IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

A REVIEW SWOT UP ON CYBER SECURITY

[1]Bhanu Sharma,[2]Pooja Kapila, [3]Aarju Tripathi

[1] Assistant Professor,[2] Assistant Professor [3]Software Engineer
[1]Chandigarh Engineering College Jhanjeri, Mohali-140307, India
[2]Chandigarh Engineering College Jhanjeri, Mohali-140307, India
[3]Volkswagen IT Services, Pune, India

Abstract: This paper highlights the needs of preventing cyber-crime. With regards to the cyber-crime issues that has been tremendously became a national issue, thus, this research is carried out with the aim of identifying what are the determinants factor for preventing cyber-crime.

Technology is on a never-ending cycle where it becomes more and more advanced with each day that passes. As we know, advancement in internet means we are getting Globalized (Globalization means we are getting closer to whole world via internet). Trade, Education, Research etc. are getting advanced day by day due to advanced and high- speed data transfer. We know Trade requires money transfer and for transferring money via internet we have to put our details online, also the details of our bank account and that’s where we talk about security. Now the question arises is how much secure is our credentials This question should rise in our mind before putting anything online.

This research looks upon the factors such as law enforcement, awareness program, and prevention process in combating cyber-crime issue. There are some recommendations highlighted as a scheme to combat cyber-crime issues and future research study for expansion and accuracy of the analysis.

1. INTRODUCTION

Now the question arise that what cyber-crime exactly means so there’s a brief definition about it i.e. The use of a computer as an instrument to further illegal ends, such as committing fraud, trafficking in child pornography and intellectual property, stealing identities, or violating privacy. We know concept like IoT, Machine Learning and Artificial Intelligence has made life easier but we should also be aware of what all can happen to our personal data when put online. A statement that is anything which is present on Internet is hackable so there’s nothing like a specific technique to maintain our privacy but there are various steps which we can use as precaution from this mis-happenings or frauds or spoofing. Today our lives is very much dependent on online services. We shop online, we work online, we play online we live online, we eat online. As our lives increasingly depend on digital services, the need to protect our information from being maliciously disrupted or misused is really importanttoo.

But most of us don’t care or ignore it carelessly without knowing about the consequences of data leak or being hacked. We can’t be sure anyhow that we are secured as

there’s always a loop hole in everything which can lead un to disastrous consequences so it’s better to be precautious about it in time so that we can be safe and guide others too for some of the measures which can make them feel safe with their credentials online.

Some of the kinds of Cyber-criminals are mentioned as below.

- Crackers: These individuals are intent on causing loss to satisfy some antisocial motives or just for fun. Many computer virus creators and distributors fall into this category.
- Hackers: These individuals explore others' computer systems for education, out of curiosity, or to compete with their peers. They may be attempting to gain the use of a more powerful computer, gain respect from fellow hackers, build a reputation, or gain acceptance as an expert without formaleducation.
- Pranksters: These individuals perpetrate tricks on others. They generally do not intend any particular or long-lasting harm.
- Career criminals: These individuals earn part or all of their income from crime, although they Malcontents, addicts, and irrational and incompetent people: "These individuals extend from the mentally ill do not necessarily engage in crime as a full-time occupation. Some have a job, earn a little and steal a little, then move on to another job to repeat the process. In some cases, they conspire with others or work within organized gangs such as the Mafia. The greatest organized crime threat comes from groups in Russia, Italy, and Asia. "The FBI reported in 1995 that there were more than 30 Russian gangs operating in the United States. According to the FBI, many of these unsavoury alliances use advanced information technology and encrypted communications to eludecapture"
- Cyber terrorists: There are many forms of cyber terrorism. Sometimes it's a rather smart hacker breaking into a government website, other times it's just a group of like- minded Internet users who crash a website by flooding it with traffic. No matter how harmless it may seem, it is still illegal to those addicted to drugs, alcohol, competition, or attention from others, to the criminallynegligent.
- Cyber bulls: Cyber bullying is any harassment that occurs via the Internet. Vicious forum posts, name calling in chat rooms, posting fake profiles on web sites, and mean or cruel email messages are all ways of cyberbullying.
- Salami attackers: Those attacks are used for the commission of financial crimes. The key here is tomakethe alteration so insignificant that in a single case it would go completely unnoticed e.g., a bank employee inserts a program into bank 's servers, which deducts a small amount from the account of every customer.

