CYBER CRIME AND SECURITY

[1]Mr.J.Jelsteen , [2]M.Mithra , [3]M.Reefath Sulthana

[1]Assistant professor,MCA.,M.Phill.,(P.hD), Department of BCA

[2,3]II BCA 'A',Department Of BCA

[1,2,3]Sri Krishna Arts And Science College,Coimbatore

[1]Email:jelsteenj@skasc.ac.in

[2]Email:mithram17bca024@skasc.ac.in

[3]Email:reefathsulthanam17bca040@skasc.ac.in

Abstract:

A special emphasis or power on the internet,where the opportunities provided by the information and communication technologies has became an essential part of our daily life. There are security issues within the cyber space that represent a security risk and challenge of recent time. this models gives an overview about the securities of our privacy needs. major security is the information and network security.

Introduction:

Cyber security is a field within IT involving the protection of computer and the prevention of unauthorised use of electronic data. It involves the protection of software , hardware and its information. It also protects computer from theft or damage.the heavy reliance on computer in the modern industry that store and transmit confidential informations.

Definition:

Cyber security or information technology are the techniques of protecting computers,networks,programs and data from unauthorized access or attacks that are aimed for destruction.[1]

Description:

Major areas covered in cyber security are:

1. Application Security
2. Information security
3. Disaster recovery
4. Network security

1)Application Security:

Application security (AS) is the use of procedural methods, hardware and software to protect the applications from external threats or danger.

2)Information Security:

Information security (IS) is designed to protect the confidentiality, integrity and availability of computer system data from those with malicious(venomous) intentions.

3)Disaster Recovery:

Disaster recovery (DR) is an area of security planning that intends to protect an organization from the effects of remarkable negative phenomenon.

4)Network Security:

Network security is an activity designed to protect the solidarity of your network and data. It includes both hardware and software technologies. It targets a variety of threats and stops them from invading or escalating on your network.

Figure 1

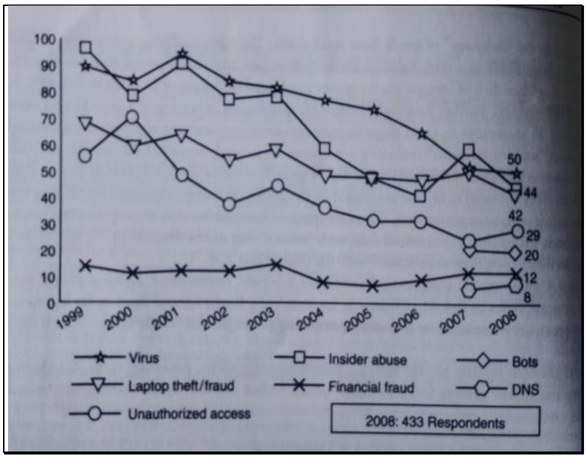


Figure 2

Current trends in Cyber Security

There are 5 Cyber Security challenges and trends:

1. Ransomware Evolution:

Ransomware is the bane (destruction) of Cyber Security, IT, data professionals, and executives.Ransomware attacks is one of the areas of cybercrime growing faster.The number of attacks has risen upto 36% currently.

2. AI Expansion (Artificial Intelligence):

Robots might be able to help and defend against the incoming cyber-attacks.

3. IOT Threats (Internet of things):

The Internet of Things will make sure that every single device you own is connected.

4. Blockchain Revolution:

A blockchain is a growing list of records, called *block*.Privateblockchains have been proposed for business use.

5. Serverless Apps Vulnerability:

Serverless apps are most commonly known as web service and data processing tools.Serverless apps can bid cyber-attacks.

Advantages of Cyber Security[3]:

1.Protects the system against viruses,worms,spyware and other unwanted programs.

2.Protection against data from robbery.

3.Protects the computer from being hacked.

4.Minimizes computer freezing and crashes.

5.Gives privacy to the users.

Disadvantages of Cyber Security:

1.Firewalls (network device) can be difficult to configure correctly.

2. It may block users from performing certain actions on the internet,until the firewalls are configured correctly.

3.It makes the system slower than before.

4.Need to keep updating the new software in order to keep security upto date.

5.It could be costly for average users.

