Introduction to Cyber Security

Arvind Kumar, Department of Computer Science and Engineering
Galgotias University, Yamuna Expressway Greater Noida, Uttar Pradesh
E-mail id - arvindkumar@galgotiasuniversity.edu.in

ABSTRACT: Cybercrime is one of the biggest crimes done by computer experts today. This paper addresses the need for cyber security, and some of the cybercrime's impacts. Cyber security is used to provide prevention against cybercrime. Cybercrime is a group of activities performed by people by causing network disruptions, stealing other essential and private data, documents, hacking bank details and accounts, and transferring money to their own. This paper contains detailed information about cyber security and cyber-crime. This covers cyber security types, cyber security challenges, cyber security problems, its benefits and drawbacks, cybercrime history, cybercrime types. Aim of Cyber Security is to protect systems, software, networks, computers and data from attack. Cyber security involves monitoring the physical access of the equipment, the program, the networks and protecting against harm that may occur through the networks. Today man can send and receive any type of data could be an email or an audio or video just by clicking a button but has he ever thought how securely his data Id is transmitted or sent to the other person safely without any information leakage.

KEYWORDS: Cyber security, Application of cyber security, cyber security parameters.

INTRODUCTION

Today man can send and receive any type of data can be an e-mail or an audio or video just by clicking a button but has he ever thought how securely his data is transmitted or sent to the other person safely without any information leakage?? Answer lies in cyber security. Today the Internet is the fastest growing infrastructure [1]. In technical environment many latest technologies are changing the face of the mankind. But all are unable to secure our private information in a very effective way due to these emerging technologies, cybercrimes are increasing day by day. More than 60 per cent of total commercial transactions are done online today, so this field required a high level of security for transparent and best transactions [2].

Fig. 1: Cyber security

WHAT IS CYBER SECURITY

Cyber security is the practice of protecting against malicious attacks computers, servers, mobile devices, electronic systems, networks, and data. It is also known as security of information technology or electronic protection of information [3].

Major areas which are included in the cyber security are:

1. Application security

2. Information security

3. Email security

4. Mobile Devices security

5. Web security

6. Wireless security

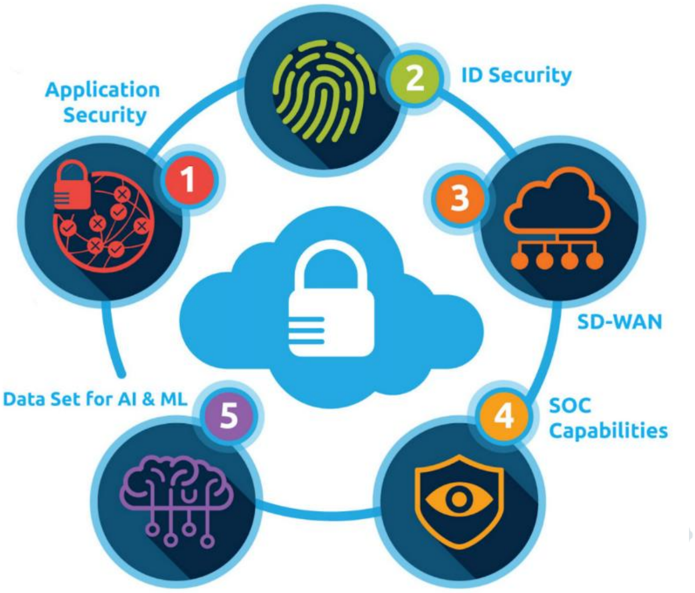

Fig. 2: Major area in the cyber security

Fig. 3: Application security

1. *Application Security*:

It focuses on keeping the software and hardware free of threads. Compromised software could provide access to data it designed to protect. Cyber security has become a most recent issue. Successful security begins in the design stage, well before the implementation of a system or computer [4].

Types of application security:

Various types of application security are present such as authentication, authorization, encryption, logging, and application security testing. To reduce security vulnerabilities developers code applications [5].

- Authentication: In authentication only the authorized users get the access. Procedures for authentication ensure a user is who they say they are. This can be achieved by allowing a username and password to be given when signing in to an application.
- Authorization: The user may be authorized to access and use the application after a user has been authenticated. By comparing the user's identity with a list of authorized users, the program will verify that a user has permission to access the application.

