Cybersecurity Essentials

-Section I

SELF PACED | ON-DEMAND | INSTRUCTOR-LED | COLLABORATE | SHARE

vivaan-lms

A new way of learning

Table of Contents

Chapter 1 – Introduction to Cybersecurity

CREATION OF CYBERSPACE – A HISTORICAL OVERVIEW

American engineers developed a new technology during the war that later formed the foundation of the entire future of information warfare. They created a basic computer that was capable of rapidly performing the calculations necessary for ballistic trajectories. These early machines were so huge, extremely expensive, and created mounds of heat. Their main purpose was to be sent into conflict onboard a battleship where it could be used to quickly produce firing solutions that made the ship's heavy guns far more accurate. Initially, very few other practical military uses were envisioned for the computer.

Computer technology advanced slowly at first, mainly since the machines tended to be extremely expensive, difficult to operate, and reliant upon very fragile components that broke down even without any external stress. Early Standalone computers occupied entire rooms and unfortunately produced enormous amounts of heat that had to be bled off otherwise the machines would cook themselves. The computer parts such as the vacuum tubes that powered the earliest models could be easily shorted out. The modern computer term "bug" came about at that time and related to a coding error that led to malfunctions and short-circuits that were created by insects interfering with the vacuum tubes.

However, in 1958, a breakthrough occurred when Jack St. Clair Kilby invented the integrated circuit, which is the basis for all modern computer technology. This breakthrough invention not only miniaturized the key component allowing for vastly greater computing power in the same-sized machine, but it also eliminated many of the heat problems and reduced the cost to construct computers. At the time, even the most optimistic fans of new technology had only expected to create a machine that was capable of raw mathematical calculations, not knowing that decades later, it would revolutionize the world's communication system and that the rest of the world would revolve around a technologically advanced online environment and lifestyle.

When the concept of the Internet was first envisioned, even its wildest tech promoters and dedicated believers had no idea of the transformative power it would have upon human society. While the Internet's creators certainly expected to develop an information-sharing system that would allow researchers in a wide variety of locations to work together on challenging projects, they never expected the system to be used for entertainment, for commerce, and to support the basic communication needs of billions of users. They also did not have the fainted idea that this massive infrastructure construction program and invention would require an effort costing billions of dollars and creating millions of jobs around the world. It was a major accomplishing milestone in history as engineers and technicians were successful in connecting the world through wires and fiber-optic cables.

Commercial Internet service providers (ISPs) emerged in the late 1980s and early 1990s. The ARPANET was decommissioned in 1990. The Advanced Research Projects Agency Network (*ARPANET*) was an early packet switching network and the first network to implement the protocol suite TCP/IP. Both technologies became the technical foundation of the Internet.

About 27 years ago on August 6, 1991, the World Wide Web became publicly available. Its creator, the now internationally known Tim Berners-Lee, posted a summary of the project on the alt.hypertext newsgroup and gave birth to a new technology which would fundamentally change the world as we know it today. By 1995, the Internet was fully commercialized in the U.S. when the NSFNet was decommissioned, removing the last restrictions on the use of the Internet to carry commercial traffic. The National Science Foundation Network (NSFNET) was a program of coordinated, evolving projects sponsored by the National Science Foundation (NSF) beginning in 1985 to promote advanced research and education networking in the United States.

A DILEMMA AND CRITICAL PROBLEM SURFACES

Unfortunately, the pioneers, engineers, coders, and developers behind the Internet also tended toward optimism and devoted little thought to securing the network, thus a new dilemma and critical problem surfaces. There was little thought put into how this simple internet invention might one day facilitate the misdeeds of criminals and terror organizations, much less be used as a tool of national aggression and military conflict. Coders were successful in developing designs that facilitated information transfer and reliability but also unknowingly and simultaneously created inherent vulnerabilities that might be exploited by malicious actors.

Over time, Information or Data has been considered an aspect of power. Information's role has gained importance in both international relations and security, typically its huge information generation for political matters.

The ability for huge data generation and management has increased thereby manipulation of information has become the power source and to control some of the tangible resources such as raw materials, economy, productivity and many more, thus causing concern on the security of the data.

In this chapter, the information security logic is described in different sections, with providing the necessary technical background information on why it's insecure, how data/computers are vulnerable, who can exploit the information, and in which different ways.

WHY IS CYBER SECURITY IMPORTANT?

Whether you're conducting online business meetings, making an online transaction, or conversing with people online for business or personal reasons, you probably spend a lot of time online. Computers, smartphones, and tablets make it easy to access the Internet from just about anywhere. It's probably not surprising to learn that the average American between the ages of 7 and 16 spends about three hours a day on the Internet. We're now living in an age where the Baby Boomers (born 1946-1965) is waking up to the convenience of online shopping and the Millennial (a person reaching young adulthood in the early 21st century) has grown up to expect it as a staple part of their lifestyle.

