INTERNATIONAL RESEARCH JOURNAL OF HUMANITIES AND INTERDISCIPLINARY STUDIES
(Peer-reviewed, Refereed, Indexed & Open Access Journal)
DOI : 03.2021-11278686 ISSN : 2582-8568 IMPACT FACTOR : 5.71 (SJIF 2021)

A Survey on Cyber Security in Covid 19 and Pandemic

Prof. Jyoti Mayur Bohra
Assistant Professor
V. P. Institute of Management Studies & Research,
Sangli (Maharashtra)
E-mail: jmbohra@vpimsr.edu.in

DOI No. 03.2021-11278686 **DOI Link::**https://doi-ds.org/doilink/08.2021-33211918/IRJHISICPC210853

Abstract:

Security in cyber world plays a vital role within the field of data technology. Whenever we expect about the cyber security the primary thing that involves our mind is 'cyber crimes' which are increasing immensely day by day. Many various organizations are working on task of removing cybercrimes. Besides various measures cyber security remains a really big concern to several. In Covid pandemic situation everyone is wholly dependent on cyber world and here in this paper, focus is on the cyber security techniques, ethics and the trends changing the face of cyber security.

Keywords: *cyber security, cybercrime, cyber ethics, technology.*

INTRODUCTION:

Today man is in a position to send and receive any sort of data could also be an e-mail or an audio or video just by the press of a button but did he ever think regarding the security of data which is being transmitted to the right destination .Cyber security is the key. Today Internet is the fastest growing infrastructure in everyday life But thanks to these emerging technologies we are unable to safeguard our private Since these technologies hold some important information regarding an individual their security has become a requirement thing. Cyber security plays a crutial role now a days. It is need of the hour to increase cyber security & protect important critical information. For this proper cyber security infrastructure is needed for countries security and economic wellbeing. Need to make Internet safer isvital to the development of new services as well as Government policy.

CONCEPT OF CYBER SECURITY:

Cyber security ensures the upkeep of the safety properties of the organization and user's assets against security risks within the networked environments

Elements of cyber security include:

- Application security which is the use of software, hardware, and procedural methods to protect applications from external threats.
- The details can vary greatly, counting on the dimensions and scope of a corporation and therefore the way it does business. For some businesses, issues like supply chain logistics are most vital and are the main target on the plan.
- Users need to know about how to avoid attacks and literate about cyber securityTraining on how to avoidedcybercrimes. Also, sometimes actions to be taken just in case if they're victim

CHALLENGES IN CYBER SECURITY:

Cyber security has been considered together of the foremost urgent national security problems. A report says, in a speech during his presidential campaign, President Obama promised to "make cyber security the top priority

Cyber security must address not only deliberate attacks like from disgruntled employees, industrial espionage and terrorists but inadvertent compromises of the knowledge infrastructure thanks to user errors equipment failures, and natural difficulties. Vulnerabilities might allow an attacker to penetrate a network, gain access to control software, and alter load conditions to destabilize a network in unpredictable means.

The defense of cyberspace necessarily involves the forging of effective partnerships between the general public organizations charged with ensuring the safety of cyberspace and people who manage the utilization of this space by myriad users like government departments, banks, infrastructure, manufacturing and repair enterprises and individual citizens. The protection of cyberspace has a superior feature. The national territory or space that's being defended by the land, sea and air forces is well defined. Outer space and cyberspace are dissimilar. They are inherently international even from the attitude of national interest.

CYBER CRIME:

Cyber crime may be a term for any criminality 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 incorporate any criminality that uses a computer for the storage of evidence. The growing list of cyber crimes includes crimes that are made possible by computers, like network intrusions and therefore the dissemination of computer viruses, also as computer-based

variations of existing crimes, like fraud , stalking, bullying and terrorism which became as major problem to people and countries. Usually in common man's language cyber crime could also be defined as crime committed employing a computer. More online transactions and digital data. Comparatively all organizations need to to be clearer than before. Majority of individuals want to access to corporate networks through their mobile devices for day to day activitiesthough smarter technology devices increases connectivity and but present latest sorts of security risks. Hackers can crack these securities and obtain a simple entry into corporate networks.

1. In December 2010, a famous E-business website was attacked by dozens of individuals claiming to be a part of the unnamed group. They attempted to perpetrate a denial of service attack in reprisal for website to shut down payment services to other websites. Many hackers were arrested in that crime.

