10 KEYSTONES OF CYBERSECURITY THAT YOU MUST KNOW!

TABLE OF CONTENTS

INTRODUCTION

The world is evolving & so is technology! With all the digital transformations, came the digital threats! Just a decade ago, most of us believed that cybersecurity was only limited to techies. But today, it has become a headache that nobody can afford to ignore!

It has become such an issue that every day, some type of hacking attacks are being executed in order to cause chaos & for some financial gains! This has brought us to this E-Book showcasing some of the major aspects of cybersecurity!

1. THE RIGHT APPROACH TO CYBERSECURITY!

A successful cybersecurity approach includes multiple layers of protection spread across the computers, networks, programs, or data that one intends to keep safe. In a corporation, the people, processes, and technology must all complement each other to make an efficient defense from cyberattacks.

- **People**

Users must understand basic data security principles like choosing strong passwords, being wary of attachments in email, and backing up data.

- **Processes**

Organizations must have a framework for a way they affect both attempted and successful cyberattacks. This is useful for protecting systems, identifying an attack, recovering from a successful attack & detecting or responding to threats.

- **Technology**

It is important to provide the computer system & security tools to organizations and individuals for defending against cyberattacks. Overall, 3 main entities must be protected: endpoint devices like computers, smart devices, and routers; networks; and moreover, the cloud.

2. WHY IS CYBERSECURITY ESSENTIAL?

In the current world, cybersecurity has become the need of an hour for protecting information, networks, or systems from online threats. All the recent cyber threats can take numerous forms including malware, ransomware, app attacks, phishing or exploit kits. However, recent technological progress has opened doors to new possibilities for neutralizing cyber crimes.

Contrary to this fact, adversaries have also benefited from these same advancements as well. Automation, advanced tools & recent tech evolution is helping attackers to deploy large-scale cyber attacks at significantly less time & low cost.

3. MAJOR CYBERSECURITY CHALLENGES!

- **Endpoint security:** Endpoint security is the process of protecting remote access to a company's network.

- **Cloud security:** Cloud has become one of the go-to technologies for almost all workplaces after the onset of a pandemic. Because of this, 1000s & 1000s of files are now being stored on the cloud. Protecting data during a 100% online environment presents enormous challenges.

- **Mobile security:** All the latest smartphones and tablets are highly vulnerable to digital threats.

- **Network security:** Even today, protecting the network from unwanted users, attacks and intrusions is a difficult task.

- **Application security:** To ensure digital security from cyber threats, apps require constant updates & testing.

- **Data security:** Data is an integral part of every application & network. Protecting the data of all the customers & even employees adds up as a separate layer of security.

- **Identity management:** Giving the right access to every employee is very crucial. The right identity management in an organization can be the game-changer for data leaks or cybercrimes.

- **Database and infrastructure security:** In a network, everything is related to physical equipment & databases. Defending the database & IT infrastructure is important.

- **Disaster recovery/business continuity planning:** In case of any emergency like a natural disaster or data breach, there should always be a recovery plan so that business can continue. t

4. MAJOR TYPES OF CYBERSECURITY RISKS!

There are mainly 3 different types of cybersecurity risks. These are as follows:

- **Cybercrime**

It is committed by one or more individuals who target systems to cause havoc or for financial gain.

- **Cyberattacks**

These are often committed for political reasons or competitive advantage over counterparts and may be designed to collect and often distribute sensitive information.

- **Cyber terrorism**

Cyber terrorism is designed to breach electronic systems to instill panic and fear in its victims. It is generally targeted over a specific geographical region.

5. VARIOUS CATEGORIES OF CYBER ATTACKS!

The categories of cyber attacks are as follows:

- **Attacks on confidentiality**

These attacks can be designed to steal your personal identifying information and your bank account or credit card information.

- **Attacks on integrity**

A cybercriminal/hacker will access and release sensitive information for the purpose of exposing the data and influencing the public to lose trust in a person or an organization.

- **Attacks on availability**

These attacks can be used to block users from accessing their own data until they pay a fee or ransom. Typically, a cybercriminal will infiltrate a network and authorized parties from accessing important data, demanding that a ransom be paid.

6. SOME OF THE MOST POPULAR CYBER THREATS!!

- **SQL injection**

An SQL (structured language query) injection is a sort of cyberattack that will take hold of any personal or business information and steal data from an organizational database. Cybercriminals/hackers exploit vulnerabilities in data-driven applications to insert malicious code into a database via a malicious SQL statement. This gives them access to the sensitive information contained within the database.

- **Phishing**

In Phishing, cybercriminals/hackers target victims with emails that appear to be from a legitimate company asking for sensitive information. Phishing attacks are often used to take advantage of 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/hacker intercepts communication between two individuals in order to steal/spy data. For example, in an unsecured Wi-Fi network, an attacker could intercept data being passed from the victim's device and the network.

- **Denial-of-service attack**

It is a type of online attack, wherein, a hacker overwhelms the networks & servers with high traffic to prevent a computing system from fulfilling legitimate requests. This can prevent an organization from carrying out vital functions for the business.

