Cyber Security: The Need for Today's Environment

[1]Jayesh Patil, [2]Keshav Sule, [3]Jagjot Singh Saini
[1]Yashwant Public School, MHOW, MP, India
[2]Indore Public School, Indore, MP, India
[3]The Emeralds Heights International School, Indore, MP, India

Abstract
Cybersecurity first came into consideration in the year 1988, as a result, one of the first ever registered online virus "The Morris Worm" the worm caused as many as of the 60,000 computer connected to the internet get affected by the worm and slow down. More recently cybersecurity has come to signify a form of protection from attacks designed to paralyze website, financial networks and other computer systems by flooding them with data from outside computer. At present, the biggest challenge is to secure information from cyber-attacks. Cybercrime is the main aspect of which we are moving toward the cybersecurity as they are increasing immensely day by day. In order to prevent these cybercrimes governments and companies are taking several measures i.e., governments are making strict laws against cybercrimes and companies are hiring data science specialist.

In this research paper, we talk about what is cyber security, cyber-attacks, types of attacks, governing bodies and how to be secure from such type of attacks?

Keywords
Cyber Security, Cyber Attacks, Cyber Crimes, Cyber Ethics, Social Networking, Cloud Computing, Risk, Threat, Vulnerability, Breaching, Governing Bodies.

I. Introduction

In this competitive world, everyone wants to be fast and easy their daily lives so people are attracting towards online services like transactions, shopping, etc. To access this service everyone needs to provide their personal information and to keep this information secure from breaching everyone needs to be aware of cyber security which can assist them to evade from major nuts of frauds.
For example, an online payment, we provide our private information like account number, pin, username and passwords which can be used by hackers to steal money from our account which can lead to bank frauds.

A bank fraud from the UK British banks accounted to lost approx. tens of millions of pounds after a gang of Russian hackers affected network in about 100 of financial institutions worldwide using a computer virus. The hacker used to manage bank computer system for months using a malware which helps them collecting the bank user information from the internal computer system and the gang used it to manipulate bank accounts. This incidence introduces a new stage in the emergence of cybercriminal exercise where greedy users avoided targeting local user and directly steal money from banks [1].
A cyber scam faced by a well-known company Yahoo was reported by them in September 2016 that around 3 billion Yahoo user data was breached in 2014. After four months they also disclosed a cybercrime which compromised the breach of data in 2013 of more than billions of Yahoo user. The company did not explain that why it took them such a long time to report these breach which could lead them to a problem with regulators [2].

Fig. 1:

Although cybersecurity is transforming, cybercrime is also transforming tremendously day by day. Nowadays crime has become the ceaseless news headline this transformed from a perceived threat to actual headline. Since cooperative and government bodies seem helpless in securing the data from cybercrime hacker's world. Breaching and another form of cyber mischief has reached a complexness that the credential of many companies to defeat against the crime. To move parallel to this competitive world we also need to transform and be aware with the cybercrime tactics i.e. cyber-attacks, breaching, viruses, vulnerability and many other threats.
The practice of cybersecurity ensures integrity, confidentiality, and availability of information. It preserves you against the accidents like hard drive failure, power outage, adversary's attacks capable of executing advanced persistent made by hackers and criminals. Makes serious threats to enterprise data. Security should be mandated to senior enterprise authority. Strong cyber security controls are required as information is very fragile these days. The highest priority should be given to employee training and standardized security which should be looked at by the management.

Table 1: The Comparison of Cybersecurity Circumstance Mentioned in Cyber999 in Malaysia from January-June 2012 and 2013 Clearly Exhibits the Cyber Threats [3].

Incidents	Jan-June 2012	Jan-June 2013	% Increase/ (Decrease)
Fraud	2439	2490	2
Intrusion	2203	1726	(22)
Spam	291	614	111
Malicious Code	353	442	25
Cyber Harassment	173	233	35
Content Related	10	42	320
Intrusion Attempts	55	24	(56)
Denial Of Service	12	10	(17)
Vulnerability Reports	45	11	(76)
Total	5581	5592	

II. What is Cyber Security?

Cybersecurity as the name itself suggests that it is used to protect against the criminal or unauthorized use of data or the measure taken to achieve it. This field is of great importance due to increasing reliance on a computer system. Cybersecurity refers to a set of techniques used to shield the integrity, program, and data from attacks, damages or unauthorized access. Cybersecurity reports in the safeguarding and recovering from casualty such as hard disk failure or power outage and also from an attack of adversaries [4].

Fig. 2:

Major areas covered by cyber security are:

Application Security - The measures that are taken during the development stage of application to protect it from threats that can come through defects in the application design, development, deployment, upgrade and maintenance.

Some techniques used for Application Security are

- Input Parameter Validation.
- User/Role Authentication and Authorization.
- Session Management, Parameter Manipulation and Exception Management.
- Auditing and Logging.

