Shodh Sari-An International Multidisciplinary Journal

2023, Vol. 02, Issue 03, 26-41
ISSN: 2959-1376
DOI: https://doi.org/10.59231/SARI7590

Challenges and Emerging Trends in Cyber Security

Bora, Rajani

Assistant Professor, Department of Humanities and Social Sciences, JIET, Jodhpur.

Abstract

Cyber Security plays a very important role in the field of information technology. Securing the information has become one of the biggest challenges in the contemporary society. Whenever we think about the cyber security, the first thing that comes to our mind is 'cyber crimes' which are increasing tremendously day by day. Various government authorities and private organizations are taking many measures to prevent these cybercrimes. Besides various measures cyber security is still a very big concern to all of us. This paper mainly focuses on challenges faced by cyber security on the latest technologies. It also focuses on latest cyber security techniques, ethics and the trends changing the face of cyber security.

Keywords*:* *Cybercrime, Hacking, Phishing, Vishing, Cybersquatting, cyber security, social media, cyber ethics, android apps, cloud computing.*

INTRODUCTION

Today we are 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 we 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's life. In today's technical environment many latest technologies are changing the face of the human beings. But due to these emerging technologies we are unable to safeguard our private information in a very effective way and hence in these days' cybercrimes are increasing day by day. Today more than 70 percent of total commercial transactions are done online, so this field required a high quality of security for transparent and best transactions. Hence cyber security has become a latest issue. The scope of cyber security is not just limited to securing the information in IT industry but also to various other fields like cyber space etc.

@2023 International Council for Education Research and Training
ISSN: 2959-1376
2023, Vol. 02, Issue 03, 26-41
DOI: https://doi.org/10.59231/SARI7590

Even the latest technologies like cloud computing, mobile computing, E-commerce, net banking etc. also needs high level of security. Since these technologies hold some important information regarding a person their security has become a must thing. Enhancing cyber security and protecting critical information infrastructures are essential to each nation's security and economic wellbeing. Making the Internet safer (and protecting Internet users) has become integral to the development of new services as well as governmental policy. The fight against cybercrime needs a comprehensive and a safer approach. Given that technical measures alone cannot prevent any crime, it is critical that law enforcement agencies are allowed to investigate and prosecute cybercrime effectively. Today many nations and governments are imposing strict laws on cyber securities in order to prevent the loss of some important information. Every individual must also be trained on this cyber security and save themselves from these increasing cyber crimes

What is 'Cyber Crime'?

Cybercrime 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 cybercrime to include any illegal activity that uses a computer for the storage of evidence. (Lyne) The growing list of cybercrimes 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 cybercrime may be defined as crime committed using a computer and the internet to steal 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 cybercrimes also will increase along with the technological advances.

Types of cybercrime:

As we all know that cybercrime is a term generally used to describe criminal activity in which computers or computer networks are a tool, a target, or a place of criminal activity and include everything from electronic cracking to denial-of-service attacks. It is also used to include traditional crimes in which

@2023 International Council for Education Research and Training
ISSN: 2959-1376
2023, Vol. 02, Issue 03, 26-41
DOI: https://doi.org/10.59231/SARI7590

computers or networks are used to enable the illicit activity. Computer crime mainly consists of unauthorized access to computer systems data alteration, data destruction, theft of intellectual properly. Cybercrime in the context of national security may involve activism, traditional espionage, or information warfare and related activities. Some of these cybercrimes are as follows:

1. Cyber Stalking

Cyber stalking is use of the Internet or other electronic means to stalk someone. This term is used interchangeably with online harassment and online abuse. Stalking generally involves harassing or threatening behavior that an individual engages in repeatedly, such as following a person, appearing at a person's home or place of business, making harassing phone calls, leaving written messages or objects, or vandalizing a person's property. (Bocij, 2004)

Cyber stalking is a technologically-based "attack" on one person who has been targeted specifically for that attack for reasons of anger, revenge or control. Cyber stalking can take many forms, including:

1. Harassment, embarrassment and humiliation of the victim.
2. Emptying bank accounts or other economic control such as ruining the victim's credit score.
3. Harassing family, friends and employers to isolate the victim.

The term can also apply to a "traditional" stalker who uses technology to trace and locate their victim and their movements more easily (e.g., using Facebook notifications to know what party they are attending). A true cyber-stalker's intent is to harm their intended victim using the anonymity and untraceable distance of technology. In many situations, the victims never discover the identity of the cyber stalkers who hurt them, despite their lives being completely upended by the perpetrator.