2. CYBERTHREATS

Even with firewalls, antivirus solutions, and cyber security awareness training for the employees, cybercriminals still manage to exploit any vulnerabilities or loop hole they found. This could be because they've discovered vulnerabilities that are not yet known to you.

Cyber-attacks are not a matter of "if," but "when" they will occur. Unless you somehow gain omniscience (if that happens, be sure to reach out and we can split the cost of a lotto ticket), there's really no way for you to know every single vulnerability that exists on your network or within your organization. Security risks come in all shapes, sizes, attack vectors, and levels of potency in the digital world.

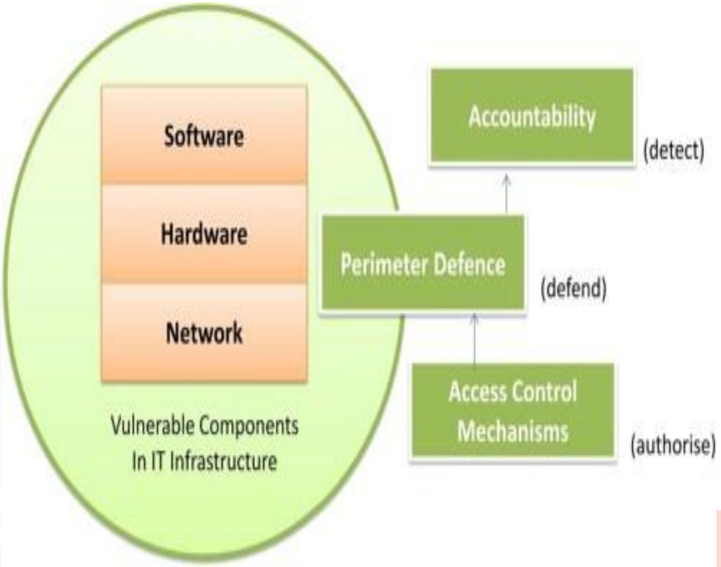
And, considering that threats to cyber security are continually changing and adapting, it's a challenge to keep up with them all. As these attackers are not limited with number of techniques to attack an organization.

So, the question arises what can you do? You can take the time to learn about as many cyber security threats as possible and work to identify and address as many holes in your defenses that you possibly can protect your organization (regardless of its size).

We know advancement can make life easier but as we know everything has two faces one positive and a negative side. When powers are used wisely for betterment then it's helpful but if the power is used in exploiting then it could be really disastrous. Some of the threats faced by organization are:

- Data Breaches-Enterprises are particularly at risk for data breaches, due to the amount of sensitive data they process. Just look at the Equifax breach where hackers stole birth dates, social security numbers and other personal data from millions of people. According toan article on MIT Technology Review, hackers may start targeting companies that compile data about personal web browsing habits, due to the companies' unregulatednature.
- IoT Vulnerabilities-For industries like healthcare, the growing use of IoT makes them a growing target for hackers, according to an article on Forbes. As more patients and healthcare providers useconnecteddevices to track and store sensitive medical data, the greater the chance they'll be targeted. These devices need the same level of cybersecurity protection that other devices and systems receive or they will become gateways to even bigger networks of personal data.

- Ransomware-While ransomware isn't a new threat, experts predict it will still be a major threat this year. As major cloud providers like Amazon, IBM and Google make major investments in their security, other smaller cloud- based companies will be the next likely target, according to an article on MIT Technology Review. With the amount of data, they hold, targeting them with a ransomware attack will still lead to a significantpayday.
- Insider Threats-Whether intentional or unintentional, employees can be a significant risk factor of organizations. Organizations put a lot of sensitive data in the hands of their employees and they can introduce a major threat with a few clicks. Implementing more sophisticated anti-virus software that uses the latest in behavioural and ransomware blockers can help protect the company. Pairing it with an in-depth cybersecurity education program can help ensure that employees are doing their part in identifying and avoiding threats to thebusiness.
- AI And Machine Learning-The recent advances in AI and machine learning are a double-edged sword for cybersecurity, according to an article on MIT Technology Review. Researchers and cybersecurity experts are using AI and machine learning to better anticipate attacks and identify them faster. But hackers are using this same technology to boost the effectiveness of theirattacks.



