EXORDIUM ON CYBER SECURITY

Author: Kirthiga L

Corresponding Author: Mohammed Sadiq Hussain

qad@srmtech.com

Abstract: *In today's society, which is governed by technology and network connections, understanding cyber security and being able to use it successfully is critical. If there is no security to secure it, systems, vital files, data, and other important virtual items are at risk. Whether it is an IT firm or not, every company must be protected equally. The attackers, likewise, do not fall behind with the development of new cyber security technology. They are employing improved hacking tactics and focusing on the weak points of many businesses. Cyber security is critical because the military, political, financial, medical, and corporate institutions collect, practice, and store vast amounts of data on PCs and other devices. Whether financial data, intellectual property, or personal information, sensitive data can make up a significant portion of such data*

Key Words: *IT, DATA*

INTRODUCTION

It is critical to understand what cyber security is and how to apply it successfully in today's society, driven by technology and network connections. If there is no security to secure it, systems, vital files, data, and other important virtual items are at risk. Whether it is an IT firm or not, every company must be protected equally. The attackers do not fall behind with the advancement of new cyber security technology. They are improving their hacking tactics and focusing on the weak points of various businesses.

Cyber security is the process of preventing cyber-attacks on sensitive data, networks, and software applications. Exploiting resources, unauthorized access to networks, and ransomware assaults to encrypt data and extract money are all examples of cyber-attacks.

WHY IS CYBER SECURITY IMPORTANT?

Understanding the necessity of cyber security is essential to keep the systems intact. Hackers have taken the game to a new level; therefore, businesses and their employees should be aware of the dangers if they are not addressed.

The cost of cyber risks has reached an all-time high, and security system breaches can go undetected for months. Advanced persistent threats, for example, make repeated attempts to hack into computer systems, acquire access, and remain within for months, tracking and monitoring the behavior of companies before being detected. Let's take a deeper look at why cyber security is so important:

- The financial impact of data breaches. As we all know, many restrictions have been put in place to secure users' data.

- Cyber-attacks can be costly. Those who portray themselves as unaware of cyber security is and how much it costs can become victims of financial fraud. Most hackers are motivated by monetary gain, but don't be fooled; this isn't the sole reason. Cybercriminals can obtain a political, ethical, social, or intellectual edge by utilizing their skills.

Business and government entities aren't the only ones who need to be concerned about cyber security. It should be for everyone who uses digital devices such as computers, smartphones, tablets, and other similar gadgets.

WHAT IS THE KEY CONCEPT OF CYBER SECURITY?

Cyber security is a broad phrase that can have a variety of definitions that revolve around the digital world. "The CIA Triad" is a three-part idea that helps people comprehend cyber security.

Confidentiality, Integrity, and Availability are the three pillars of every organization's security.

- **Confidentiality:** Confidentiality principles state that only authorized parties have access to sensitive data and functions. Military secrets, for example.

- **Integrity:** The principles of integrity state that sensitive information and functions can only be changed, added, or removed by authorized persons and means. A user, for example, may enter inaccurate data into the database.

- **Availability:** According to availability principles, systems, functions, and data must be available on demand based on agreed-upon parameters and service levels.

ROLE IN CYBERSECURITY

Identify:

Create policies and processes for cyber security and identify and regulate who has access to your company's information. Conduct background checks and produce separate user accounts for each employee to create policies and procedures for cyber security.

Protect:

Employee access to data and information should be restricted. Surge protectors and uninterruptible power supplies (UPS) should be installed, and your operating systems and applications should be patched on regularly. Firewalls, both software and hardware, should be installed and activated on all of your company's networks. Set up web and email filters after securing your wireless access point and network. Encrypt vital company information before safely disposing of obsolete computers and media. Employees should be given training about the company's information security policies and best practices.

Detect:

Maintain and monitor logs after installing and updating antivirus, anti-spyware, and other anti-malware products.

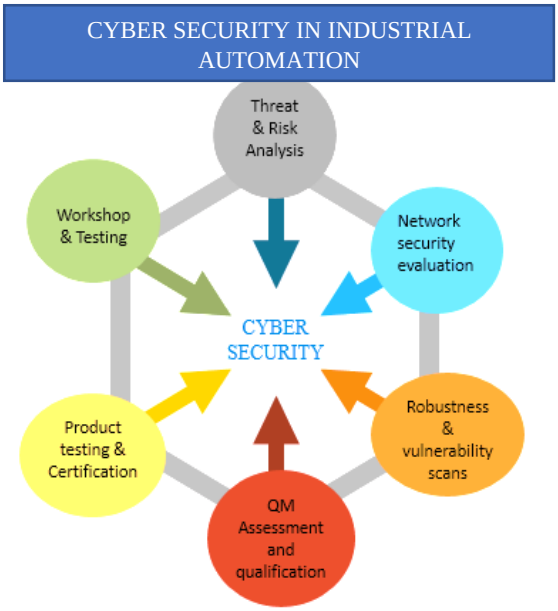
Respond:

Create a catastrophe and information security incident plan.