2. Hacking

"Hacking" is a crime, which entails cracking systems and gaining unauthorized access to the data stored in them. Hacking had witnessed a 37% increase this year. A case of suspected hacking of certain web portals and obtaining the residential addresses from the e-mail

@2023 International Council for Education Research and Training
ISSN: 2959-1376
2023, Vol. 02, Issue 03, 26-41
DOI: https://doi.org/10.59231/SARI7590

accounts of city residents had recently come to light.(Erickson, 2008)

Crackers are people who try to gain unauthorized access to computers. This is normally done through the use of a 'backdoor' program installed on your machine. A lot of crackers also try to gain access to resources through the use of password cracking software, which tries billions of passwords to find the correct one for accessing a computer. Obviously, a good protection from this is to change passwords regularly.

In computer networking, hacking is any technical effort to manipulate the normal behavior of network connections and connected systems. A hacker is any person engaged in hacking. (Grossi) The term "hacking" historically referred to constructive, clever technical work that was not necessarily related to computer systems. Today, however, hacking and hackers are most commonly associated with malicious programming attacks on the Internet and other networks.

M.I.T. engineers in the 1950s and 1960s first popularized the term and concept of hacking. Starting at the model train club and later in the mainframe computer rooms, the so-called "hacks" perpetrated by these hackers were intended to be harmless technical experiments and fun learning activities. Later, outside of M.I.T., others began applying the term to less honorable pursuits. Before the Internet became popular, for example, several hackers in the U.S. experimented with methods to modify telephones for making free long-distance calls over the phone network illegally. As computer networking and the Internet exploded in popularity, data networks became by far the most common target of hackers and hacking.

3. Phishing

Phishing is just one of the many frauds on the Internet, trying to fool people into parting with their money. Phishing refers to the receipt of unsolicited emails by customers of financial institutions, requesting them to enter their username, password or other personal information to access their account for some reason. Customers are directed to a fraudulent replica of the original institution's website when they click on the links on the email to enter their information, and so they remain unaware that the fraud has occurred. The fraudster then has access to the customer's

@2023 International Council for Education Research and Training
ISSN: 2959-1376
2023, Vol. 02, Issue 03, 26-41
DOI: https://doi.org/10.59231/SARI7590

online bank account and to the funds contained in that account.(Milhorn, 2007)

Phishing is the act of sending an e-mail to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft. The e-mail directs the user to visit a Web site where they are asked to update personal information, such as passwords and credit card, social security, and bank account numbers, that the legitimate organization already has. The Web site, however, is bogus and set up only to steal the user's information.

For example, in 2003, we saw the proliferation of a phishing scam in which users received e-mails supposedly from eBay claiming that the user's account was about to be suspended unless he clicked on the provided link and updated the credit card information that the genuine eBay already had. Because it is relatively simple to make a Web site look like a legitimate organizations site by mimicking the HTML code, the scam counted on people being tricked into thinking they were actually being contacted by eBay and were subsequently going to eBay's site to update their account information. By spamming large groups of people, the "phisher" counted on the e-mail being read by a percentage of people who actually had listed credit card numbers with eBay legitimately.

Phishing, also referred to as brand spoofing or carding, is a variation on "fishing," the idea being that bait is thrown out with the hopes that while most will ignore the bait, some will be tempted into biting. (Stamp, ISBN: 978-0-470-62639-9.)

Phishing is an e-mail fraud method in which the perpetrator sends out legitimate-looking email in an attempt to gather personal and financial information from recipients. Typically, the messages appear to come from well-known and trustworthy Web sites. Web sites that are frequently spoofed by phishers include PayPal, eBay, MSN, Yahoo, BestBuy, and America Online. A phishing expedition, like the fishing expedition it's named for, is a speculative venture: the phisher puts the lure hoping to fool at least a few of the prey that encounter the bait. Phishers use a number of different social engineering and e-mail spoofing ploys to try to trick their victims.

@2023 International Council for Education Research and Training
ISSN: 2959-1376
2023, Vol. 02, Issue 03, 26-41
DOI: https://doi.org/10.59231/SARI7590

4. Vishing

One emerging threat called vishing has already affected thousands of people in the Midwest. In these cases, criminals use the power of Voice over Internet Protocol to spoof caller IDs and prey on unsuspecting financial institution customers. Believing the information displayed on their caller IDs is accurate, customers are willing to share their private personal and financial information with the caller who is not, as their caller ID claims, a financial institution employee.