Although the internet can be a fun, convenient and powerful tool that's prevalent both in the business and personal world, it's important to remember that it can also be unsafe. People's interpersonal data such as birthdates, Social Security numbers, and financial information are inputted into a variety of different websites every day. Most of the time, these websites are perfectly secure, but sometimes criminals can access a website and steal this data. Making sure the websites and the data they contain remain safe and secure is the job of cybersecurity experts. We spend more of our time online each year, so it's very important to keep in mind the basic concepts of safe online engagement so that we are not exposing ourselves to the detrimental vulnerabilities that leave us raw and victims to cybercriminals. It's important to remember that the more time we spend on the Internet, the more we expose ourselves to cybercriminals.

Technology Can Turn Against Us

Technological advances have benefited our world in immeasurable ways, but there is an ominous flip side: our technology can be turned against us. Hackers can activate baby monitors to spy on families, thieves are analyzing social media posts to plot home invasions, and stalkers are exploiting the GPS on smartphones to track their victims' every move. We all know today's criminals can steal identities, drain online bank accounts, and wipe out computer servers, but that's just the beginning. The fact of the matter is that to date, no computer has been created that could not be hacked. This vulnerability is not reassuring knowing and giving our radical dependence on these machines for everything from our nation's power grid, to air traffic control, to financial services.

As ubiquitous as technology seems today, along with the fast rate of growth for innovation and technology, if today's Internet is the size of a golf ball, tomorrow's will be the size of the sun! Welcome to the generation of the Internet, a generation where everything revolves around this global information grid, where every physical object will be online, and where the billions of people in the world come together to collaborate and share information across the internet "freeway." But with greater connections in this convenient privileged world, come greater risks, so we must be prepared for the unknown dangers lurking around the corners of this powerful tool.

A scary thought comes when we examine a glimpse at how cybercriminals can pose a danger to us, shows that even the items that were initially designed to help improve and assist human living can ultimately be turned upon us. For example, implantable medical devices such as pacemakers can be scanned and hacked to deliver a lethal jolt of electricity and a car's brakes can be disabled at high speeds from miles away. Meanwhile, 3-D printers can produce guns, bioterrorist can download the recipe for Spanish Flu or other diseases, and cartels are using fleets of drones to ferry drugs across borders.

Bad actors are primed to hijack the technologies of tomorrow, including robotics, synthetic biology, nanotechnology, virtual reality, and artificial intelligence. These fields hold the power to create a world of unprecedented abundance and prosperity. But the technological bedrock upon which we are building our common future is deeply unstable, and like a house of cards, can come crashing down at any moment.

The internet is a fascinating new tool and vehicle used to accomplish many fascinating new inventions, build empires of online businesses, complete global transactions in a split second used to collaborate with teammates, conduct global meetings and a myriad of other personal online interactions that humans have with each other.

However, there is a dark side of technological innovation and the unintended consequences of our connected world.

Everything is connected, everyone is vulnerable, so what can we do about it?

With these vulnerabilities at stake, there is a special branch and field of study and career called Cyber Security. Aan Systems offers this course as a way to protect your company and yourselves whether at work or home from the dangers of online crimes like data and security breaches, cyber-attacks, viruses, social media, and technology device vulnerabilities, and much more.

WHAT IS CYBER SECURITY

Cybersecurity is a branch of computer science that deals with protecting information systems from damage or theft. Cybersecurity experts are responsible for protecting the hardware and software of computers and computer networks, as well as the information stored on them. Cybersecurity experts are also responsible for protecting computer networks from disruption or misdirection of services.

Cybersecurity involves more than just making sure there are no suspicious programs running on a computer network. Individual computers, including servers, need to be inspected and secured as well.

Countermeasures

Cybersecurity experts create countermeasures. Countermeasures are actions, devices, or methods that prevent or eliminate a threat. Countermeasures can be used to protect both software and hardware. The software can be designed from the ground up with security as the main feature. This kind of software will usually include a system that tracks user activity, allowing security experts to follow a cybercriminal's trail once an attack has been detected.

Firewalls

Firewalls are the most common form of network security. They can be software based or hardware based. Firewalls are used to filter or block data being sent between two or more computer networks. Firewalls prevent viruses and other threats from infecting a computer that is connected to the Internet or another outside network.

Physical Countermeasures

Physical countermeasures are built directly into the computer itself. Some computers have intrusion or break-in detection systems. These are special devices or software that know when a computer's case is opened. This can alert security experts that a computer has been tampered with. Another way to physically secure a computer is by disabling USB ports. This prevents unauthorized access to the computer and prevents someone from connecting an infected device to a secure computer.

Encryption

One way to protect digital data is through encryption. Encryption translates the data into a form that can't be read unless you have the correct password.