3. CYBERLAWS

To maintain the security constraints of all on online activities some of the rules and regulations are made so that the fear of being hacked minimizes. Cyber Law is the law governing cyber space. Cyber space is a very wide term and includes computers, networks, software, data storage devices (such as hard disks, USB disks etc.), the Internet, websites, emails and even electronic devices such as cell phones, ATM machines etc. Law encompasses the rules of conduct:

1. That have been approved by thegovernment.
2. Which are in force over a certain territory,and
3. Which must be obeyed by all persons on that territory. Violation of these rules could lead to government action such as imprisonment or fine or an order to paycompensation

Cyber law encompasses laws relating to:

1. CyberCrimes
2. Electronic and DigitalSignatures
3. IntellectualProperty
4. Data Protection andPrivacy

Cyber-crimes are cold acts where the computer is used either as a tool or a target or both. The enormous growth in electronic commerce (e-commerce) and online share trading has led to a phenomenal spurt in incidents of cyber-crime.

Electronic signatures are used to authenticate electronic records. Digital signatures are one type of electronic signature. Digital signatures satisfy three major legal requirements – signer authentication, message authentication and message integrity. The technology and efficiency of digital signatures makes them more trustworthy than hand written signatures which helps in both of the security constraints to be fulfilled i.e., Integrity and Confidentiality.

Intellectual property refers to creations of the human mind e.g., a story, a song, a painting, a design etc. The facets of intellectual property that relate to cyber space are covered by cyber law.

4. FUNDAMENTALS OF CYBERLAWS

Different fundamentals laws under Cyber Law are:

- Copyright law in relation to computer software, computer source code, websites, cell phone contentetc,
- Software and source codelicences
- Trademark law with relation to domain names, meta tags, mirroring, framing, linkingetc
- Semiconductor law which relates to the protection of semiconductor integrated circuits design andlayouts,
- Patent law in relation to computer hardware and software.

Data protection and privacy laws aim to achieve a fair balance between the privacy rights of the individual and the interests of data controllers such as banks, hospitals, email service providers etc. These laws seek to address the challenges to privacy caused by collecting, storing and transmitting data using new technologies.

5. Famous Attacks on Cyber Space

We know internet can be defined as collection of networks around the world and internet made us close to each other via text message, video conference etc. Internet gave birth to many facilities that no one ever dreamt of but everything has its advantages and disadvantages. Nothing is perfect and perfection can be called as myth as internet provides us of so many useful facilities but sometimes, we can severely suffer due to this too. It's not that Cyber Crime is a new thing and done only nowadays but it came to existence with the Internet's arrival.

There are some of those attacks which changed the perspective of those who think they are safe over Internet:

