CYBER SECURITY

The history of Cyber Security

- About forty years ago words like worms, viruses, Trojan-horse, spyware, malware weren't even a part of conventional information technology (IT) vocabulary. Cyber security only came into existence because of the development of viruses. But how did we get here?
- The history of cyber security began as a research project. In the 1970's, Robert Thomas, a researcher for BBN Technologies in Cambridge, Massachusetts, created the first computer "worm". It was called **The Creeper**. The Creeper, infected computers by hopping from system to system with the message "I'M THE CREEPER: CATCH ME IF YOU CAN." Ray Tomlinson, the inventor of email, created a replicating program called **The Reaper**, the first antivirus software, which would chase Creeper and delete it.
- Late in 1988, a man named Robert Morris had an idea: he wanted to test the size of the internet. To do this, he wrote a program that went through networks, invaded Unix terminals, and copied itself. The Morris worm was so aggressive that it slowed down computers to the point of being unusable. He subsequently became the first person to be convicted under Computer Fraud and Abuse Act.
- From that point forward, viruses became deadlier, more invasive, and harder to control. With it came the advent of cyber security.

What is Cyber Security?

"Cyber security is the body of technologies, processes, and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access."

- The term cyber security refers to techniques and practices designed to protect digital data.
- The data that is stored, transmitted or used on an information system. After all, that is what criminal wants, data. The network, servers, computers are just mechanisms to get to the data.
- Effective cyber security reduces the risk of cyber-attacks and protects organizations and individuals from the unauthorized exploitation of systems, networks, and technologies.

- Robust cyber security implementation is roughly based around three key terms: people, processes, and technology. This three-pronged approach helps organizations defend themselves from both highly organized attacks and common internal threats, such as accidental breaches and human error.

Why is cyber security important?

Listed below are the reasons why cyber security is so important in what's become a predominant digital world:

- With each passing year, the sheer volume of threats is increasing rapidly. According to the report by McAfee, cybercrime now stands at over $400 billion, while it was $250 billion two years ago.
- Cyber attacks can be extremely expensive for businesses to endure. In addition to financial damage suffered by the business, a data breach can also inflict untold reputational damage.
- Cyber-attacks these days are becoming progressively destructive. Cybercriminals are using more sophisticated ways to initiate cyber attacks.
- Regulations such as GDPR are forcing organizations into taking better care of the personal data they hold.

Because of the above reasons, cyber security has become an important part of the business and the focus now is on developing appropriate response plans that minimize the damage in the event of a cyber attack. But, an organization or an individual can develop a proper response plan only when he has a good grip on cyber security fundamentals.

Fundamental objectives of cyber security: CIA Triad

Confidentiality, integrity, and availability, also known as the CIA triad, is a model designed to guide companies and organizations to form their security policies. Technically, cyber security means protecting information from unauthorized access, unauthorized modification, and unauthorized deletion in order to provide confidentiality, integrity, and availability.

➢ Confidentiality

Confidentiality is about preventing the disclosure of data to unauthorized parties. It also means trying to keep the identity of authorized parties involved in sharing and holding data private and anonymous. Often confidentiality is compromised by cracking poorly encrypted data, Man-in-the-middle (MITM) attacks, disclosing sensitive data.

Standard measures to establish confidentiality include:

- Data encryption
- Two-factor authentication
- Biometric verification
- Security tokens

➢ Integrity

Integrity refers to protecting information from being modified by unauthorized parties. It is a requirement that information and programs are changed only in a specified and authorized manner. Challenges that could endanger integrity include turning a machine into a “zombie computer”, embedding malware into web pages.

Standard measures to guarantee integrity include:

- Cryptographic checksums

- Using file permissions
- Uninterrupted power supplies
- Data backups

➢ Availability

Availability is making sure that authorized parties are able to access the information when needed. Data only has value if the right people can access it at the right time. Information unavailability can occur due to security incidents such as DDoS attacks, hardware failures, programming errors, human errors.

Standard measures to guarantee availability include:

- Backing up data to external drives
- Implementing firewalls
- Having backup power supplies
- Data redundancy

All cyber attacks have the potential to threaten one or more of the three parts of the CIA triad. Confidentiality, integrity, and availability all have to work together to keep your information secured. So, it's important to understand what the CIA Triad is, how it is used to plan and implement a quality security policy while understanding various principles behind it.

Safeguards against the computer security breaches

In a world filled with computations we can't expect everything to go normal. Things go wrong sometimes. The reason may be an internal source or an external source. Data breaches have increased in numbers year by year. Measures have been taken by every company to prevent the data breach and the criminals find a better way to get access to the company. The information accessed by the hackers includes mostly names, date of birth, social security numbers and sometimes credit card or debit card numbers. Data breaches can occur due to many reasons like hackers gaining access to the information or losing a device which has unencrypted information. It is always better to prevent than to cure. Let us look into some ways to prevent data security breaches.