Information Security - It is used to safeguard information from unauthorized access of personal detail avoiding identity theft and protects privacy.

Major techniques used to cover Information Security are:

- Identification, Authentication, and Authorization of user.
- Cryptography.

Disaster Recovery - This is a process that includes performing risk assessment, establishing priorities, development recovery strategies in case of a disaster. Any business should have a concrete plan for disaster recovery to resume normal business operation as quickly as possible after a disaster.

Networking Security - This includes activities to protect the usability, integrity, reliability, and safety of the network. Effective network security finds a variety of threats and blocks them from disturbing or spreading on the network.

Components of network security are

- a) Anti-virus and Anti-spyware.
- b) Firewall to block unauthorized access to your network.
- c) IPS-Intrusion Prevention System is used to figure out fast-spreading threats such as zero-day or zero-hour attacks.
- Virtual Private Networks (VPNs to provide secure remote access)[5].

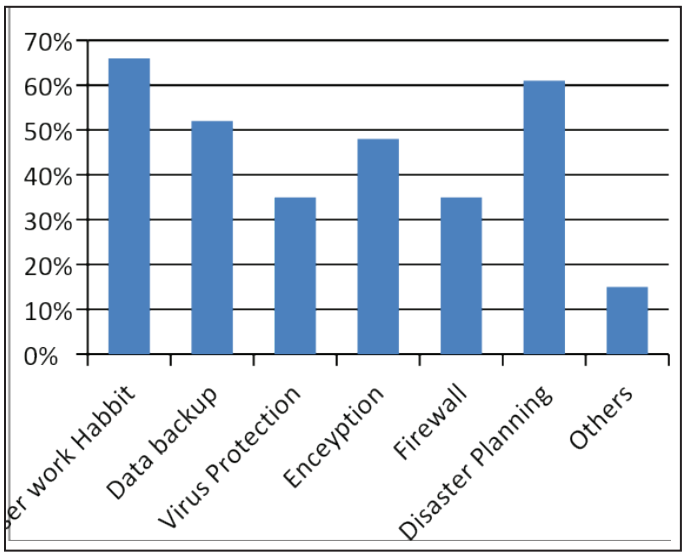

Fig. 3:

A. Types of Cyber Threats

1. Attacks on Confidentiality

Many methods are used by hackers to compromise confidentiality following are some common method.

(i). Packet Capturing

Commonly known as packet sniffing is a type of attack in which data packets are captured typically Ethernet frames. Once the capturing of data is done attackers can go through sensitive information like password and card numbers, unless the network traffic is not encrypted. Wire shark is the most popularly used packet capture software.

(ii). Password Attackers

For accessing the computer password hackers are used to hack the password of target computers and brute force attack.

(iii). Port Scanning and Pig Sweeps

By using port scanning method attackers scanning the TCP/UDP ports try to discover service running on the target computer. Here the attacker tries to attack the Ports because of which the attackers could find out software products running on target computers. Finally, attackers negotiating vulnerability in that product. A Pig Sweep is a network where the intruder tries to send ICMP ECHO packets to a range of IP ADDRESS ICMP ECHO REPLY. Thus attackers can identify which computers are up and which are down.

(iv). Dumpster Diving

Searching through company's dumpster for any useful information so that the network could be attacked.

(v). Wiretapping

In this type, the telecommunications devices are undertaken to listen to the phone calls of others.

(vi). Phishing and Pharming

In phishing sensitive information is tried to be sourced such action financial details including a password is tried to be extracted by email and fake URLs. Pharming aims at redirecting the traffic of one website to another.

(vii). Keylogger
It is a program that runs in the background of the computer which logs the user keystrokes. Whenever the user enters a password, the password is stored in the log created by the keylogger and forwarded to the attacker.

(viii). Social Engineering
It is performed by a person who is having very good interactive skills through which they manipulate others and reveal information about the network to steal information.

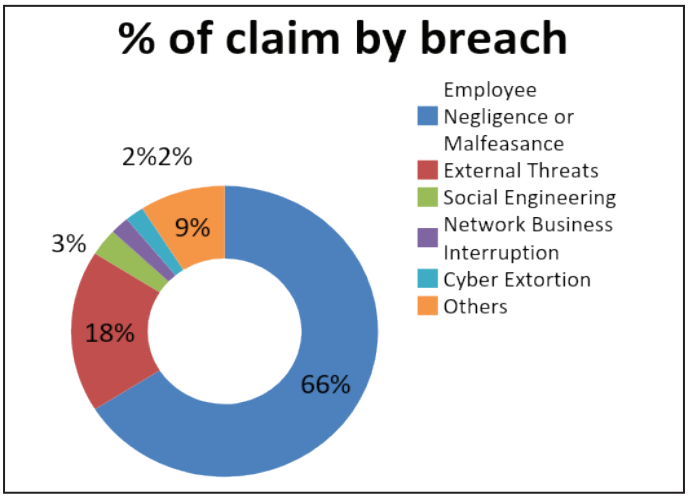

Fig. 4:

2. Attacks on Integrity

(i). Salami Attacks
Series of minor data attacks which together results into a major attack. Example when a deduction of the small amount of money is done from various accounts all together it becomes a large amount.

