A Seminar Report

On

“_CYBER SECURIT_”

Submitted By

Mr. KALPESH G. GAVANE

Guided By

Mr. ROHAN NAIK

Submitted To

NaranLala College of Professional and Applied Sciences,

Veer Narmad South Gujarat University, Surat.

Year: 2019-2020

NARANLALA

COLLEGE OF PROFESSIONAL & APPLIED SCIENCES

BHAGVATI SANKUL, NEAR ERU CHAR RASTA,

NAVSARI – 396 450

CERTIFICATE

This is to certify that **Mr. KAlPESH G. GAVANE,** Exam No.000284 student of **B.C.A. 6th semester** of our college have successfully prepared and submitted Seminar Report on "**CYBER SECURITY**" as a partial fulfillment for the course of **Bachelor of Computer Application** during the academic year **2019-2020**.

____________ ________________

DATE:- **Guide: Mr.Rohan Naik**

(ASST PROFESSOR OF BCA)

________________ ________________ ________________

Dr. S. M. NAIK **Dr. A. B. PATEL** **(EXTERNAL EXAMINER)**

(I/C PRINCIPAL, NLCPAS) **(DEPT. HEAD, BCA)**

INDEX :

CYBER SECURITY

Figure 1:

Abstract:

As more business activities are being automated and an increasing number of computers are being used to store sensitive information, the need for secure computer systems becomes more apparent. This need is even more apparent as systems and applications are being distributed and accessed via an insecure network, such as the Internet. The Internet itself has become critical for governments, companies, financial institutions, and millions of everyday users. Networks of computers support a multitude of activities whose loss would all but cripple these organizations. As a consequence,

cybersecurity issues have become national security issues. Protecting the Internet is a difficult task. Cybersecurity can be obtained only through systematic development; it can not be achieved through haphazard seat-of-the-pants methods. Applying software engineering techniques to the problem is a step in the right direction. However, software engineers need to be aware of the risks and security issues associated with the design, development, and deployment of network-based software. This paper introduces some known threats to cybersecurity, categorizes the threats, and analyzes protection mechanisms and techniques for countering the threats.

History

Important milestones in cybersecurity history include the following:

- In 1971, the creeper virus was found; it is commonly recognized as the first computer virus.

- In 1983, Massachusetts institute of Technology was granted a patent for a cryptographic communications system and method -- the first cyber security patent.

- In the 1990 the advent of computer Computer viruses led to the infection of millions of personal computers (PCs), causing cyber security to become a household concern and facilitating the creation of more antivirus software.

- In the 1993, the first Def Con conference was held; its focus was cyber security.

- In the 2003, Anonymous was formed -- the first well-known hacker group.

- In 2003, Anonymous was formed -- the first well-known hacker group.

- In 2013, the Target breach occurred in which 40 million credit and debit card records were accessed and stolen.

- In 2016, Yahoo reported two cybersecurity breaches in which hackers gained access to data from over 500 million user accounts.

- In 2017, the Equifax security breach occurred, which exposed the personal information of up to 147 million people.

- In 2018, the General Data Protection Regulation (GDPR) was implemented. It focused on the protection of end-user data in the European Union (EU).

- Also in 2018, the California Consumer Privacy Act (CCPA) was implemented. It supports individuals' right to control their own PII.

Definition*:* Cyber security or information technology security are the techniques of protecting computers, networks, programs and data from unauthorized access or attacks that are aimed for exploitation.

THE IMPORTANCE OF CYBER SECURITY

Cyber security is important because government, military, corporate, financial, and medical organizations collect, process, and store unprecedented amounts of data on computers and other devices. A significant portion of that data can be sensitive information, whether that be intellectual property, financial data, personal information, or other types of data for which unauthorized access or exposure could have negative consequences. Organizations transmit sensitive data across networks and to other devices in the course of doing businesses, and cyber security describes the discipline dedicated to protecting that information and the systems used to process or store it. As the volume and sophistication of cyber-attacks grow, companies and organizations, especially those that are tasked with safeguarding information relating to national security, health, or financial records, need to take steps to protect their sensitive business and personnel information. As early as March 2013, the nation’s top intelligence officials cautioned that cyber-attacks and digital spying are the top threat to national security, eclipsing even terrorism.

Description: Major areas covered in cyber security are:

1) Application Security

2) Information Security

3) Disaster recovery

4) Network Security

1. Application security encompasses measures or counter-measures that are taken during the development life-cycle to protect applications from threats that can come through flaws in the application design, development, deployment, upgrade or maintenance. Some basic techniques used for application security are: a) Input parameter validation, b) User/Role Authentication & Authorization, c) Session management, parameter manipulation & exception management, and d) Auditing and logging.

2. Information security protects information from unauthorized access to avoid identity theft and to protect privacy. Major techniques used to cover this are: a) Identification, authentication & authorization of user, b) Cryptography.

3. Disaster recovery planning is a process that includes performing risk assessment, establishing priorities, developing recovery strategies in case of a disaster. Any business should have a concrete plan for disaster recovery to resume normal business operations as quickly as possible after a disaster.