- Encryption: Certain security measures will protect sensitive data from being seen or even used by a cybercriminal after a user has been authenticated and is using the application. In cloud-based applications where traffic that includes sensitive data passes between the end user and the server, the traffic can be encrypted to keep the data secure.
- Logging: If an application has a security breach, then logging can help identify who has access to the data, and how. Application log files provide a time-stamped record of what and by whom elements of the application were accessed.
- Application security testing: It is used to ensure that all of these security controls work properly [6].

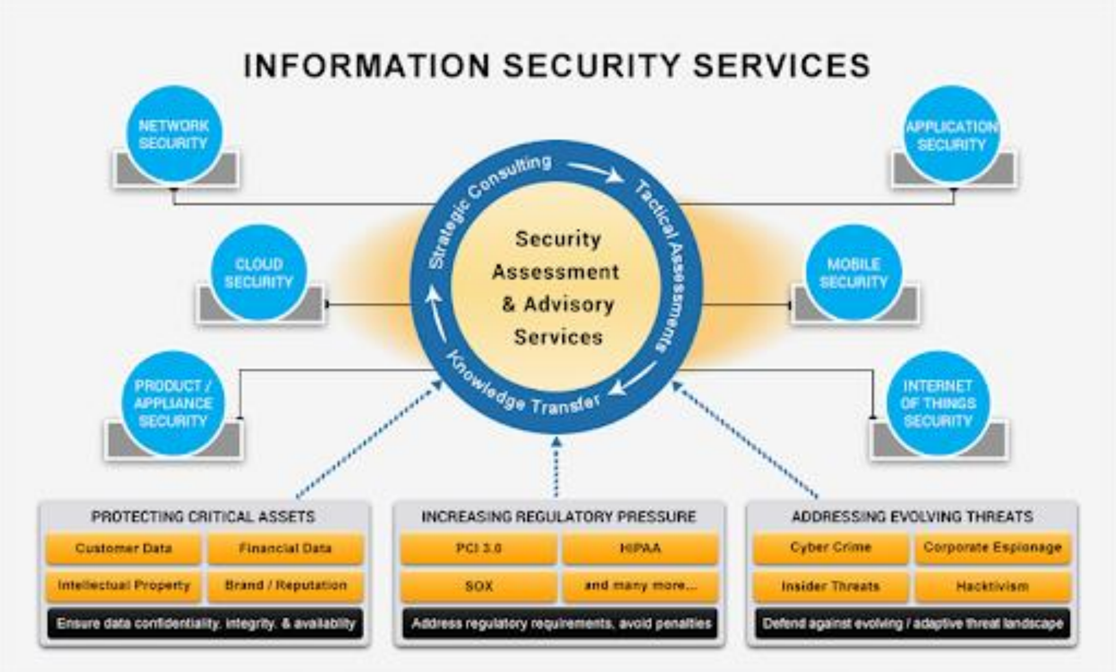
INFORMATION SECURITY SERVICES
NETWORK SECURITY
APPLICATION SECURITY
CLOUD SECURITY
MOBILE SECURITY
PRODUCT / APPLIANCE SECURITY
INTERNET OF THINGS SECURITY
Strategic Consulting
Tactical Assessments
Knowledge Transfer
Security Assessment & Advisory Services
PROTECTING CRITICAL ASSETS
Customer Data
Financial Data
Intellectual Property
Brand / Reputation
Ensure data confidentiality, integrity, & availability
INCREASING REGULATORY PRESSURE
PCI 3.0
HIPAA
SOX
and many more...
Address regulatory requirements, avoid penalties
ADDRESSING EVOLVING THREATS
Cyber Crime
Corporate Espionage
Insider Threats
Hacktivism
Defend against evolving / adaptive threat landscape

Fig. 4: Information security

2. *Information Security*:

It protects data integrity and confidentiality, both in storage and in transit. The number one threat vector for a security breach is the email gateways. Attackers use personal information and social engineering techniques to create sophisticated phishing campaigns to confuse recipients and transfer them to malware-serving sites. An email security program blocks incoming threats and monitors outgoing messages to prevent sensitive data from missing out [7].