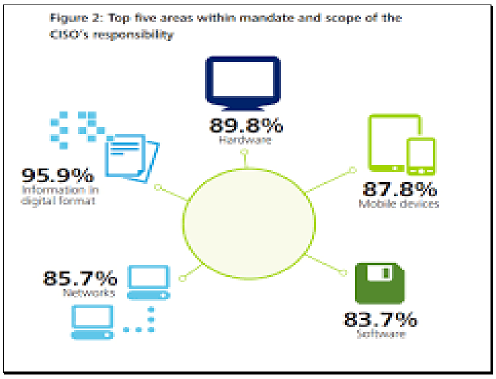


Figure 3

The Major causes of cyber security attacks

1. Faling to hide its basics.
2. Not understanding what generates corporate cyber security risks.

3. Inadequate policy.

4. Perplexed compliance with cyber security.

5. Human factor – the weakest link.

6. Bring your own device policy (BYOD) and the cloud.

7. Funding and resources constraints.

8. No information training.

9. Lack of a retrieval plan.

10. Constantly rising risks.

The 10 most common Cyber attack types[5]:

1. Denial-of-service (DOS):

   DOS is a cyber attack in which the hacker seeks to make a network resource unavailable to users temporarily or permanently disrupting serivices of the host connected to internets.

2. Man-in-the-middle (MITM) attack:

   MITM is an attack where the attacker secretly relay and alter the communication between two peoples,who believe that is a private connection,but that conversation is controlled by thehacker.

3. Phishing and spear phishing attacks:

   Attackers attempts to trick victims to share the sensitive informations like,password and credit card details.

4. Drive-by attack:

   Method of spreading malware into the unsecured websites.one who visits the websites, would directlyinstall the malware.

5. Password attack:

   Thepasswordcrackingistheprocess.recovering passwords or easily crackablepassword to make an unauthorized access to a system.

6. SQL injection attack:

   It is a code injection technique , used to attack data driven applications in sql statements are inserted into an entry field.

7. Cross-site scripting (XSS) attack:

This is also known as XSS , enables attackers to inject client side scripts into web pages which viewed by number of users.

8. Eavesdropping attack:

It is a sudden attack , where someone tries to steal information on computer or smart phones or other electronic device which transmit over a network.

9. Birthday attack:

A birthday attack can be used to find collision in a cryptographic hash functions.

10. Malware attack:

Malware performs activities on victims computer without their knowledge.

Examples: spyware, ransomeware (this is more than a word virus).

8 Tips to reduce the risk of a Cyber attack[6]:

1.Strengthens your current security system.

2.Use patches (walls).

3.Safeguard your outbound data.

4.Increase awareness.

5.Be acute about passwords.

6.Don’t ignore physical security.

7.Encrypt data.

8.Procure a cyber insurance policy.

Figure 4

Cyber Security Applications[7]:

Mobile:

Mobile security is a protection of smart phones, laptops, other portable electronic devices and networks they connect to from threats and vulnerability associated with wireless computing. This is also known as wireless security.

Document Signing:

Document signing is a software that allows you to sign documents electrically without printer or scanner etc,..It is a profit for business and personal use. Electronic signatures are trusted by millions and is available in dozens of languages.

Strong Authentication:

Strong authentication is any method that is used to verify the identity of the user or the device that is intrinsically stringent enough to ensure the security of the system and protects them by withstanding from any attacks.

Virtual Private Networks:

It is a programming that creates a safe and encrypted connection over a low secured network. A VPN works by utilizing the shared public infrastructure by maintaining privacy through security.

Secure Communication:

Secure communication provides a range of information security solutions to ensure communication security over public and local network. Software id developed in accordance with industry standard protocols and services.

Online Validation:

Automatic Strong Authentication validates the status of every secure connection request whether logging into a remote application opening a file on your local machine or device. The online service can process thousands of requests per second.

Secure Email:

A secured encrypted email solution that requires no software and allows professional practices to communicate sensitive data and informations safely.

Smart Cards:

The circuits in smart cards are encased in a plastic shell that is designed to tamper resistant. The card itself is designed to store encryption keyes and other informations used in authentication.

Counterfeit Prevention:

The risk of purchasing counterfeit components and having them enter into the supply chain is an ongoing problem.our goal is to provide guidance about the procedures and practices , receiving and installing counterfeit electronic parts.

Time Stamping:

In computing time stamping refers to the use of an electronic time stamp to provide a temporal order among a set of events. This is a sequence of characters or encoded information. The sequencial numbering of events somrtimes called time stamping.

example : When was this record created or last modified?