4. Network security includes activities to protect the usability, reliability, integrity and safety of the network. Effective network security targets a variety of threats and stops them from entering or spreading on the network. Network security components include: a) Anti-virus and anti-spyware, b) Firewall, to block unauthorized access to your network, c) Intrusion prevention systems (IPS), to identify fast-spreading threats, such as zero-day or zero hour attacks, and d) Virtual Private Networks (VPNs), to provide secure remote access.

CHALLENGES OF CYBER SECURITY

For an effective cyber security, an organization needs to coordinate its efforts throughout its entire information system. Elements of cyber encompass all of the following:

- Network security
- Application security
- Endpoint security
- Data security
- Identity management
- Database and infrastructure security
- Cloud security
- Mobile security
- Disaster recovery/business continuity planning
- End-user education

The most difficult challenge in cyber security is the ever-evolving nature of security risks themselves. Traditionally, organizations and the government have focused most of their cyber security resources on perimeter security to protect only their most crucial system components and defend against known treats. Today, this approach is insufficient, as the threats advance and change more quickly than organizations can keep up with. As a result, advisory organizations promote more proactive and adaptive approaches to cyber security. Similarly, the National Institute of Standards and Technology (NIST) issued guidelines in its risk assessment framework that recommend a shift toward continuous monitoring and real-time assessments, a data-focused approach to security as opposed to the traditional perimeter-based model.

Purpose of cybersecurity

Cyber security measures should always be implemented to protect the data of small and large organizations and individuals. Even though significant security breaches are the ones that often get publicized, small organizations still have to concern themselves with their security posture, as they may often be the target of viruses and phishing.

Why cybersecurity is important?

Cybersecurity is important because it helps protect an organization's data assets from digital attacks that could damage the organization or individuals if placed in the wrong hands. Medical, government, corporate and financial records all hold personal information. Security incidents can lead to losses in terms of reputation, money, theft of data, deletion of data and fraud.

What cybersecurity can prevent

Cybersecurity helps prevent data breaches, identity theft and ransomware attacks, as well as aiding in risk management. When an organization has a strong sense of network security and an effective incident response plan, it is better able to prevent and mitigate cyberattacks. The process of keeping up with new technologies, security trends and threat intelligence is a challenging task.

Types of cyber threats

The threats countered by cyber-security are three-fold:

1.Cybercrime includes single actors or groups targeting systems for financial gain or to cause disruption.

2. Cyber-attack often involves politically motivated information gathering.

3. Cyberterrorism is intended to undermine electronic systems to cause panic or fear.

So, how do malicious actors gain control of computer systems? Here are some common methods used to threaten cyber-security:

Malware:

Malware means malicious software. One of the most common cyber threats, malware is software that a cybercriminal or hacker has created to disrupt or damage a legitimate user's computer. Often spread via an unsolicited email attachment or legitimate-looking download, malware may be used by cybercriminals to make money or in politically motivated cyber-attacks.

There a number of different types of malware, including:

Virus: A self-replicating program that attaches itself to clean file and spreads throughout a computer system, infecting files with malicious code.

Trojans: A type of malware that is disguised as legitimate software. Cybercriminals trick users into uploading Trojans onto their computer where they cause damage or collect data.

Spyware: A program that secretly records what a user does, so that cybercriminals can make use of this information. For example, spyware could capture credit card details.

Ransomware: Malware which locks down a user's files and data, with the threat of erasing it unless a ransom is paid.

Adware: Advertising software which can be used to spread malware.

Botnets: Networks of malware infected computers which cybercriminals use to perform tasks online without the user’s permission.

SQL injection:

An SQL (structured language query) injection is a type of cyber-attack used to take control of and steal data from a database. Cybercriminals exploit vulnerabilities in data-driven applications to insert malicious code into a databased via a malicious SQL statement. This gives them access to the sensitive information contained in the database.

Phishing:

Phishing is when cybercriminals target victims with emails that appear to be from a legitimate company asking for sensitive information. Phishing attacks are often used to dupe people into handing over credit card data and other personal information.

Man-in-the-middle attack:

A man-in-the-middle attack is a type of cyber threat where a cybercriminal intercepts communication between two individuals in order to steal data. For example, on an unsecure WiFi network, an attacker could intercept data being passed from the victim’s device and the network.

Denial-of-service attack:

A denial-of-service attack is where cybercriminals prevent a computer system from fulfilling legitimate requests by overwhelming the networks and servers with traffic. This renders the system unusable, preventing an organization from carrying out vital functions.

Cyber safety tips - protect yourself against cyberattacks

How can businesses and individuals guard against cyber threats? Here are our top cyber safety tips:

1.**Update your software and operating system:** This means you benefit from the latest security patches.

2.**U se anti-virus software:** Security solutions will detect and removes threats. Keep your software updated for the best level of protection.

3.**Use strong passwords:** Ensure your passwords are not easily guessable.