(ii). Data Diddling Attacks
When data is altered illegally or unauthorized. Changing data before or it is input into a computer or output.

(iii). Trust Relationship Attacks
Exploration of the network between different devices is the trust relationship attack.

(iv). Man in The Middle Attack
In this type, the attacker sits in between the communicating devices and manipulates data as it moves between them.

(v). Session Hijacking Attack
Hacking of computer session to access information or services in a computer system illegally.

3. Attacks on Availability

(i).DOS (Denial of Service Attacks)
DOS is a type of attack where the large number of service requests which cannot be handled back a network server, resulting into server crash and legitimate users are denied the service.

(ii). DDOS (distributed denial of service attacks)
When computers originating from different regions attacking in nature are distributed denial of service Attacks.

(iii). SYN flood attacks and ICMP flood attacks
Attackers send various TCP SYN Packets to initiate TCP connected, but never send an SYN-ACK pack back. In ICMP flood attacks the victim computer is sent with many false ICMP packets[6].

B. Types of Vulnerabilities and Attacks
The vulnerability is a fault in the design, implementation, operation or internal control. Most of the vulnerabilities that have been discovered are documented in the Common Vulnerabilities and Exposure (CVE) database.

CVE is the system that provides a reference method for publicly known information security vulnerabilities and exposures and it is operated by 'MITRE Corporation' funded by National Cyber Security Division[7][8].

Backdoor – It is a technique used to bypass the system securities mechanism undetectably to access the computer or its data. It is also known as a trapdoor.

1. Denial of Service Attacks (DoS)
DoS makes the computer or network inaccessible to the intended user and forcefully shuts down the system by flooding the target with traffic or sending the information that triggers the crash.

2. Direct Memory Access Attacks (DMA)
It is a side channel attack that exploits the presence of high-speed expansion port that permits Direct Memory Access that can penetrate the computer device/system.

3. Eavesdropping
It is the act of secretly listening intercepting someone else's private communication/data/information.

4. Snooping
It refers to unauthorized access else data, email, computer activity, or data communication.

5. Tampering
It is a technique used to describe a malicious modification of the application/product.

6. Privilege Escalation
It is an act to gain more access to a resource that is hidden from application or user by exploiting bugs, design flaw or configuration oversight in a software application or operating system.

7. Phishing
It is a technique used to obtain confidential information by gaining as a trustworthy entity in an electronic communication.

8. Click Jacking
It is a malicious technique in which an attacker tricks a user into clicking on a button or link on another webpage while the user intended to check on the top level page. It is also known as "UI redress attack" or "User Interface redress attack".

9. Multivector Polymorphic Attacks
It is a new class of cyber threats that combined several types of attacks and change the system setting to avoid cybersecurity controls as they spread. These threats have been classified as fifth-generation cyber-attacks.

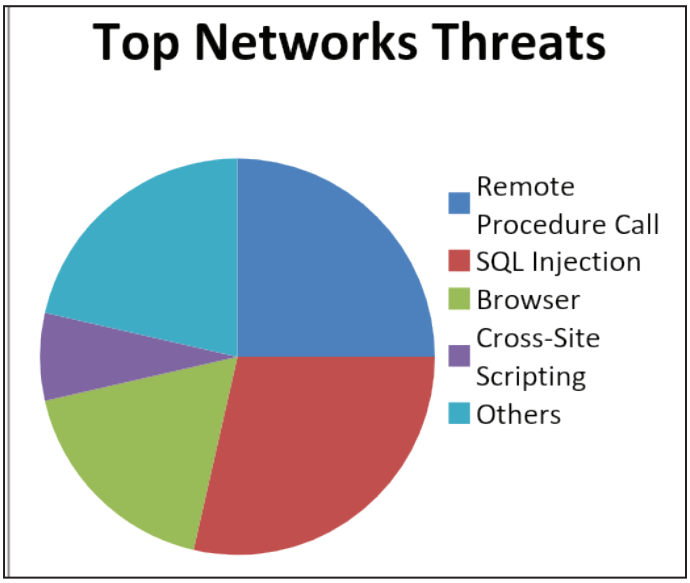

Fig. 5:

C. Famous Cyber Attacks

1. Hackers stoles tens of millions of credit card details (2009)

T Gonzales a hacker from Miami led to one of the biggest bank fraud in the files of the United States. He sealed millions of credit card and debit card numbers from 250 or more financial companies. He hacks the payment card network of some renowned companies including the 7-eleven convenient store chain.