Vishing (voice or VoIP phishing) is an electronic fraud tactic in which individuals are tricked into revealing critical financial or personal information to unauthorized entities. Vishing works like phishing but does not always occur over the Internet and is carried out using voice technology. A vishing attack can be conducted by voice email, VoIP (voice over IP), or landline or cellular telephone. (Markus Jacobsson and Zulfikar Ramzan)

Vishing is difficult for authorities to trace, particularly when conducted using VoIP. Furthermore, like many legitimate customer services, vishing scams are often outsourced to other countries, which may render sovereign law enforcement powerless.

Consumers can protect themselves by suspecting any unsolicited message that suggests they are targets of illegal activity, no matter what the medium or apparent source. Rather than calling a number given in any unsolicited message, a consumer should directly call the institution named, using a number that is known to be valid, to verify all recent activity and to ensure that the account information has not been tampered with.

5. Bot Networks

A cybercrime called 'Bot Networks', wherein scamsters and other perpetrators of cybercrimes remotely take control of computers without the users realizing it, is increasing at an alarming rate. Computers get linked to Bot Networks when users unknowingly download malicious codes such as Trojan horse sent as e-mail l attachments. Such affected computers, known as zombies, can work together whenever the malicious code within them get activated, and those who are behind the Bot Networks attacks get the

@2023 International Council for Education Research and Training
ISSN: 2959-1376
2023, Vol. 02, Issue 03, 26-41
DOI: https://doi.org/10.59231/SARI7590

computing powers of thousands of systems at their disposal. (Byrne, ISBN: 1-59749-135-)

Attackers often coordinate large groups of Bot-controlled systems, or Bot networks, to scan for vulnerable systems and use them to increase the speed and breadth of their attacks. Trojan horse provides a backdoor to the computers acquired. A 'backdoor" is a method of bypassing normal authentication, or of securing remote access to a computer, while attempting to remain hidden from casual inspection. The backdoor may take the form of an installed program, or could be a modification to a legitimate program. Bot networks create unique problems for organizations because they can be remotely upgraded with new exploits very quickly and this could help attackers pre-empt security efforts.

In a first of its kind initiative in India to tackle cybercrime, police have taken the initiative to keep an electronic eye on the users of the various cyber cafes spread over the city. The Kerala State IT Mission has launched a Web portal and a call center to tackle cybercrime. (The Hindu Business Line, Tuesday Jul 31, 2007). The Central Bureau of Investigation (CBI) and the Mumbai police have recommended issuance of licenses to cyber cafe owners.

Many countries, including India, have established Computer Emergency Response Teams (CERTs) with an objective to coordinate and respond during major security incidents/events. These organizations identify and address existing and potential threats and vulnerabilities in the system and coordinate with stakeholders to address these threats. Policy initiatives on cybercrime are as yet lethargic because of a general sense that it is nothing more than juvenile hackers out to have fun or impress someone. Prateek Bhargava, cyber law expert says, "There is huge potential for damage to national security through cyber-attacks. The internet is a means for money laundering and funding terrorist attacks in an organized manner.

What is '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

@2023 International Council for Education Research and Training
ISSN: 2959-1376
2023, Vol. 02, Issue 03, 26-41
DOI: https://doi.org/10.59231/SARI7590

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.