Recover:

Make complete backups of critical corporate data and documents. Continue to make incremental backups and think about purchasing cyber insurance. Improve the process, methods, and technology.

CYBER SECURITY IN INDUSTRIAL AUTOMATION



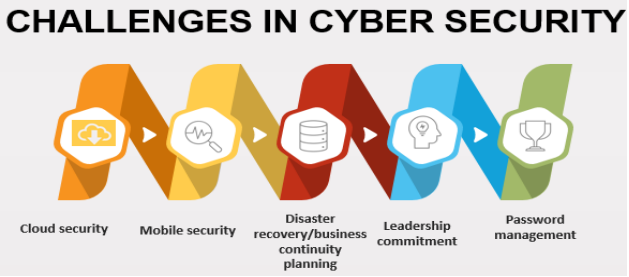
Threat and Risk Analysis: In the most basic terms, a cyber threat and risk assessment is the process of assessing the threat, vulnerability, and information value of a cyber-system.

Network Security Evaluation: A network security assessment's goal is to keep your networks, devices, and data safe and secure by identifying any possible entry points for cyber-attacks from both inside and outside your company.

Robustness and Vulnerability scan: Robustness in Cyber security Vulnerability Scan is used to detect vulnerabilities in computers, programs, or networks, as the name implies. A scanner (software) is used for this purpose, and it can uncover and identify vulnerabilities that emerge from network misconfiguration and programming flaws.

Workshops and training: Many firms of all sizes have made cyber security training, also known as security awareness training, a priority in order to educate employees on current and new cyber security threats.

CHALLENGES IN CYBER SECURITY



Cloud Security:

Policies, procedures, and controls that secure cloud-based systems and user privacy are referred to as cloud security, or cloud computing security. As more people and businesses resort to the cloud to process and store data, this is becoming increasingly critical.

Mobile Security:

Mobile is the most prominent part of securing mobility solutions. Security is the most prominent part of securing mobility solutions. The use of mobile devices is increasing, posing a greater danger to information security. Malware, spyware, viruses, and other risks can all be prevented using mobile security software.

The anticipated number of mobile devices is around 5.8 billion and is expected to rise dramatically over the next five years, reaching nearly 12 billion in four years. That means each person on the earth will have an average of two mobile devices. We have become entirely reliant on mobile devices to perform personal and professional tasks, with our sensitive data being sent back and forth. These factors make mobile security a crucial part to address.

The concept of mobile security refers to the protection of our mobile devices against possible attacks by other mobile devices or the wireless environment in which they are linked.

The following are the most serious dangers to mobile security:

- Misplacement of a mobile device. This is a typical problem that might put you, as well as your connections, at risk of phishing & impersonation attacks.

- Mobile applications hacking and breaches are the second most crucial concern. Many of us have installed and downloaded mobile apps for specific purposes. For marketing purposes, some ask for additional permissions or rights, such as access to your location, contacts, and browser history.

- Smartphone theft is a widespread concern. On the wrong hand, such devices are prone to data theft where they can gain access to corporate data, account credentials, and email access.

Disaster recovery/business continuity planning:

After a cyber security event or natural disaster, disaster recovery is an organized way to immediately redirect IT resources toward restoring data and regaining access to IT infrastructure. DR is frequently seen as a part of Business Continuity Planning in the information security arena.

Leadership commitment:

Cyber resiliency requires leadership commitment. It is difficult to establish or enforce successful processes without it. Top-level management must be willing to spend money on cyber security resources like awareness training and implementing advanced technologies.

When a leader decides to make a change, they usually go ahead and make it happen, presumably with sufficient funding. That is insufficient for transition to be successful.

Leadership commitment is required for successful change. Commitment to leadership necessitates courage, communication, and focus.

- **Courage** – Be a role model for others by changing yourself. You set an example for others by having the fortitude to change. When leading a change, you must have unwavering determination in your commitment to ensuring a successful transition.
- **Communication** - The medium via which the organizations clear definition of success (the objective) is shared and aligned. To reinforce your commitment & keep the momentum going, you'll need to communicate frequently. Many things might detract from the success of the transition, and There are chances of losing sight of the goal if communication is not maintained appropriately

- **Focus** - Leadership commitment demands the ability to make decisions on own despite circumstances to add value to the transition. It's discordant to demand change from others while failing to demonstrate your own commitment. The level of commitment and concentration should be consistent throughout the transition. The leader's approach towards the transition should be long-term focused.
- Commitment to leadership is complex, and when leading an unpopular change, there may be personal costs. On the other hand, true leaders are distinguished by their leadership dedication from others in leadership positions. Evaluate your degree of dedication the next time you're in a place to lead a change. Going forward without strong focus
- Instincts, and communication will be difficult to experience a successful transition.

Password Management:

Password management is defined as a system that allows users to store passwords in a simple, secure manner and retrieve them promptly when needed.

The one-stop answer for this modern dilemma is password management. A password organizer allows users to manage their passwords, both personal and professional, from a single spot. A password manager is more than just a way to keep track of your passwords. It assists you in creating sufficiently complex passwords, ensuring timely password rotation, and enforcing a number of recommended cyber security practices.