1. Protect Information:

Sensitive information must be protected wherever it is stored sent or used. Do not reveal personal information inadvertently.

2. Reduce transfer of data:

The organization should ban shifting data from one device to another external device. Losing removable media will put the data on the disk under risk.

3. Restrict download:

Any media that may serve as an allegiance to the hackers should be restricted to download. This could reduce the risk of transferring the downloadable media to an external source.

4. Shred files:

The organization should shred all the files and folder before disposing storage equipment. There are applications which can retrieve information after formatting.

5. Ban unencrypted device:

The institution should have a ban on the device that is unencrypted. Laptops and other portable devices that are unencrypted are prone to attack.

6. Secure transfer:

The use of secure courier services and tamper proof packaging while transporting bulk data will help in preventing a breach.

7. A good password:

The password for any access must be unpredictable and hard to crack. Change of password from time to time

8. Automate security:

Automating systems that regularly check the password settings, server and firewall configuration might bring about reduction of risk in the sensitive information.

9. Identify threats:

The security team should be able to identify suspicious network activity and should be prepared if there is an attack from the network.

10. Monitor data leakage:

Periodically checking security controls will allow the security team to have a control on the network. Regular check on internet contents to locate if any private data is available

for public viewing is also a good measure to monitor data.

11. Track data:

Tracking the motion of data within the organizational network will prevent any unintentional use of sensitive information.

12. Define accessibility:

Defining accessibility to those who are working on company's sensitive data will bring down the risk of malicious users.

13. Security training:

Providing privacy and security training to all employees, clients and others related to data related activities will bring about awareness on data breach.

14. Stop incursion:

Shutting down the avenues to the company's warehouse will prevent incursions by the hacker. Management, production and security solutions must be combined to prevent the targeted attacks.

15. Breach response:

Having a breach response plan will help in triggering quick response to data breaches and help in the reduction of harm. The plan could contain steps involving notification of the concerned staff or the agency that could contain the breach.

Security Management Tools

1. **Access Rights Manager :**

Manage and audit access rights across your IT infrastructure

Key Features

- Understand and act on high-risk access
- Minimize the impact of insider threats
- Improve compliance by detecting changes
- Identify who has access to what fast
- Fast, accurate account provisioning
- Identify and monitor high-risk accounts

2. **Security Event Manager**

   Improve your security posture and quickly demonstrate compliance with a lightweight, ready-to-use, and affordable security information and event management solution.

   Key Features

   - Centralized log collection and normalization
   - Automated threat detection and response
   - Integrated compliance reporting tools
   - Intuitive dashboard and user interface
   - Built-in file integrity monitoring
   - Simple and affordable licensing

3. **Server Configuration Monitor**

   Detect unauthorized configuration changes to your servers and applications

   Key Features

   - Baseline server and application configurations on Windows and Linux
   - Alert and report on deviations from the baseline in near real time
   - See who's making configuration changes on servers or applications
   - Compare current configurations to previous versions
   - Correlate configuration changes with performance metrics
   - Track server hardware and software inventory

4. **Patch Manager**

   Patch management software designed to quickly address software vulnerabilities

   Key Features

   - Microsoft WSUS patch management
   - Integrations with SCCM
   - Third-party application patching
   - Prebuilt/pretested packages
   - Patch compliance reports
   - Patch status dashboard

5. **Managed File Transfer Server**

Enhance security and control over file transfers in and outside your organization

Key Features

- Reliable FTP server software for secure file transfer
- Ad hoc file sharing to easily send and request files
- Anywhere, anytime file transfer from web and mobile devices
- Upload and download large files quickly and easily
- Centralized file transfer management and automation
- Maintain regulatory compliance

6. **File Transfer Protocol Server**

Simple, affordable, easy-to-use FTP server software

Key Features

- File transfer using FTP and FTPS
- Quick and easy file transfers from the web and mobile devices
- Transfer multiple and large files easily
- Simple file transfer administration and management
- Secure gateway helps avoid data at rest in DMZ networks
- Easily manage file transfer settings and permissions

Good Security Practices:

Cyber security best practices encompass some general best practices like being cautious when engaging in online activities, abiding by company rules, and reaching out for help when you encounter something suspicious. Here's a the 10 cyber security best practices

1. Protect your data

In your daily life, you probably avoid sharing personally identifiable information like your Social Security number or credit card number when answering an unsolicited email, phone call, text message, or instant message. It's important to exercise the same caution at work. Keep

in mind that cybercriminals can create email addresses and websites that look legitimate. Scammers can fake caller ID information. Hackers can even take over company social media accounts and send seemingly legitimate messages.