COMMON MISCONCEPTIONS OF CYBER SECURITY

Informed people become safer people that are more aware of their actions and surroundings, thereby greatly reducing the incidents of data and security breaches and vulnerabilities. Often, people have a misconception of internet safety and initially don't even acknowledge that this is even a problem. Some people believe that hackers only hack the rich or famous. In reality, millions of average people around the world are hacked every day, partly due to the ignorance and perceived notion that people think they cannot be hacked. This can be attributed to reasons such as:

(1) **They think that using Macintosh computers gives them immunity to hackers.** This is a rumor and is false, as there are major attacks that exist for the Macintosh Operating System. Computerworld states that there is a recent warning that Mac malware exploits climb 270% (https://www.computerworld.com/article/3262225/apple-mac/warning-as-Mac-malware-exploits-climb-270.html)!

(2) **They believe they don't visit dangerous websites, so they cannot be hacked.** While this is a great thing to do, it simply is not good enough. Hackers go out of their way to make their hacks seem very legitimate, fooling you into giving up your data. This is often called social engineering. In the context of information security, social engineering is the use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes.

(3) **They believe that they cannot be hacked because they use antivirus and firewall programs.** Although it is very good to use antivirus and firewall programs, there is much more that needs to be done to stay safe.

How big of a role you play in the maintenance of cyber security in your company gives a clue to Hackers that you are important and that they want to target you to get through into the company's network. With this access, hackers can essentially control everything in your company.

COMPONENTS OF CYBER SECURITY:

Some Elements of Cyber Security are

- Application
- Network
- Information/Data
- Disaster Recovery
- User Education

Figure 1.1: Components of Cyber Security

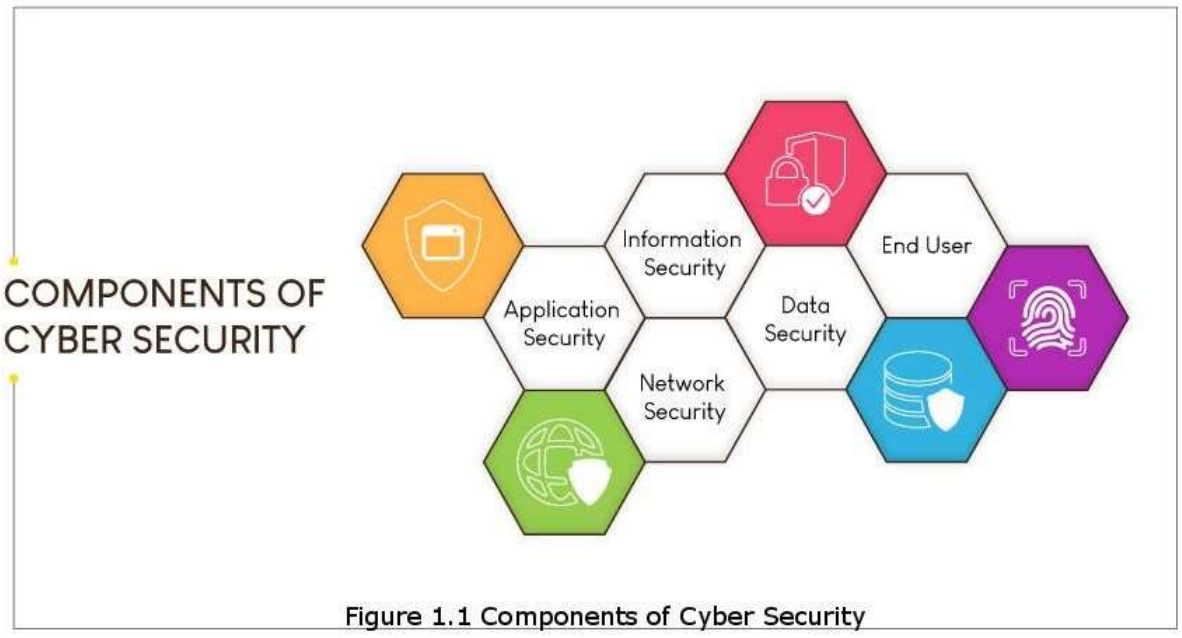


Figure 1.1 Components of Cyber Security

Application Security

The application is a program or a set of programs that are developed for end users. This application carries the risk or vulnerabilities of attack when installing on the system or during use.

The hardware and software are the main assets for the organization and refers to the value of data in the file or the systems. Hence, to reduce the risk, security can be introduced to the application and security steps taken throughout the whole application. Normally, threats may arise due to vulnerabilities of an application when security policies are not applied.

Information / Data Security:

Data and information security relate to the concept of protecting and securing data on a multi-level approach and addresses concepts such as leakage, damage or misuse. This security system has different modules for the administrators. It is important that this data is kept secure and confidential to protect it from loss, damage, or theft.

Network Security:

Network security refers to preventing information access to files and directories in a computer network against hacking, misuse, and unauthorized changes to the system. An example of network security is an anti-virus system and to approve the check for the proper user id and password to access the systems. This security refers to activating policies which are approved for the organization in an aggressive manner to monitor the unwanted access and misuse of the network.