Traditional password management solutions are no longer viable, especially in 2022. When remote work is the norm and forgetting a password might mean being entirely locked out of the office infrastructure. Another security danger is storing passwords where family members or acquaintances can access them, whether physically or digitally. This is a widespread practice, especially among employees with poor technical hygiene.

BEST CYBER SECURITY PRACTICES

1. Bio Metrics Security

Biometrics ensures Fast authentication, secure access management, and precise staff monitoring are all made possible by biometrics. Businesses must verify users' identities before granting them access to important assets. Voice recognition, fingerprint scanning, palm biometrics, facial recognition, and behavioral biometrics are all excellent ways to Verify and authenticate

As one of the best practices for data security, Biometrics enables more secure authentication than passwords and SMS verification. As a result, biometrics has already established itself as a vital component of multi-factor authentication.

Authentication isn't the sole application for biometrics, though. A wide range of biometrics-driven technologies is available to security professionals, allowing them to detect compromised privileged accounts in real time.

The study of how people interact with input devices is known as behavioral biometrics. Technology delivers a warning to security staff whenever anomalous conduct is identified, allowing them to react quickly.

There are a variety of behavioral biometrics that can be used by users and companies

- **Keystroke dynamics** – To develop user behavior profiles, it considers typing speed and the inclination to make common mistakes in certain terms.
- **Mouse dynamics** – Monitors the time between clicks as well as the cursor's speed, rhythm, and style.

- **Eye movement biometrics** – Records eye movement patterns and detects unique patterns using eye and gaze tracking devices.

2. Use Multi-Factor Authentication

To log in to a device or an account using multi-factor authentication, you must provide more than one authentication factor.

For example, you need to enter a passcode and scan your fingerprint to unlock your phone.

This security feature is available from many software makers and other service providers, allowing you to add an extra layer of protection to your devices and online accounts. To access a device or an account with this functionality enabled, you must give multiple pieces of authenticating information. If cybercriminals acquire access to one piece of information (for example, your password), they will still need to offer additional information to obtain access to your accounts.

Think of it like this: You use a password to prove that you are the account owner and to validate your identity when you try to log in to your online banking account. The idea is that the password linked with that account should only be known by you.

The issue is that utilizing a single factor to authenticate you, such as a password, is insecure. Your password can be stolen or guessed by a cybercriminal.

That's when having at least a second authentication factor comes in handy.

Multi-factor authentication "OK, you have one piece of information that identifies you as the account owner," software suppliers and other service providers (e.g., a bank) can say. However, could you give me two pieces of information? "Is it three or four?

Key Words: Password

Multi-factor authentication is an important cyber security feature since it allows you to log in with more than one factor. Multi-factor authentication adds an extra degree of security to devices, accounts, and data.

1. Monitor Third-Party Access To Your Data

Controlling third-party access is an essential component of any security plan.

Remote employees, subcontractors, business partners, suppliers, and vendors are just a few of the people and businesses who may have remote access to your data.

Monitoring third-party actions is an excellent approach to protect your sensitive data against breaches caused by third-party access. You may control the level of access granted to third-party users and keep track of who connects to your network and why.

User activity monitoring should be used in conjunction with one-time passwords to offer full tracking of all user actions so that malicious behavior can be detected and investigations conducted as needed.

2. Raise Employee Awareness

Cybercrime may strike any company, big or little, in any industry. They have one thing in common: they are all more than likely to develop due to human error. According to Cybint, this is how 95 percent of cyber security breaches happen. This implies that when fighting cybercrime and keeping your company's data safe, your employees are one of the weakest links in the chain.

It is critical to have open lines of communication with staff. In terms of cyber security, everyone in the company has a responsibility to play. One of the most important things you can do is start a conversation on the importance of cyber security and giving guidance on how to stay secure and recognize potential danger.

Employee security awareness emails aren't the only way to interact with them. You shouldn't just rely on one delivery method to communicate and educate the staff. There must be an effective internal communications strategy. If they've been exposed to communications in a variety of channels and forms, they're more likely to notice, remember, and put things in practice.

Desk Alerts, an internal communications software system, is an excellent approach to coordinate a campaign like this. You can transmit crucial cyber security messages in a variety of formats, including:

- Pop up alerts
- Desktop tickers
- Corporate screensavers
- Corporate wallpapers
- Lock screen alerts
- Digital signage

Schedule your content ahead of time and distribute it to the entire company or to select groups of employees based on your requirements. You can also use the Desk Alerts polls, quizzes, and surveys module to test your employees' knowledge. For example, issuing a ransomware quiz.

Any findings will be available in real-time, and you'll be able to see if there are any knowledge gaps among your staff that could pose a risk to the organization.

References

https://www.bitdegree.org/tutorials/what-is-cyber-security/

https://cltc.berkeley.edu/scenario-back-matter/

https://www.getcybersafe.gc.ca/en/blogs/why-multi-factor-authentication-essentail-part-cybersecurity

.