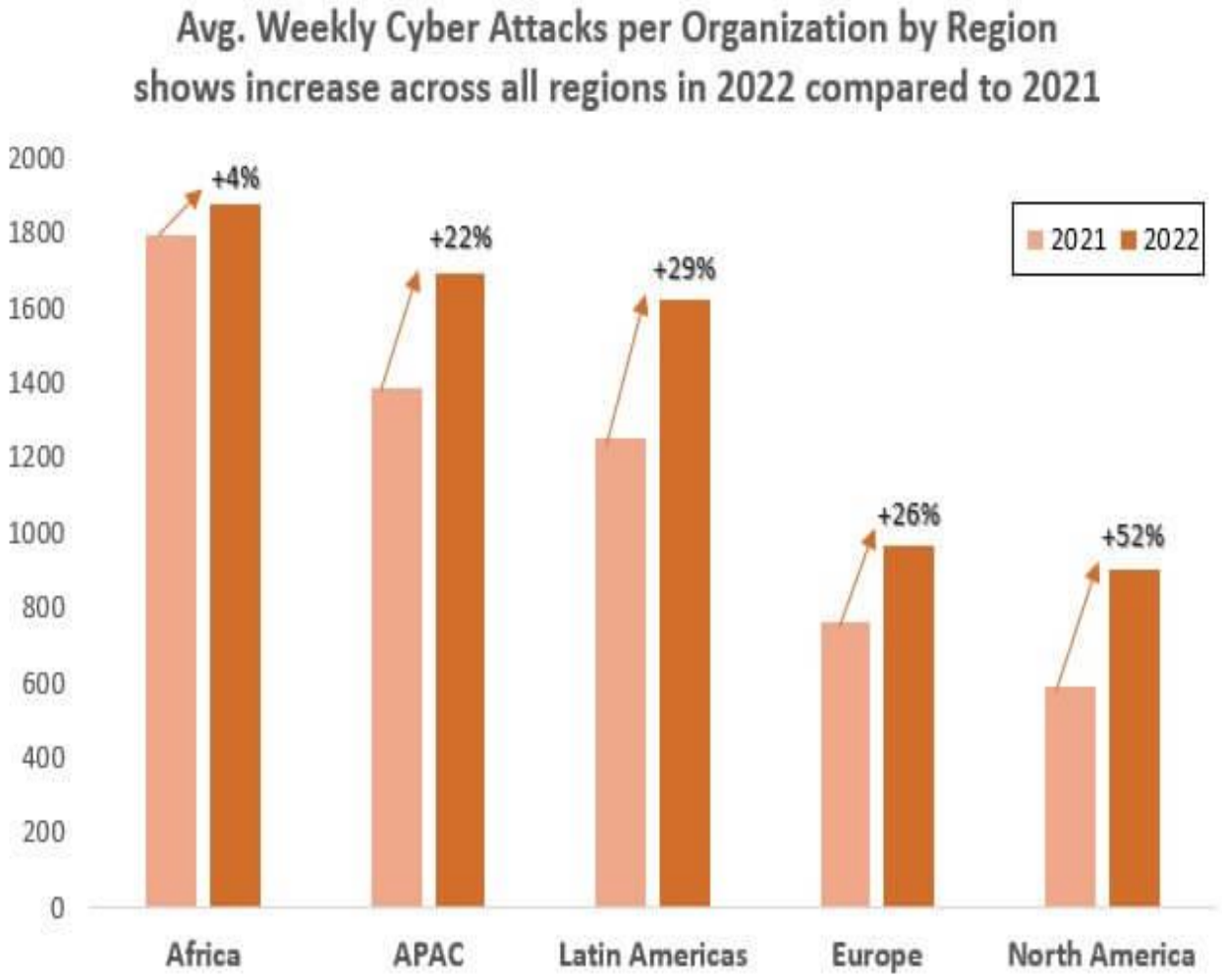


Fig. 1: Average weekly cyber-attacks as per organization by region shows increase across all regions in 2021-2022. (Check point research report)

It clearly exhibits the cyber security threats increases continuously. As crime is increasing even the security measures are also increasing. According to the survey of U.S.

@2023 International Council for Education Research and Training 2023, Vol. 02, Issue 03, 26-41
ISSN: 2959-1376 DOI: https://doi.org/10.59231/SARI7590

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.

1. 98% of companies are maintaining or increasing their cyber security resources and of those, half are increasing resources devoted to online attacks this year.

2. The majority of companies are preparing for when, not if, cyber-attacks occur.

3. Only one-third are completely confident in the security of their information and even less confident about the security measures of their business partners.

There will be many new attacks on Android operating system-based devices, but it will not be on massive scale. The fact tables share the same operating system as smart phones means they will be soon targeted by the same malware as those platforms. The number of malware specimens for Macs would continue to grow, though much less than in the case of PCs. Windows 8 will allow users to develop applications for virtually any device (PCs, tablets and smart phones) running windows 8, thus it will be possible to develop malicious applications like those for Android, hence these are some of the predicted trends in cyber security.

TRENDS CHANGING CYBER SECURITY

Below mentioned here are some of the trends that are having a huge impact on cyber security.