Code Signing:

Code signing is the process of digitally signing executables and scripts to confirm the software author and guarantee the code has not been altered. The process uses a cryptographic hash to validate the integrity.

Single Sign-on:

Single sign on is a property of access control of multiple and related software systems, it is an authentication process that allows a user to access multiple applications.

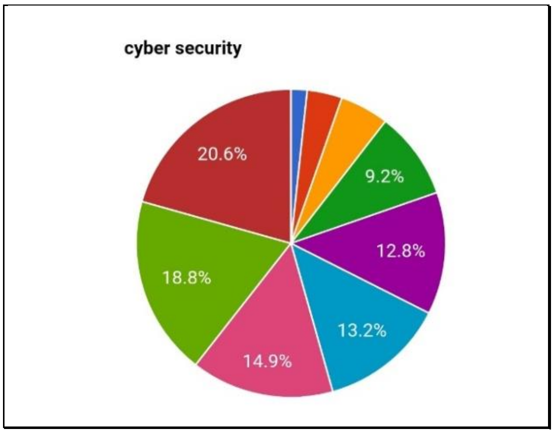
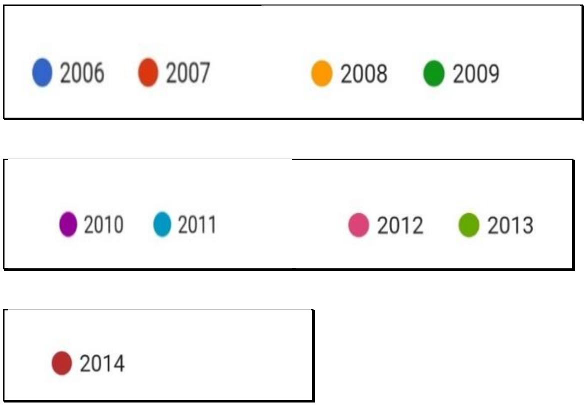


Figure 5



A pie chart representing how Cyber Security has been increased from 2006 till 2014 is being displayed in the above shown image.

Conclusion:

The future of cyber security will in sense be like the present : hard to define and potentially unbounded and as digital technologies interact with human beings.The most insight is gained when particular organisation use scenarios like positioning, capability and risk tolerance.

Reference:

[1] Schatz, Daniel; Bashroush, Rabih; Wall, Julie (2017). "Towards a More Representative Definition of Cyber Security". Journal of Digital Forensics, Security and Law. 12 (2). ISSN 1558-7215.

https://economictimes.indiatimes.com/definition/cyber-security

[2] "Reliance spells end of road for ICT amateurs", 7 May 2013, The Australian

https://www.globalsign.com/en-in/blog/cybersecurity-trends-and-challenges-2018/

Author : john mason

Published : may 7,2013

[3] Turner, Rik (May 22, 2018). "Thinking about cyberattacks in generations can help focus enterprise security plans". Informa PLC. Ovum.

https://sites.google.com/site/xinyicyber/the-disadvantages-and-advantages-of-cyber-security

[4]Author : Han Ping Fung

[5]Villasenor, John (2010). "The Hacker in Your Hardware: The Next Security Threat". *Scientific American*. **303** (2): 82–88. Bibcode:2010SciAm.303b..82V. doi:10.1038/scientificamerican0810-82. Archived from the original on 12 March 2014.

https://blog.netwrix.com/2018/05/15/top-10-most-common-types-of-cyber-attacks/

Author: villasenor

Published: Mar12,2014

[6] Kelly Jackson Higgins (18 November 2008). "Secure OS Gets Highest NSA Rating, Goes Commercial". Dark Reading. Archived from the original on 3 December 2013.Retrieved 1 December 2013.

https://www.sadlerco.com/8-tips-to-reduce-the-risk-of-a-cyber-attack/

Author:Kelly Jackson Higgins

[7] *YuanzhongXu, Alan M. Dunn, Owen S. Hofmann, Michael Z. Lee, Syed Akbar Mehdi, and Emmett Witchel (23 November 2014). "Application-Defined Decentralized Access Control". Proceedings of the Usenix ... Annual Technical Conference.Usenix Technical Conference.* ***2014****: 395–408. PMC 4241348. PMID 25426493*

http://www.sio2corp.com/cyber-security-applications/