2. Google China hit by a cyber-attack

The Google Chinese headquarter detected a security violation in mid-December, it opens up a whole can of worms, implicating the Chinese government. Hackers stole intellectual property by gaining access to several Google corporate servers. In a blog, Google said, "Evidence to suggest human right activist Gmail accounts". As they searched more they found many Gmail users from the United States, China, and Europe had routinely accessed without permission into emails belonging to Advocated of human rights in China. This evidently proved the guilt of the Chinese Government which has accused of flagrantly disregarding human rights for years.

3. Despacito has been deleted from by hackers after reaching 5 billion views

Despacito after making history by becoming to reach 5 billion views. The video was deleted from YouTube by the hackers, known by the names Prosov and Quroi'sh[10].

D. International Laws and Policies

1. Council of Europe

- Budapest Convention on Cybercrime (2001).
- Council of Europe's effort to harmonize disparate national cybercrime laws.
- EU Network and Information Security (NIS) Directive

In January 2016, EU Parliament approved NIS Directive, proposed in 2013 EU

Cyber Security Strategy. Expect formal approval by Council of Ministers, then EU countries must implement into national law within 21 months.

2. Privacy – Proposed EU General Data Protection Regulation

Extraterritorial Application and Enforcement. The new law would apply to any company that controls or processes the personal data of Europeans through the offering of goods and services – even if the company has no physical presence in Europe. Fines of up to 4% of the company's annual global revenue or €20 million for violations[11].

III. Conclusion

Computer security is a vast topic because of increase in interconnected activities such as transactions, inter-connected networks, transferring of sophisticated data etc. has rapidly increased since the last decades. Cybercrime continues to multiply each year so does the security for protecting information increases. Advancement and introduction of new technology each year pave's way for an increase in threats, the most challenging state of today's era is how to unfasten the increase in such activities. Now we require new platforms and intelligence to curb or eradicate challenges. There is no impeccable solution for cybercrimes but we should try our supreme level to reduce them so to have a safe and secure future.

References

[1] The Telegram (2015),"Hackers steal £650 million in world's biggest bank raid" [Online] Available:https://www.telegraph.co.uk/news/uknews/crime/11414191/Hackers-steal-650-million-in-worlds-biggest-bank-raid.html.

[2] EC-COUNCIL (2017),"10 Biggest Cyber Crimes and Data Breaches Till Date", [Online] Available: https://www.eccouncil.org/10-biggest-cyber-crimes-data-breaches-till-date/

[3] CIO Asia, September 3rd, HI 2013: Cybersecurity in Malaysia by Avanthi Kumar.

[4] CSO (2017),"What is cyber security? How to build a cybersecurity strategy" [Online] Available: https://www.csoonline.com/article/3242690/data-protection/what-is-cyber-security-how-to-build-a-cyber-security-strategy.html.

[5] THE ECONOMIC TIMES (2018). "Definition of Cyber Security", [Online] Available: https://economictimes.indiatimes.com/definition/cyber-security.

[6] G. Nikhita Reddy, G.J.Uganser Reddy,"A study of cybersecurity challenges and its emerging trends on latest technologies".

[7] James Lyne,"Eight trends changing network security", A Sophos Article Vol. 01, No. 04, 2012. DNA.

[8] Sunit Belapure, Nina Godbole,"Cybersecurity: Understanding Cyber Crimes".

[9] G. Nikita Reddy, G.J. Ugander Reddy,"Study of Cloud Computing in Healthcare Industry", International Journal of Science And Engineering Research, Vol. 4, Issue 9, pp. 68-71, 2013.

[10] Audrie Krause,"Computer Security Practices in Non-Profit Organizations – A network Report".

[11] Luis Corrons,"A look back on cybersecurity – Panda Labs".

Jayesh Patil received his high school graduation from Yashwant Public School, Mhow, Indore, Madhya Pradesh, India, in May 2017. His primary subjects at the high school include Physics, Chemistry, Mathematics, English, and Physical Education. His research interest includes securing the Integrity of confidential data (Cyber Security). At present, He is researching on a technology related to the Internet of Things (IoT).

Keshav Sule received his high school graduation from Indore Public School, Indore, Madhya Pradesh, India, in May 2018. His primary subjects at the high school include Physics, Chemistry, Mathematics, English, and Informatics Practice (Computer). His research interest includes securing the Integrity of confidential data (Cyber Security). At present, he is researching on an environmental issue on method for saving trees.

Jagjot Singh Saini will receive his high school graduation from The Emerald Heights International School, Indore, Madhya Pradesh, India, in May 2019. His primary subjects at the high school include Physics, Chemistry, Mathematics, English, and Informatics Practices. His research interest includes securing the Integrity of confidential data (Cyber Security). He is currently researching on Sterling Engine.