- ***Multifactor Authentication*** **-** Multi-factor authentication is a method of login verification where at least two different factors of proof are required. There are generally three recognized types of authentication factors:
  - **Type 1 – Something Known –** includes passwords, PINs, combinations, code words, or secret handshakes. Anything that you can remember and then type, say, do, perform, or otherwise recall is categorized in type 1.
  - **Type 2 – Something You Have –** includes all items that are physical objects, such as keys, smartphones, smart cards, USB drives, and token devices. A token device produces a time-based PIN or can compute a response from a challenge number issued by the server.
  - **Type 3 – Something You Physically Are –** includes any part of the human body that can be offered for verification, such as fingerprints, palm scanning, facial recognition, retina scans, iris scans, and voice verification.

This security can include three levels of authentication used in combination for robustness and starts with multi-factor criteria based on the policies such as one factor for passwords or pins and security checks, and other multi-factor criteria for passwords mixed with dongle and mobile. Other levels of security involve checking the user credentials to provide them access to the network's data or to allow information exchange. Firewall access policies will check for unauthorized access to the network. Potential malware content (like Trojans and worms) is detected by antivirus software and deletes it accordingly. Unexpected or uncontrollable content is detected using a rarity detection system, which monitors the network traffic. By monitoring a network's traffic, situations like service attacks or

tampering of files can be avoided. All events and incidents taking place within the network are logged to trace during scrutiny.

Disaster recovery/business continuity planning

Disaster Recovery, an aspect of security planning, aims to protect an organization from significant negative events. Following a disaster, it allows for organizations to quickly recover and continue with their mission-critical functions.

Disaster recovery planning is a critical function, wherein a structured approach is put in place to respond to unplanned incidents that can jeopardize a company's IT infrastructure.

- **Components of a disaster recovery plan:**
  - Disaster recovery policy statement
  - Key personnel and their contact information
  - Description of steps to be taken immediately after the incident
  - Diagram of entire network and recovery site
  - Directions to reach the recovery site
  - A list of software and systems to be used for recovery
  - Sample templates for a variety of technology recoveries
  - Tips to handle the media
  - Summary of insurance coverage
  - Proposed actions for dealing with financial and legal issues

End User:

Unfortunately, ensuring end-to-end cyber safety and computer protection has been challenging for most organizations, with reasons being attributed to a variety of factors including a shortage of skills, lack of awareness and training, inefficient education and delayed incident response planning.

End-user education and awareness is a very critical aspect of Cyber Security, which needs to be addressed regularly to avoid vulnerability. When you evaluate your company's security, you will be surprised to find that the end user in the company is the first to breach security. This is usually done so due to lack of awareness.

With ever-increasing cybercrime, as well as an increase in BYOD (Bring Your Device), it is more important to educate employees about staying safe from cyber attacks. On the one hand, BYOD has provided flexibility to users, and on the other hand, it has also given rise to an increase in security breaches.

Employees need to be educated to be vigilant at all times and need to be able to handle sensitive information carefully. Security policies and its thorough implementation within the company is a must. Employees must also understand and comply with regulations to help maintain the health of the company. Employees should also be mandated to take online courses on cybersecurity to stay updated on the latest information.

SOCIAL MEDIA SECURITY

With the rampant use of social media comes a host of security breaches. Threats like social engineering, targeted phishing attacks and misuse of fake accounts are on the rise. Companies are in a dilemma as to whether social media access is to be blocked for employees or take the risk of malware and other breaches.

To continue to enable usage of social media at the workplace, strong security policies and awareness are essential. Here are a few tips to consider while developing a social media security plan.

Develop a Social Security Policy

Develop a social media security policy to help significantly reduce security breaches, which can also be used to govern social media usage by employees. Proper enforcement and continuous monitoring of the policies will help in successfully protecting the company.

Multi-Dimensional Risk-Based Approach

Poorly protected infrastructure and information and badly managed systems become a vulnerable target to cyber threats. Thus, have a multi-dimensional risk-based approach that is information-centric, which takes into account the unique problems of social media usage.

Identify Safe Social Media Sites for Employees

Since not all of the social media sites are safe, help employees identify safe social media sites and only allow employees access to the safe ones. Companies need enhanced network visibility to monitor, detect and in turn, protect their assets. This can be done by data loss prevention and web content filtering solutions.

Classify Sensitive Data

Companies need to identify sensitive data and define it clearly in the social media security policy.

Protect Endpoints

Information access across multiple devices needs to be monitored (laptops, tablets, phones, etc). The kind of sites that can be accessed across devices needs to be defined.

Educate Employees

Employees need to be provided with proper guidance on the kind of social media content they can and cannot access in the workplace.

CONCEPT OF CYBER SECURITY

Cybersecurity has an intrinsic quantitative element and in particular has established methods, technologies, and practices that are available for assessing the strength of Cyber Security. Under well-specified conditions, the methods are namely known as **cryptography and authentication methods** (e.g., password authentication). In other fields, considering the cost of collecting data, empirical investigations have approximated the probability that the attacker would succeed with different attacks on the level of abstraction manageable in enterprise security.