2. Avoid pop-ups, unknown emails, and links

Beware of phishing. Phishes try to trick you into clicking on a link that may result in a security breach. Phishes prey on employees in hopes they will open pop-up windows or other malicious links that could have viruses and malware embedded in them. That's why it's important to be cautious of links and attachments in emails from senders you don't recognize. With just one click, you could enable hackers to infiltrate your organization's computer network.

Here's a rule to follow: Never enter personal or company information in response to an email, pop-up webpage, or any other form of communication you didn't initiate. Phishing can lead to identity theft. It's also the way most ransom ware attacks occur.

3. Use strong password protection and authentication

Strong, complex passwords can help stop cyber thieves from accessing company information. Simple passwords can make access easy. If a cybercriminal figures out your password, it could give them access to the company's network. Creating unique, complex passwords is essential.

A strong password contains at least 10 characters and includes numbers, symbols, and capital and lowercase letters. Companies also should ask you to change your passwords on a regular basis. Changing and remembering all of your passwords may be challenging. A password manager can help.

Companies may also require multi-factor authentication when you try to access sensitive network areas. This adds an additional layer of protection by asking you to take at least one extra step such as providing a temporary code that is sent to your Smartphone to log in.

4. Connect to secure Wi-Fi

Office Wi-Fi networks should be secure, encrypted, and hidden. If you're working remotely, you can help protect data by using a virtual private network, if your company has one. A VPN is essential when doing work outside of the office or on a business trip. Public Wi-Fi networks can be risky and make your data vulnerable to being intercepted.

But keep in mind; some VPNs are safer than others. If your company has a VPN it trusts, make sure you know how to connect to it and use it. Norton Secure VPN provides powerful VPN protection that can help keep your information private on public Wi-Fi.

5. Enable firewall protection at work and at home

Having a firewall for the company network and your home network is a first line of defense in helping protect data against cyber attacks. Firewalls prevent unauthorized users from accessing your websites, mail services, and other sources of information that can be accessed from the web.

6. Invest in security systems

Smaller businesses might hesitate when considering the cost of investing in a quality security system. That usually includes protections such as strong antivirus and malware detection, external hard drives that back up data, and running regular system checks. But making that investment early could save companies and employees from the possible financial and legal costs of being breached.

All of the devices you use at work and at home should have the protection of strong security software. It's important for your company to provide data security in the workplace, but alert your IT department or Information Security manager if you see anything suspicious that might indicate a security issue. There may be a flaw in the system that the company needs to patch or fix. The quicker you report an issue, the better.

7. Install security software updates and back up your files

Following IT security best practices means keeping your security software, web browsers, and operating systems updated with the latest protections. Antivirus and anti-malware protections are frequently revised to target and respond to new cyber threats.

Cyber threats often take aim at your data. That's why it's a best practice to secure and back up files in case of a data breach or a malware attack. Your company will probably have rules about how and where to back up data. Important files might be stored offline, on an external hard, drive, or in the cloud.

8. Talk to your IT department

Your IT department is your friend. Reach out to your company's support team about information security. You might have plenty to talk about.

It's a good idea to work with IT if something like a software update hits a snag. Don't let a simple problem become more complex by attempting to "fix" it. If you're unsure, IT can help.

It's also smart to report security warnings from your internet security software to IT. They might not be aware of all threats that occur.

It's also important to stay in touch when traveling. Let your IT department know before you go, especially if you're going to be using public Wi-Fi. Have a great trip — but don't forget your VPN.

Remember to make sure IT is, well, IT. Beware of tech support scams. You might receive a phishing email from someone claiming to be from IT. The goal is to trick you into installing malware on your computer or mobile device, or providing sensitive data. What to do? Don't provide any information. Instead, contact your IT department right away.

9. Employ third-party controls

Here's a fact that might be surprising. It's common for data breaches to begin from within companies. That's why organizations need to consider and limit employee access to customer and client information.

You might be an employee in charge of accessing and using the confidential information of customers, clients, and other employees. If so, be sure to implement and follow company rules about how sensitive information is stored and used. If you're in charge of protecting hard or soft copies, you're the defender of this data from unauthorized third parties.

Companies and their employees may also have to monitor third parties, such as consultants or former employees, who have temporary access to the organization's computer network. It's important to restrict third-party access to certain areas and remember to deactivate access when they finish the job.

10. Embrace education and training

Smart companies take the time to train their employees. Your responsibility includes knowing your company's cyber security policies and what's expected of you. That includes following them. If you're unsure about a policy, ask.

A little technical savvy helps, too. Learning the process for allowing IT to connect to your devices, along with basic computer hardware terms, is helpful. That knowledge can save time when you contact support and they need quick access and information to resolve an issue.

If you want to back up data to the cloud, be sure to talk to your IT department first for a list of acceptable cloud services. Organizations can make this part of their AEU policy. Violation of the policy might be a cause for dismissal.