4.**Do not open email attachments from unknown senders:** These could be infected with malware.

5. **Do not click on links in emails from unknown senders or unfamiliar websites:** This is a common way that malware is spread.

6. **Avoid using unsecure Wi-Fi networks in public places:** Unsecure networks leave you vulnerable to man-in-the-middle attacks.

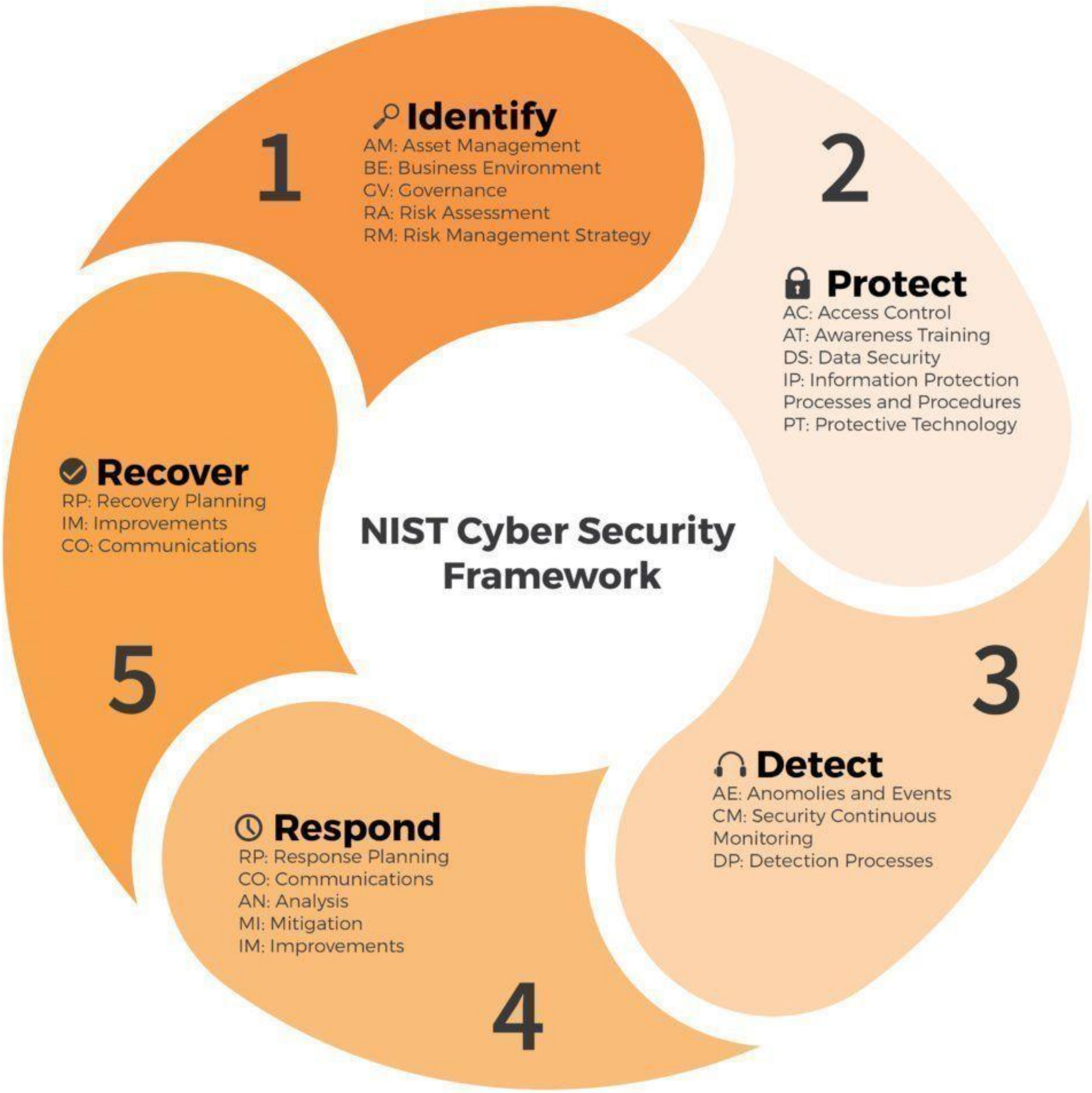

Figure 2: framework of cyber security.

Benefits of cybersecurity

The benefits of implementing cyber security initiatives include the following:

business protection malware, ransomware, phishing and social engineering;

- Protection for data and networks;
- Prevention of unauthorized users accessing digital assets;
- Improvement of recovery time after a breach;
- Protection of end users and their personally identifiable information.
- Improvement of confidence in the organization
- Fight against computer hackers and identity theft

Disadvantages of Cyber Security:

- It will be costly for average users.
- Firewalls can be difficult to configure correctly
- Need to keep updating the new software in order to keep security up to date.
- Make system slower than before.

BIBLIOGRAPHY:

The above content for this seminar report has been taken from the following resources:

a) www.google.com
b) www.wikipedia.com
c) www.encyclopedia.com