Results are described in theory and used in the model concerning **software vulnerabilities** where there is empirical data available concerning publicly disclosed software vulnerabilities in databases. It is also possible to identify the vulnerabilities for which exploit code is publicly available. Models have been developed to predict how many cybersecurity vulnerabilities that will be publicly disclosed for a product.

Number of Vulnerabilities Correlation

For instance, the number of vulnerabilities found in a software product has been found to correlate with the number of user-months the product has accumulated and the time it has been on the market.
The effectiveness of different procedures for **deploying security** and its subsequent patches has also been assessed. When it comes to the development of new exploits, it is reasonable to assume that this is a straightforward task for a professional penetration tester when patch information is available for the vulnerability.

The basic argument is that poorly designed and maintained software systems tend to embed highly complex code and architectures, which in turn increase the likely occurrence of vulnerabilities waiting to be exploited.

Intrusion Detection System

An intrusion detection system (IDS) is a system that monitors network traffic for suspicious activity, and issues alert when such activity is discovered.

Benefits of Intrusion Detection Systems:

- Ability to identify security incidents.
- Used to help analyze the quantity and types of attacks.
- Organizations can use this information to dynamically change their security systems.
- Organizations can implement more effective controls.
- IDS can also help the enterprise get and meet regulatory compliance by giving greater visibility across their networks, making it easier to meet security regulations.
- IDS can help improve security responses, and since they are automatic, they reduce the error associated with manual data collection.

Features and Capabilities of Intrusion Detection Systems:

- Reacts to intruders by blocking them or the server.
- Generates an alarm when security has been breached.
- Recognizes and reports when the IDS detects that the data files have been altered.
- Monitors the operation of routers, firewalls, servers, and files.
- Provides a way for administrators to troubleshoot, tweak, tune, organize, and understand relevant operating system audit trails and other logs that are otherwise difficult to obtain or track.
- Provides a user-friendly interface so non-expert staff can easily assist with managing system security.
- Includes an extensive attack signature database.

PROTECTING PERSONAL DATA FROM CYBER ATTACKS

In recent times, we notice that cyber attacks are on the rise, as we witness them on the front page of newspapers. In many practical cases, the victim does not even know that they are being attacked. Therefore, knowing to identify the new methods by which cyber attacks are taking place is a key step to preventing and stopping cyber attacks.

Ways to Secure Our Data from Cyberattacks:

Stay-Informed
Keeping personnel current on a frequent basis about threats that affect the user is the easiest way to protect the data in the security world. The Federal Communications Commission (FCC) is an independent agency of the United States government created by statute (47 U.S.C. § 151 and 47 U.S.C. § 154) to regulate interstate communications by radio, television, wire, satellite, and cable. The FCC tracks digital scams and informs the user, free of charge. For those who need to protect their data from scams and attacks, the FCC also provides training for the user to learn about cybersecurity facts.

Canary Tokens
The Canary Token is a free tool that is available at canarytokens.org and is a tripwire tracking tool that helps the user to identify whether their systems have been hacked or breached. The tokens allow you to implant traps in your production system by having the attackers announce themselves. What this means is that if the attacker ever uses the token that you generated, an email or SMS notification is sent to you that the attacker visited the site you have set the Canary Token at.
As a bonus, canarytokens.org gives the user a bunch of hints and tools that increase the likelihood of an attacker tripping on a Canary Token. It's one of the digital tracking methods to let the user determine if any unauthorized access happened to the computer or file which is protected by the user. This can be used by simply creating a token for the particular file and waiting for the hacker to trigger the alert. This security measure is a free, quick and easy way to help defenders discover if they've been breached and consists of a unique identifier that can be embedded in either HTTP URLs or hostnames. Whenever that URL is requested, or hostname is resolved, a notification email or SMS is sent to you immediately to indicate that your site was visited or breached.

Encrypted-Email
Email encryption often includes authentication and protects the email from other entities on behalf of the intended entities by disguising the content of email messages to protect potentially sensitive information from being read by anyone other than intended recipients. Email providers often use standard encryption to keep it safe from hackers. Sensitive data that requires encryption include messages, personal information, addresses, and financial information.

End-to-end encryption (E2EE) is a step up from just standard encryption and is a system of communication that ensures that only the communicating users can read the messages and no other third parties can interfere, read, or decipher data or messages being communicated or stored. End-to-end encrypted service is a secure form of communication and helps only the intended person to read it. This system is designed to defeat any attempts at surveillance or tampering because the data is scrambled and protected from third party eyes and they cannot decipher the data being communicated or stored.