Social engineering

It is a type of attack that is focused on the confidentiality of the user. It involves the process of psychologically manipulating people into performing actions to share personal or sensitive information. Phishing attacks are the foremost common sort of social engineering. Phishing attacks usually are available mostly from a deceptive email with the goal of tricking the recipient into sharing personal or sensitive personal information.

Malware, or malicious software

This attack is based on availability. It refers to software that's designed to realize access to or damage a computer without the knowledge of the owner. Malware can do everything from stealing your login information and using your computer to send spam, to crashing your computing system. Several common sorts of malware include spyware, keyloggers, true viruses, and worms.

Ransomware

Another sort of malicious software, it is also a kind of attack on availability. Its goal is to lock and encrypt your computer or device data—essentially holding your files hostage—and then demand a ransom to revive access. A victim typically must pay the ransom within a limited amount of your time mostly provided by the attacker or risk losing access to the business/personal information forever. Common sorts of ransomware include crypto-malware, lockers, and scareware.

7. LATEST CYBER THREATS THAT YOU SHOULD KNOW!!

- **APTs**

APTs or Advanced Persistent Threats are based on integrity. In such attacks, hackers infiltrate any network undetected & stay there for a long time. Here, instead of harming the network, the main intent is to steal the data. It is commonly seen in industries or sectors having a high volume of data or information. These may be manufacturing industries, national defense, or even the finance sector.

- **Dridex malware**

Dridex is a financial trojan. It infects computers through phishing emails o existing malware. It is capable of stealing passwords, banking details, and personal data which can be used in fraudulent transactions.

- **Romance scams**

Cyberattackers/hackers take advantage of people seeking new partners on online dating platforms, duping victims into giving away personal data.

- **Emotet malware**

Emotet is a sort of sophisticated trojan that will steal your data and load other malware as well. It is thriving mainly on a simple or unsophisticated user password. This is also a reminder to everyone for creating a secure, long & complicated password to guard against it.

8. IMPORTANCE OF END-USER PROTECTION!

End-user protection or endpoint security is typically a crucial aspect of cybersecurity. It is especially for an individual (the end-user) who accidentally uploads malware or another sort of cyber threat to their desktop, laptop, or mobile device.

End-user security software helps in detecting & removing pieces of malicious code by scanning the computer.

Many end-user protection software use heuristic and behavioral analysis to monitor the behavior of a program and its code to defend against viruses or trojans that change their shape with each execution.

9. HOW TO PROTECT AGAINST CYBER ATTACKS?

- Ensure to update software and operating systems regularly.
- Install and regularly update antivirus and antispyware software in each device.
- Avoid opening or downloading email attachments from unknown senders.
- Avoid clicking on links in emails from unknown senders or unfamiliar websites.
- Avoid using unsecured Wi-Fi networks publicly places
- Regularly update/change passwords. Make sure to use strong passwords consisting of mixed characters such as symbols, alphabets, numbers, and special characters.
- Try implementing Two-factor authentication for every important credential's logins.
- Make sure Wi-Fi access is limited and the network is hidden.
- Take regular backup copies of important information and encrypt the backed-up data to avoid any misuse or unauthorized access to it.
- Ensure to use a firewall for the Internet connection.
- Prevent human error by being aware of the latest modus operandi.
- Develop a response plan in case of any disaster and make sure to test the plan regularly.
- Restrict physical access to personal systems.
- Avoid sharing passwords of devices or crucial websites to family, friends, or colleagues.
- Avoid using the same or similar passwords for each and every website.

10. HOW YOU CAN HELP ORGANIZATIONS?

With time & technological evolution, cyber threats have evolved as well. Apart from critical thinking, you must have a good knowledge of important cybersecurity tools, recent updates & advanced cybersecurity concepts.

If you are looking to enter this field, or level up with all the recent breakthroughs, advanced tools & technologies, then you can even start with advanced certifications revolving around ethical hacking & cybersecurity. It is the best way to master various aspects of cybersecurity as it provides interactive education, gamified learning, real-time implementations from world-famous cybersecurity experts.

One recommendation that is trusted by the 100s of learners across the world is “Cybersecurity E-Degree”. It helps you master all the essential concepts including basic to advanced cybersecurity tools, cloud security, ethical hacking techniques, vulnerability exploitation, pen-testing & much more.

Not only this, but you will also learn some advanced & recent concepts of the cybersecurity world such as DevSecOps, Zero Knowledge Proof, Ring Structure & Homomorphic Structure. If you are looking to upskill then, you can find the link of this E-Degree in the description & try out yourself!

Prevent Businesses From Cybercrime!!

Learn Cybersecurity With Cybersecurity E-Degree

- 6 Modules
- 140+ Lectures
- 20+ Hrs of Learning
- 6+ Practical Projects
- Lifetime Support
- Certificate

Weekend Special Offer!

Save **Extra 60%**

Use Coupon Code: **CSHS60**

• 30 Days Money-Back Guarantee •