428361

[17] https://www.academia.edu/40910470/A_STUDY_OF_CYBER_SECURITY_CHALLENGES_AND_ITS_EMERGNING_TRENDS_ON_LATEST_TECHNOLOGIES



Techniques on cyber security

7. CYBER ETHICS

Cyber ethics sometimes referred to as computer ethics or online ethics is the study of technology use that is morally and responsibly done, especially when it comes to the internet and digital communications. It entails thinking about the ethical and societal ramifications of technology as well as the proper ways for people, groups, and society to use it. There's a fair probability that we'll use the internet safely and appropriately if we put these cyber ethics into practice. Here are a handful of them:

- DO engage in social interaction and communication over the Internet. Staying in contact with friends and family, interacting with co-workers at work, and exchanging ideas and information with people nearby or across the globe is made simple by email and instant messaging.

- Refrain from being an online bully. Don't try to harm someone in any way, including calling them names, lying about them, sending embarrassing photos of them, or anything else.
- Since the internet is thought of as the world's largest library, it is always important to use this material properly and lawfully, covering any topic under the sun.
- Never use someone else's password to access their account.
- Never attempt to infect other people's systems with malware of any kind.
- Never give out your personal information to anyone since there's a high likelihood that someone else will misuse it and you'll wind yourself in hot water.
- Never try to build a phony account on someone else or claim to be someone else when you're online, as it could put both of you in danger.

These are some of the cyber ethics that one needs to abide by when using the internet. We are taught appropriate behaviour from an early age, and the same is true in cyberspace[18].

8. CONCLUSION

Because networks are being used to conduct vital transactions and the world is getting more interconnected, computer security is a broad topic that is growing more relevant. Organizations face challenges in protecting their infrastructure not just from emerging and disruptive technologies but also from constantly emerging cyber tools and threats that call for new platforms and intelligence. While there is no fool proof way to stop cybercrimes, we should do everything in our power to reduce them so that people can use the internet safely and securely in the future.

[18] https://www.linkedin.com/pulse/cyber-security-omkar-talekar?trk=public_profile_article_view