Anti-Malware
Antimalware (anti-malware) is a type of software program designed to prevent, detect and remove malicious software, called malware, on IT systems, as well as individual computing devices. In today's Internet world, where every device is connected, we need to be aware of cyber attacks and keep antivirus software up to date. During a cyber attack, the malicious malware software is designed to infiltrate and attack your computer. This detrimentally damaging malware can be in the form of viruses, worms, Trojan horses or spyware. By using a recommended Anti-Malware software to detect and remediate malicious programming on individual computing devices and IT systems, you can be protected from this layer of danger coming from malware.

Perform Updates
Performing regular updates on your computer systems and devices is a critical step to maintaining the integrity and robustness of your systems and keeps them safe from the latest security threats. Many of the more harmful malware attacks take advantage of software vulnerabilities in common applications like operating systems and browsers. Keeping your software up-to-date is critical so that your systems can remain stable and ready to face the next security threats successfully. These are big programs that require regular updates to keep your systems safe and stable. So, instead of procrastinating about software updates, regard this as essential steps you can take when it comes to protecting your information. If possible, select auto-update for software on both your mobile devices and computers. For software that doesn't auto update, make it a habit to check for and apply available updates regularly. Software updates might seem unnecessary or annoying but only take a few minutes of your time. Skipping updates creates a vulnerability and keeps the door open for hackers to access your private information, putting you at risk for identity theft, loss of money, credit, and more. Before downloading any software, read reviews to make sure it`s safe to install.

The recent Equifax data breach is a good prime example of a cyber attack caused by the carelessness and refusal of companies to update their computer systems. Here, 143 million Americans were potentially affected, with Social Security numbers, birth dates, and

home addresses exposed. The hackers were able to access the credit reporting agency's data through a known vulnerability in a web application. A fix for this security hole was available two months before the breach, but the company failed to update its software. This was a tough lesson for all to learn from and easily could have been prevented. This proves that software updates are important because they often include critical patches to security holes.

Secure-Wi-Fi-Network

Many users may be ignorant about securing the network due to a lack of knowledge or due to investments. However, adopting simple methods of strong passwords and periodically changing the same would secure their Wi-Fi network devices.

Use an inconspicuous non-attention-grabbing network name (SSID) provides an extra incremental layer for protection of data. This might seem like a moot point and a basic concept because though it doesn't seem like the network name could compromise security, it certainly can. Using too common of an SSID, like wireless or the vendor's default name (router name/type) can make it easier for someone to crack the personal code of WPA or WPA2 security. The reason is that the encryption algorithm incorporates the SSID, and password cracking manuals used by hackers are preloaded with common and default SSID. Using just the default SSID makes the hacker's job easier.

Destroy-Hard-Drives

A typical home computer hard drive can contain your credit card numbers, bank account numbers, social security information, tax records, and website logins and passwords and this information can remain even if "erased" or reformatted. Therefore, when disposing of an old PC, there is only one sure way to securely erase the information on the hard drive: You must destroy the magnetic platter inside before it ends up in the trash. To destroy the magnetic platter, use a T7 screwdriver to remove as many screws as you can access. Using a combination of the screwdriver and the hammer, remove the main circuit board from the enclosure. Strike the hard drive until the case opens and take out the magnetic platter. Using the hammer, strike the magnetic platter to ding, scratch, and dent up this plate.

Turn Off Your Computer

To reduce the chances of being exposed to security threats, if you are not using your Internet connection or the computer, then turn them off. When we leave our computer systems turned ON, this is an easy access point to your personal information. By turning the computer off after the completion of work, this reduces chances for hackers and thieves to steal personal information from the systems.

PROTECTING THE ENVIRONMENT IN CYBER SECURITY

For every business, the series of data or the information which connects to the sensitive data is subjected to security threats. Any business can be affected by cyber attacks, so every business needs to have a proper measure of protection.

Know Your Network and the Data you Handle

Know what information exists on your network and be aware of the kinds of data that are present on the network and the consequences in case of its compromise. Creating segments in the network and providing access to only those who need it helps to protect sensitive information.

Create Security Policies and Educate Staff

Create security policies and procedures and educate your staff on them. Educate employees on how to create strong passwords, the do's and don'ts of downloading, and how to spot phishing attempts. Installing security patches is also an effective way to protect your business. Make sure all employees are following security procedures and create a disciplinary action for employees who don't comply.

Track Compliance

Track and verify your company's compliance with federal, state, and industry regulations. Comply with industry-specific regulations across different industries, state and federal regulations like Federal Trade Commissions and consumer privacy and data securities that apply to all businesses. Additionally, financial regulations such as Data Security Standard (PCI DSS) are to be followed. A data breach out of compliance can lead to penalties and enforcement actions.

Incidence Response Plan

Have an incident response plan in place so that you can limit the damage when a potential data breach happens. During the occurrence of a data breach, the vulnerability that led to the data loss needs to be fixed quickly. Then, you need to analyze the findings and determine whether customers and regulators need to be notified. Having a plan and being

ready to execute it can save your business.