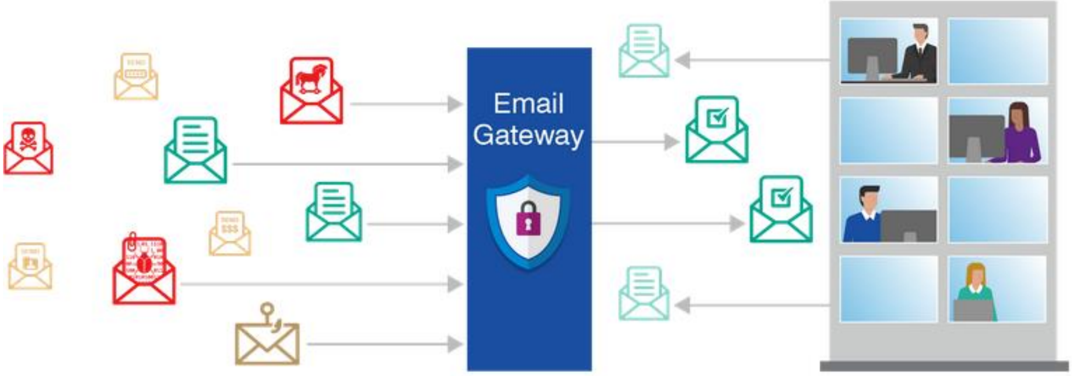

Fig. 5: Email security

3. *Mobile Device security:*

Cyber criminals are targeting mobile devices and applications more. 90 per cent of IT organizations will support corporate applications on personal mobile devices within the next 3 years [8]. The users need to control which devices can access their network. The user must also configure their connections so that network traffic is kept private [9].

Fig. 6: Mobile device security

4. *Web security*:

   "Web security" also refers to the steps taken to protect own website. It will secure the web gateway on website or in the cloud [10].

5. *Wireless security*:

Wireless network means connecting an Internet access point, like a cable from your Internet Service Provider, to a router in order to allow multiple devices to connect to the network very quickly**.** Wireless networks are not much secure as wired ones are. LAN can be like putting Ethernet ports everywhere, including the IOT parking [11].

Fig. 7: Web Security

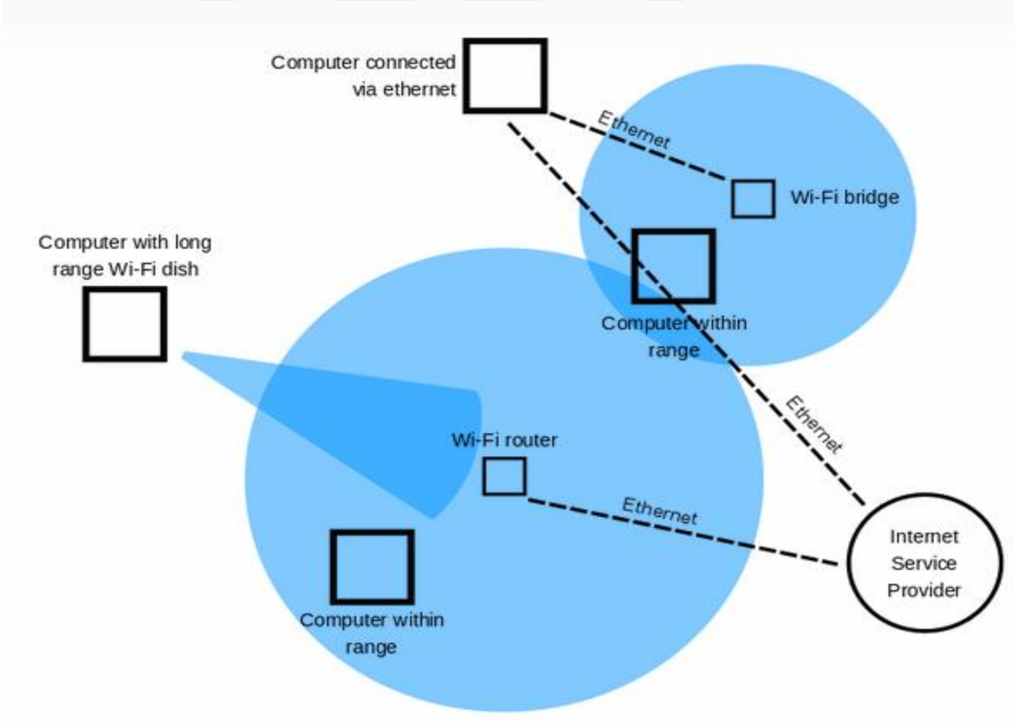
Computer connected via ethernet
Ethernet
Wi-Fi bridge
Computer with long range Wi-Fi dish
Computer within range
Ethernet
Wi-Fi router
Ethernet
Internet Service Provider
Computer within range

Fig. 8: Wireless security

CYBER SECURITY PARAMETERS

Parameters for Cyber security are:

1. Identify threats
2. Identify vulnerabilities
3. Access risk explore
4. Establish contingency plan
5. Respond to cyber security accident
6. Establish contingency plan

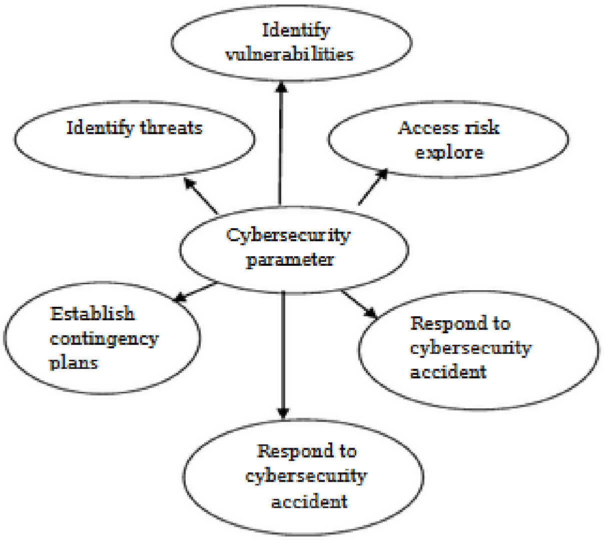
Identify vulnerabilities
Identify threats
Access risk explore
Cybersecurity parameter
Establish contingency plans
Respond to cybersecurity accident
Respond to cybersecurity accident

Fig. 9: CYBER SECURITY PARAMETERS

CONCLUSION

Every smart device capable of transferring data to one or more other devices (either through a network or not) is included within the scope of Cyber Security, which covers almost the entire foundation of modern society. Everyone needs to be aware of cyber security, cybercrimes and its triggers. There is little concern about protection with respect to internet, social and other practices through which the probability of danger is increased. This usually causes data loss, data alteration and deletion of useful information such as personal details, mail account passwords, social media or bank accounts. Citizens may also know about cybercrime laws and regulations or cyber rules and steps to be taken and how to fight against crime. Computer security is a vast subject that is becoming increasingly important because the environment is becoming highly interconnected, with the use of networks for sensitive transactions. With each New Year that passes, cybercrime continues to diverge through different paths and so does information security. There is no perfect solution for cybercrimes, but one should try our best to minimize them to ensure a safe and stable cyber space future.

REFERENCES

[1] R. Von Solms and J. Van Niekerk, "From information security to cyber security," *Comput. Secur.*, 2013, doi: 10.1016/j.cose.2013.04.004.

[2] M. Sonntag, "Cyber security," in *IDIMT 2016 - Information Technology, Society and Economy Strategic Cross-Influences - 24th Interdisciplinary Information Management Talks*, 2016, doi: 10.2478/hjbpa-2019-0020.

[3] Cyber Security Working Group, "Guidelines for Smart Grid Cyber Security: Vol. 2, Privacy and the Smart Grid," 2010.

[4] K. K. R. Choo, "The cyber threat landscape: Challenges and future research directions," *Comput. Secur.*, 2011, doi: 10.1016/j.cose.2011.08.004.

[5] M. Robinson, K. Jones, and H. Janicke, "Cyber warfare: Issues and challenges," *Comput. Secur.*, 2015, doi: 10.1016/j.cose.2014.11.007.

[6] Homeland Security, "Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies," *Ics-Cert*, 2016.

[7] A. Humayed, J. Lin, F. Li, and B. Luo, “Cyber-Physical Systems Security - A Survey,” *IEEE Internet Things J.*, 2017, doi: 10.1109/JIOT.2017.2703172.

[8] L. Hansen and H. Nissenbaum, “Digital disaster, cyber security, and the copenhagen school,” *Int. Stud. Q.*, 2009, doi: 10.1111/j.1468-2478.2009.00572.x.

[9] A. S. Elmaghraby and M. M. Losavio, “Cyber security challenges in smart cities: Safety, security and privacy,” *J. Adv. Res.*, 2014, doi: 10.1016/j.jare.2014.02.006.

[10] C. Leuprecht, D. B. Skillicorn, and V. E. Tait, “Beyond the Castle Model of cyber-risk and cyber-security,” *Gov. Inf. Q.*, 2016, doi: 10.1016/j.giq.2016.01.012.

[11] G. N. Ericsson, “Cyber security and power system communicationessential parts of a smart grid infrastructure,” *IEEE Trans. Power Deliv.*, 2010, doi: 10.1109/TPWRD.2010.2046654.