- **Robert Tappan Morris and the Morris Worm (1988)-** Creator of the first computer worm transmitted through the Internet, Morris, a student at Cornell University in the USA, claimed it his progeny was not aimed to harm but was made for the innocuous intent to determine the vastness of the cyberspace. Things went pear-shaped when the worm encountered a critical error and morphed into a virus which replicated rapidly and began infecting other computers resulting in denial of service. The damage? 6000 computers were reportedly affected causing an estimated $10-$100 million dollars in repairbills. While this event could be pinned as being an unfortunate accident, it no doubt played a part in inspiring the calamitous distributed denial-of-service (DdoS) type of attacks we see today.
- **Google China hit by cyber-attack (2009)-** Google entered the Chinese market with www.google.cn in 2006 and capitulated to China's stringent Internet censorship regime. The cyber-attacks in December 2009 resulted in the company's re- evaluation of its business in thecountry.In March 2010, Google relocated its servers for google.cn to Hong Kong in order to escape China's Internet filteringpolicy.
- **Teen hacks NASA *and* US Defence Department-** The year was 1999. Jonathan James was 15 at the time but what he did that year secured him a place in the hacker's hall of fame. James had managed to penetrate the computers of a US Department of Defence division and installed a 'backdoor' on its servers. This allowed him to intercept thousands of internal emails from different government organisations includingonescontaining usernames and passwords for various military computers. Using the stolen information, James was able to steal a piece of NASA software which cost the space exploration agency $41,000 as systems were shut down for threeweeks.
- **Phone lines blocked to win Porsche (1995)-** Kevin Poulsen is famous for his work in hacking into the Los Angeles phone system in a bid to win a Ferrari on a radio competition.LA KIIS FM was offering a Porsche 944 S2 to the 102th caller. Poulsen guaranteed his success as he took control of the phonenetwork and effectively blocked incoming calls to the radio station's number. He won the Porsche but the law caught up to him and he was sentenced to five years in prison. Poulsen later became the senior editor for IT security publication, Wired News.
- **MafiaBoy causes $1 billion dollars in damages (2000) -**Another 15-year-old that caused mischief in cyber space wasMichael Calce a.k.a.MafiaBoy.In 2000, Calce, now 25, was just a Canadian high school student when decided to unleash a DDoS attack on a number of high-profile commercial websites including Amazon, CNN, eBay and Yahoo!. An industry expert estimated the attacks resulted in a $US1.2-billion-dollar damage bill.He was later apprehended. Because he was still a juvenile, Calce was sentenced in 2001 to eight months in open custody, meaning his movements and actions would be restricted. His online access was also limited by the court. Calce and since scored gigs as a columnist and recently published a book about his ordeal.

4. "PREVENTION IS BETTER THANCURE"

As the tittle says about prevention better than cure which means if we apply some of the precautionary measures in our way of accessing or storing data on the Internet then to some extent, we can be safe from cyber-attacks. As the hackers are advancing regularly, we also have to keep our knowledge updated. MNCs hire Ethical Hackers to prevent their belongings and these Ethical Hackers have the duty to check and update the system on a regular basis so that there's no chance of getting any vulnerabilities. For a general user there are some of the measures by which he/she can save their privacy.

4.1 Steps to prevent cyber-crime: -

- Never disclose your personal information publicly on websites. This is as good as disclosing your identity to strangers in publicplace.
- Always avoid sending any photograph online particularly to strangers and chat friends as there have been incidents of misuse of thephotographs.
- Never enter your credit card number to any site that is not secured, to prevent itsmisuse.
- Always keep a watch on the sites that your children are accessing to prevent any kind of harassment or depravation in children
- Always use latest and updated Antivirus software to guard against virusattacks.
- To prevent loss of data due to virus attacks, always keep back up of yourdata.
- It is advisable to use a security program that gives control over the cookies and send information back to the site, as leaving the cookies unguarded might provefatal.
- Use of firewalls provesbeneficial.
- Website owners should watch traffic and check any irregularity on the site. Putting host-based intrusion detection devices on servers will serve thepurpose.

5. Conclusion

Capacity of human mind is profound. It is not possible to eliminate cyber-crime from the cyber space. It is quite possible to check them. History is the witness that no legislation has succeeded in totally eliminating crime from the globe. The only possible step is to make people aware of their rights and duties and to guard ourselves so that crime has no effect on us. Internet is very vast and we can't even imagine how each node is connected to other. Therefor for our security we have to take some measures and be aware of the new techniques. Today technology is getting advanced in every minute seconds so for keeping us safe online is our own responsibility and for that main thing is that we have to be aware of the consequences of any steps wetook.

References

[1] https://www.thebci.org/news/top-5-cyber-threats-facing- your-organization.html
[2] https://www.uscybersecurity.net/risks-2019/
[3] ASCL publication titled "IPR & Cyberspace - the Indian Perspective
[4]https://www.arnnet.com.au/slideshow/341113/top-10- most-notorious-cyber-attacks-history/
[5]http://cybertimes.in/?q=node/540
[6]https://www.computer.org/publications/tech- news/trends/5-cybersecurity-threats-to-be-aware-of-in- 2020/
[7]https://securityfirstcorp.com/the-top-9-network- security-threats-of-2019/
[8]https://www.britannica.com/topic/cybercrime
[9]https://www.guru99.com/cybercrime-types-tools- examples.html
[10]https://www.avast.com/c-cybercrime

IJCRT