Have a Business Recovery Plan

You should also have a business recovery plan to keep your business running due to a vulnerable situation. In a situation, whereas you are suddenly left with no access to online databases, it is important to have a local backup.

Chapter 2 – Introduction to the Digital World

PEOPLE ARE ASSETS SO PROTECT & TRAIN THEM CONSTANTLY

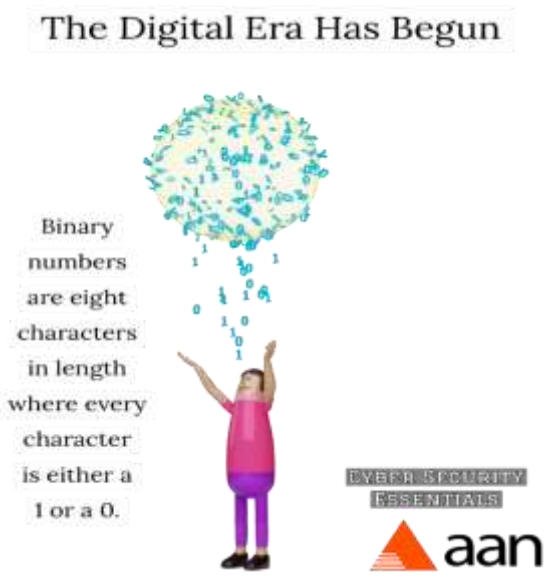
If we look at security breaches over the last five to seven years, it's pretty clear that people, whether it's through the accidental or intentional introduction of malware, represent the single most important point of failure regarding security vulnerabilities. In the past, companies used to roll out an annual best practice for security to train their employees and think that they were done. However, with the rate and changes of the digital world, this no longer is enough to keep us safe and ongoing training and knowledge is constantly required to keep systems and employees up to date on the vulnerabilities of the internet. Since your people are your assets, you need to invest in them continually, and organizations must do what is called people patching. Similar to updating hardware or operating systems, you need to consistently update employees with the latest security vulnerabilities and train them on how to recognize and avoid them. People represent a large potential attack bridge in every organization, and so it is important that appropriate ongoing security programs are in place. Security teams and cybersecurity professionals exist to protect information, people, and the business.

INTRODUCTION TO THE DIGITAL AGE & DATA DRIVEN WORLD

The Digital Age, Information Age, Computer Age, or New Media Age are all popular terms that are used to describe the advent and rise of the digital age. The digital age is closely coupled with the rise of personal computers. But the founder of the information age or information theory as it is known is Claude E Shannon, an American mathematician, electrical engineer, and cryptographer.

Shannon's thesis is considered one of the most important in the 20th century. He proved how George Boole's logical Algebra could be implemented using electronic circuits of relays and circuits. Shannon's landmark discovery showed that information could be quantitatively encoded as a series of zeros and ones, known as the binary code. Binary numbers are eight characters in length where every character is either a 1 or 0. The placement of each 1 indicates the value of that position, which is used to calculate the total value of the binary number. This is the beginning of the digital era.

Figure 2.1: Beginning of the Digital Era



By the 1970s, with the development of the Internet and a decade later with the adoption of personal computers, the Information or Digital Revolution was underway. The digitization of information has had a significant impact on traditional media businesses, such as book publishing, the music industry and major television and cable networks. As information is increasingly described in digital form, businesses have adapted and found means to capitalize on the information age.

DATA DRIVEN WORLD FACTS

Some mind-boggling facts on a data-driven world:

- ✓ 6 million developers worldwide are working on big data and advanced analytics
- ✓ More than 40% of data science tasks will be automated by 2020.
- ✓ Though 85% of companies are trying to be data-driven, only 37% of them have been successful.
- ✓ By 2020, 1.7 megabytes of information will be created every second per person

With increasing data generation, comes an ever-increasing risk of data breach and privacy issues. Cybersecurity threats are so critical in today's world that they are making front-page headlines. Privacy, security, and trust are all increasingly at severe risk and are also closely linked with the data-driven world.

Here are some simple steps to help protect ourselves from unnecessary data breaches:

- ✓ Adapt the habit of protecting sensitive information.

- ✓ Restrict downloading files from the Internet especially if you are not sure of the source.
- ✓ Do not use unencrypted devices in the workplace, which can compromise sensitive information.
- ✓ Make use of strong passwords and make sure to change it regularly.
- ✓ Monitor data leakage
- ✓ Be aware of the latest tools to protect your data.
- ✓ Access to sensitive information must be restricted to a few key people only.
- ✓ A quick response plan must be put in place to handle a data breach situation.

INTERNET

The Internet has revolutionized the computer and communications world drastically. Its discovery and exponential growth have had a profound impact on various aspects of human life. The Internet emerged in the USA in the 1970s but became visible to the public by the 1990s. Current global usage of the Internet is half the world's population.

The power of the Internet and its widely accessible reach is so profound that it can be used for almost any purpose. The Internet was born as a result of an effort to connect various research networks in the USA and Europe.