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. (Lyne)

@2023 International Council for Education Research and Training
ISSN: 2959-1376
2023, Vol. 02, Issue 03, 26-41
DOI: https://doi.org/10.59231/SARI7590

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 challenge for cyber security, as traffic can go around traditional points of inspection. Additionally, as the number of applications available in the cloud grows, policy controls for web applications and cloud services will also need to evolve in order to prevent the loss of valuable information. Though cloud services are developing their own models still a lot of issues are being brought up about their security. Cloud may provide immense opportunities but it should always be noted that as the cloud evolves so as its security concerns increase. (Lyne)

APT's and targeted attacks

APT (Advanced Persistent Threat) is a whole new level of cybercrime ware. For years network security capabilities such as web filtering or IPS have played a key part in identifying such targeted attacks (mostly after the initial compromise). As attackers grow bolder and employ more vague techniques, network security must integrate with other security services in order to detect attacks. Hence one must improve our security techniques in order to prevent more threats coming in the future. (Lyne)

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. Now-a-days firewalls and other security measures are becoming popular as people are using devices such as tablets, phones, PC's etc. all of which again require extra securities apart from those present in the applications used. We must always think about the security issues of these mobile networks. Further mobile networks are highly prone to these cybercrimes. A lot of care must be taken in case of their security issues. (Lyne)

IPv6: New internet protocol

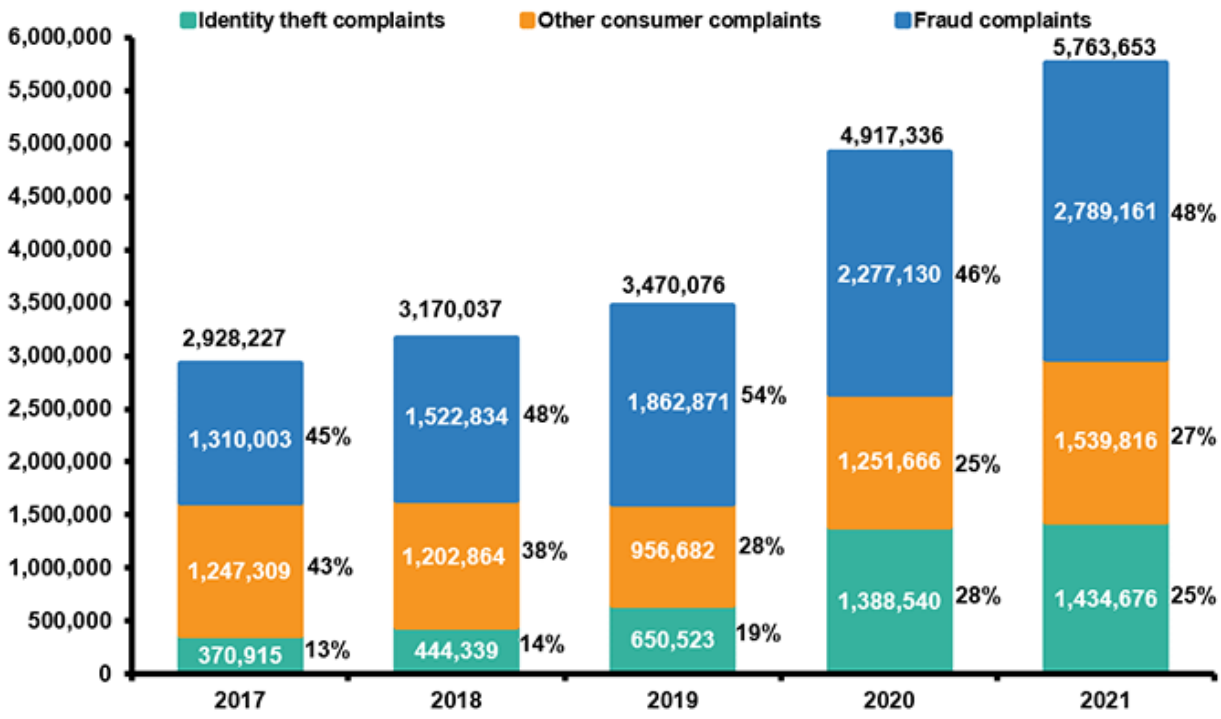
IPv6 is the new Internet protocol which is replacing IPv4 (the older version), which has been a backbone of our networks in general and the Internet at large. Protecting IPv6 is