METHODS OF ATTACKS AND AVOIDNESS:

Cyber terrorism is the use of computer viruses and worms. The attacks or methods on the pc infrastructure are often classified into three different categories.

• **Viruses**- These t ype of attack requires one to actually do something before it infects your computer. This action might be opening an email attachment or getting to a specific link.

• **Worms** - They typically start by exploiting a software vulnerability (a flaw that permits the software's intended security policy to be violated), then once the victim computer has been infected the worm will plan to find and infect other computers.

• **Trojan horses** -This is software that seems to be one thing but it acts differently behind the scenes. For example, a program that claims it'll speed up your computer may very well be sending tip to a foreign intruder.

• **Malicious code** - This category includes code such as viruses, worms, and Trojan horses. Although some people use these terms interchangeably, they need unique characteristics.

• **E-Mail Related Crime**- E-mails also are used for spreading disinformation, threats and Defamatory stuff.

• **Denial of Service** -These attacks is aimed at denying authorized persons access to a computer or computer network.

	Hardware	Software	Network
Common attacks	• Hardware Trojan • Illegal clones • Side channel attacks (i.e. snooping hardware signals)	• Software programming bugs (e.g. memory management, user input validation, race conditions, user access privileges, etc.) • Software design bugs • Deployment errors	• Networking protocol attacks • Network monitoring and sniffing
Examples of countermeasures	• Tamper-Resistant Hardware (e.g. TPM) • Trusted Computing Base (TCB) • Hardware watermarking • Hardware obfuscation	• Secure coding practice (e.g. type checking, runtime error, program transformation, etc.) • Code obfuscation • Secure design and development • Formal methods	• Firewall • Intrusion prevention and detection • Virtual Private Network (VPN) • Encryption

CYBER ETHICS:

Cyber ethics are nothing but the code of the web. When we practice these cyber ethics there are good chances folks using the web during a proper and safer way. Do use the web to speak and interact with people. Email and instant messaging facilitates in communicationwith each other. Don't be a bully on the Internet. Do not call people names, lie around them, send embarrassing pictures of them, or do anything to undertake to harm them.

Internet is taken into account as world's largest library with information on any topic in any discipline, so using this information during a correct and legal way is usually essential. Never use others accounts using their passwords.Never share your personal information to anyone as there's an honest chance of others misusing it and eventually you'd find yourself during a trouble.

When you're online never pretend to the opposite person, and never attempt to create fake accounts on somebody else because it would land you also because the other person into trouble.

Always adhere to copyrighted information and download games or videos as long as they're permissible. These are a few cyber ethics one must follow. We are always thought proper rules from out very early stages an equivalent here we apply in cyber space.

CYBER SECURITY TECHNIQUES:

Privacy and security of the info will always be top security measures that any organization takes care. In complex security information environment, all the information is maintained in a digital or a cyber-form. Social networking sites provide an area where users feel safe as they interact with friends and family. In the case of home users, cyber-criminals would still target social media sites to steal personal data. For bank transaction also one must be very careful & follow all security measures.

1 Access control and password security:

Login Credentials has been fundamental way of protecting our information. This may be one among the primary measures regarding cyber security.

2 Authentication of data:

All documents authentication needed prior to download to check their source (whether its trusted or not) and that they are not changed. Antivirus software helps in this. Thus an honest anti virus software is additionally essential to guard the devices from viruses.

3 **Malware scanners:**

This is software used to scan the files and documents present within the system for harmful viruses or code. Viruses, worms, and Trojan horses are examples of malicious software that are often

grouped together and referred to as malware.

4 Firewalls:

A firewall may be a software program or piece of hardware that helps sort hackers, viruses, and worms that attempt to reach your computer over the web. Firewall checks each incoming & outgoing message on web and blocks the one who don't meet the required security criteria

5 Anti-virus software:

Antivirus software may be a computer virus that detects, prevents, and takes action to disarm or remove malicious software programs, like viruses and worms. Most antivirus programs include an auto-update feature that permits the program to download profiles of latest viruses in order that it can check for the new viruses as soon as they are discovered. An anti virus software may be a must and basic necessity for each system.