@2023 International Council for Education Research and Training
ISSN: 2959-1376
2023, Vol. 02, Issue 03, 26-41
DOI: https://doi.org/10.59231/SARI7590

not just a question of porting IPv4 capabilities. While IPv6 is a wholesale replacement in making more IP addresses available, there are some very fundamental changes to the protocol which need to be considered in security policy. Hence it is always better to switch to IPv6 as soon as possible in order to reduce the risks regarding cybercrime. (Lyne)

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 a very beginning level protects data privacy and its integrity. But 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 information. (Lyne)



@2023 International Council for Education Research and Training
ISSN: 2959-1376
2023, Vol. 02, Issue 03, 26-41
DOI: https://doi.org/10.59231/SARI7590

Fig. 2: Major threats for networks and cyber security. (corrons)

Hence the above are some of the trends changing the face of cyber security in the world.

Role of social media incyber 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. (Godbole, 2011)

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 Risks 2013* report. (Global Risk 2013 eighth edition, 2013)

Though social media can be used for cybercrimes 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 recognize the importance of analyzing the

@2023 International Council for Education Research and Training
ISSN: 2959-1376
2023, Vol. 02, Issue 03, 26-41
DOI: https://doi.org/10.59231/SARI7590

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.

CYBER SECURITY TECHNIQUES:

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.

Authentication of data

The documents that we receive must always be authenticated be before downloading that is it should be checked if it has originated from a trusted and a reliable source and that

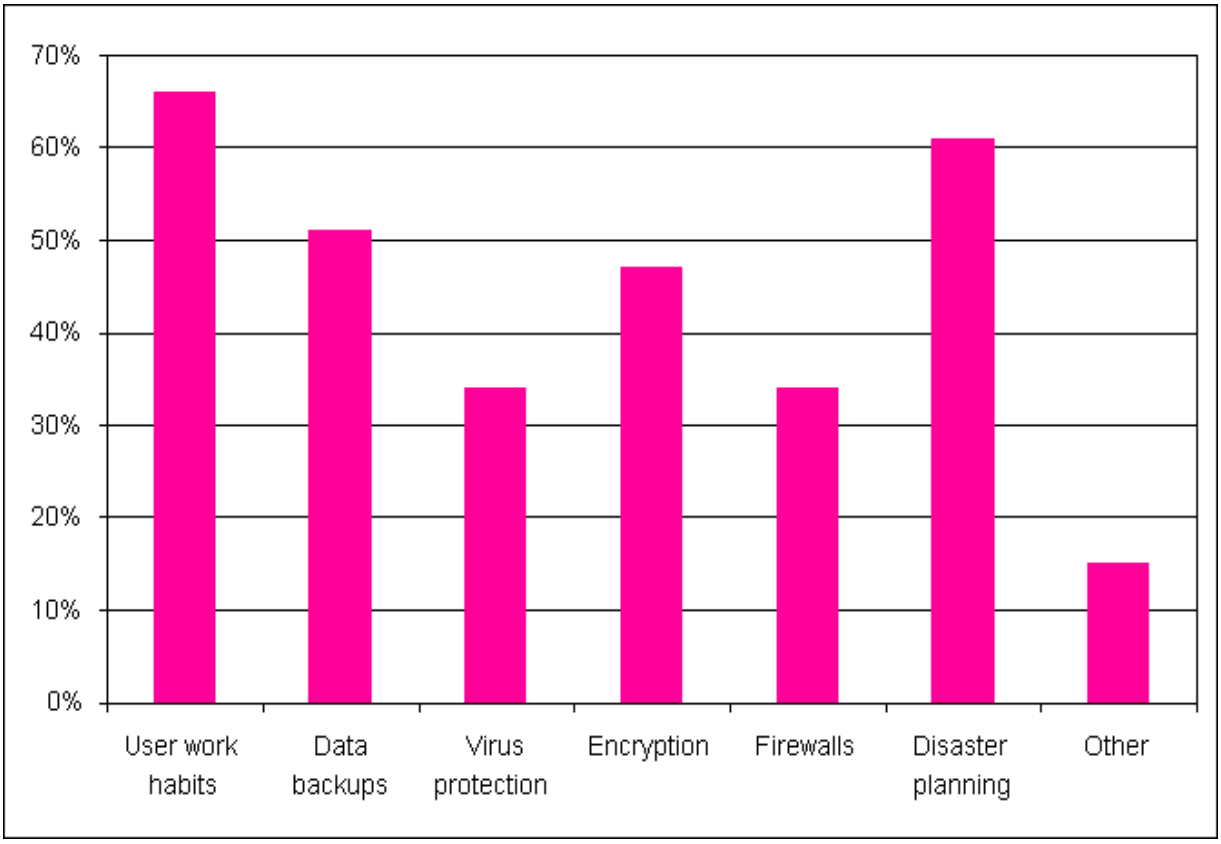


Fig. 3: Techniques of cyber security

@2023 International Council for Education Research and Training
ISSN: 2959-1376
2023, Vol. 02, Issue 03, 26-41
DOI: https://doi.org/10.59231/SARI7590