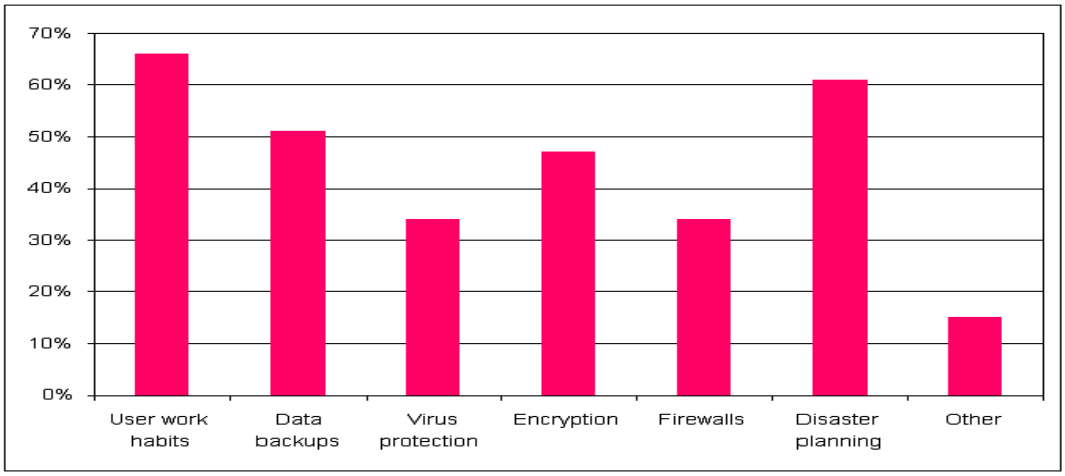

Table: Techniques on cyber security

CONCLUSION:

As there is a drastic growth in the e-commerce, internet or cyber security is a major issue in the growing countries like India. According to reliable forecasting survey, which announced that India will require five lakh cyber security professionals by 2015 to support its fast growing internet economy as per an estimate by the Union ministry of information technology. The financial sector alone is expected to hire over 2 lakh people while telecoms, utility sectors, power, oil & gas, airlines, government (law & order and e-governance) will hire the rest. Employment news says - Based on academic background and work experience, ethical hackers can don the roles of network security administrators, network defence analysts, web security administrators, application security testers, security analysts, forensic analysts, penetration testers and security auditors. The job role would be to develop and test IT products and services of organizations and ensure that they are as secure as possible. Secure programming, authorized hacking and network security surveillance are specializations in this domain.

ACKNOWLEDGEMENT:

This work was supported by our respected teachers department of Computer science of ICS College, khed. I thank to all myteahers, family and friends who have directly or indirectly supported my work.

REFERENCES:

1. A Sophos Article 04.12v1.dNA, eight trends changing network security by James Lyne.
2. http://www.cybersecuritycareers.com/
3. CSRDCI: http://perry4law.co.in/cs.html
4. Cyber Security: Understanding Cyber Crimes- SunitBelapure Nina Godbole
5. Computer Security Practices in Non Profit Organisations – A NetAction Report by Audrie Krause.
6. A Look back on Cyber Security 2012 by Luis corrons – Panda Labs.
7. *https://secureninja.com/.../national-initiative-for-cybersecurity-education-...*
8. http://study.taaza.com/study/top-ten-college-which-offer-cyber-security-course-in-india
9. 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
10. IEEE Security and Privacy Magazine – IEEECS "Safety Critical Systems – Next Generation "July/ Aug 2013.
11. CIO Asia, September 3rd, H1 2013: Cyber security in malasia by Avanthi Kumar
12. Col SS raghav: " cyber security in india's counter terrorism strategy"
13. Jeff Debrosse Research Director, ESET, North America: " Cybersecurity Review"
14. NandkumarSaravade, Director, Cyber Security and Compliance NASSCOM :Cyber Security Initiatives in India
15. *https://secureninja.com/.../national-initiative-for-cybersecurity-education-...*
16. https://www.academia.edu/40945973/CYBER_SECURITY_ISSUES_AND_CHALLENGES_A_REVIEW_ (1)
17. https://www.iesrj.com/download_pdf?doc=A_STUDY_OF_CYBER_SECURITY_CHALLENGES_AND_ITS_EMERGNING_TRENDS_ON_LATEST_TECHNOLOGIES (2)