they are not altered. Authenticating of these documents is usually done by the antivirus software present in the devices. Thus, good antivirus software is also essential to protect the devices from viruses.
(Sunit Belapure)

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. (Sunit Belapure)

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. (Sunit Belapure)

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. Antivirus software is a must and basic necessity for every system. (Sunit Belapure)

Cyber ethics

Cyber ethics are nothing but the code of conduct to use the internet. It refers to a set of moral rules or a code of behavior applied to the online environment. (Krause) As a responsible netizen, we should observe these rules to help make cyberspace a safe place. If we practice these cyber ethics there will be good chances for us using the internet in a proper and safer way. The below are a few of them:

1. DO use the Internet to communicate and interact with other people**.** Email and instant messaging make it easy to stay in touch

@2023 International Council for Education Research and Training
ISSN: 2959-1376
2023, Vol. 02, Issue 03, 26-41
DOI: https://doi.org/10.59231/SARI7590

with friends and family members, communicate with work colleagues, and share ideas and information with people across town orhalfway around the world.

2. 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.

3. 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 wayis always essential.

4. Do not operate others accounts using their passwords.

5. Never try to send any kind of malware to other's systems and make them corrupt.

6. Never share our personal information to anyone as there is a good chance of others misusing it and finally, we would end up in a trouble.

7. When we're online never pretend to the other person, and never try to create fake accounts on someone else as it would land us as well as the otherperson into trouble.

8. Always adhere to copyrighted information and download games or videos only if they are permissible. (Krause)

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. Net surfing by youngsters lures them into dangerous domain. Cybercrime continues to diverge down different paths with each New Year that passes and so does the security of the information. (G Nikhita Reddy, Sept. 2013) 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 cybercrimes but we should develop and spread human values and try to our level best to minimize them in order to have a safe and secure future in cyber space.

Bibliography:

1. Bocij, P. (2004). "Cyber Stalking - Harassment in the Internet age and How to protect your family". *Library of Congress Cataloging-in-Publication Data* .

2023, Vol. 02, Issue 03, 26-41
ISSN: 2959-1376
DOI: https://doi.org/10.59231/SARI7590

2. Byrne, G. (ISBN: 1-59749-135-). *"Botnets – The Killer Web App",.* Syngress Publishing Inc.

3. *Check point research report.*

4. corrons, L. (n.d.). A Look back on cyber security 2012.

5. Erickson, J. (2008). *"Hacking – The Art of Exploitation".* William Pollock Publishers, 2nd Edition.

6. G Nikhita Reddy, G. U. (Sept. 2013). Study of cloud computing in health care industry. *International Journal of scientific and engineering research* , 68-71.

7. (2013). *Global Risk 2013 eighth edition.*

8. Godbole, N. (2011). *CYBER SECURITY: UNDERSTANDING CYBER CRIMES COMPUTER.* Wiley India.

9. Grossi, G. F. (n.d.). "Homeland Security – Technology Challenges from. *Library of Congress, US* , ISBN: 978-59693.

10. Krause, A. *Computer security practices.* Net action report.

11. Lyne, J. (n.d.). Eight trends changing network security. *A sophos article* .

12. Markus Jacobsson and Zulfikar Ramzan. *"Crime Ware- Understaning New Attacks and.* Symantec Press.

13. Milhorn, H. T. (2007). *"Cyber Crime – How to Avoid Beconing a Victim".* Universal.

14. Stamp, M. (ISBN: 978-0-470-62639-9.). *"Information Security – Principles and Practices",.* John Wiley & Sons Inc.

15. Sunit Belapure, N. G. *Understanding cyber security.*

16. The Hindu Business Line. (Tuesday Jul 31, 2007). *The central bureau of investigation* .

Received on March 30, 2023
Accepted on May 16, 2023
Published on July 01, 2023