The rise of commercial Internet services and applications helped to fuel further commercialization of the Internet. One of the key factors for the Internet to become widespread is due to the rise of personal computers and the advent of Local Area Networks (LAN) to link personal computers.

The future of the Internet may not be 100% crystal clear, but there are endless possibilities for its growth and usage. Increasing availability of wireless networks will continue to enable access of Internet across a variety of devices. Higher network access speeds will become more readily available for mass usage. With higher network access speeds, data consumption will increase. Communications connectivity will be one of the key functions of the future of the Internet with more and more devices getting connected to the Internet.

INTRANET

An intranet is a secure and private enterprise network that shares data via the Internet. An Intranet differs from the internet, which is a public network. Intranet acts as a key business efficiency tool. Listed below are some of the benefits of the intranet.

1. **Provides a Platform for Better Internal Communications -**
   The Intranet acts as a communication platform to share announcements, memos, staff news, etc. The information can be posted on the intranet and can be accessed centrally by employees at any time.

2. **Streamlines Data Management** –
   With an intranet, documents can be uploaded and accessed by employees at any time. Employees can collaborate on projects and information.

3. **Better Customer Service** –
   With anytime access to accurate and important information, this leads to better performance and customer service by employees.

4. **Better Employee Productivity**
   Since employees have easy access to all important information on the intranet, they do not have to waste time looking for files or data, and in turn, productivity improves.

SOCIAL MEDIA

Social Media is a very common term being used in today's times. It is often used to describe sites and applications like Facebook, Instagram, Snapchat, and Twitter. Social Media is a web-based communications tool, which provides a platform for people to interact with each other and also to consume information. This may be a very broad definition of social media but listed below are a few common features of social media platforms.

COMMON FEATURES OF SOCIAL MEDIA PLATFORMS

1. ***User accounts*** - Creating your account is usually the first step for using a social media platform. You can use your account to log in to the platform and further interact with others.

2. ***Profile pages*** - A profile page is your identity on the social media platform. It generally includes your photograph, a brief write-up about you, personal information and recent activity among others.

3. ***Friends, Followers, Groups, Hashtags*** - You can use individual accounts to connect and follow others. You can also subscribe to the information you like.

4. ***News Feeds*** - When you connect with different people or groups on social media, you can see that information in real

time in your news feed.

5. ***Personalization*** - Social media platforms allow users to configure and customize their news feeds and profiles as per their preference. Users can also control their friends and followers list.

6. ***Like buttons and comments section*** – A basic interaction on social media platforms includes the 'Like' button popularized by Facebook. Further, users can post comments as well on the social media platforms.

SIMPLE CORPORATE NETWORK

Computer Networks are everywhere, but have you ever wondered how are they created and what is the technology behind it?

Corporate Network

A corporate network is a group of computers and network devices that are connected to the same area, which is all owned by the same company.

Networking Types and Structures

Networks can be wired or wireless, with most of them today is a mix of both.

Wired Networks:

Pros:

- ✓ Ethernet ports are available on almost all laptops/ PCs
- ✓ More secure than a wireless network
- ✓ Provides fast data access speed

Wireless Networks:

Pros:

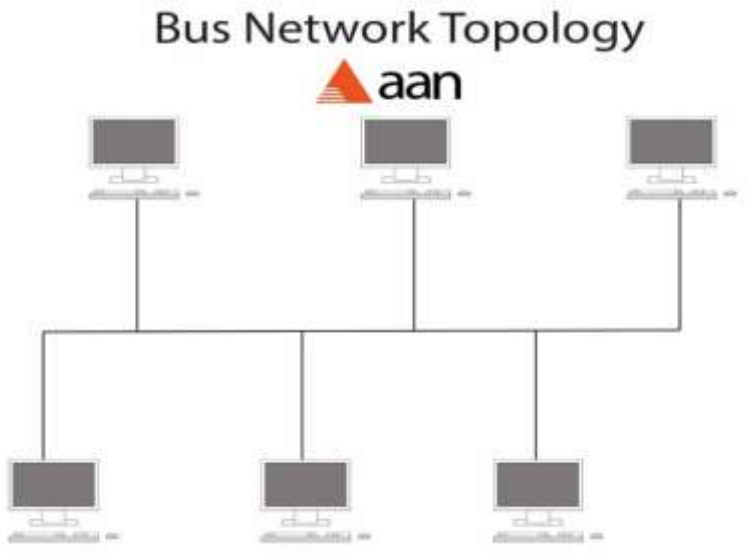
- ✓ Easy to setup
- ✓ Can be accessed across multiple devices
- ✓ No cable required
- ✓ Can be used on home and public networks
- ✓ Allows remote access management

Networking Topologies and Layout

Network nodes can be connected in many ways. It may not be very significant for small networks, but it is important for large computer networks. Some of the commonly used network topologies are Bus, Ring, Mesh, Star, and Hybrid.

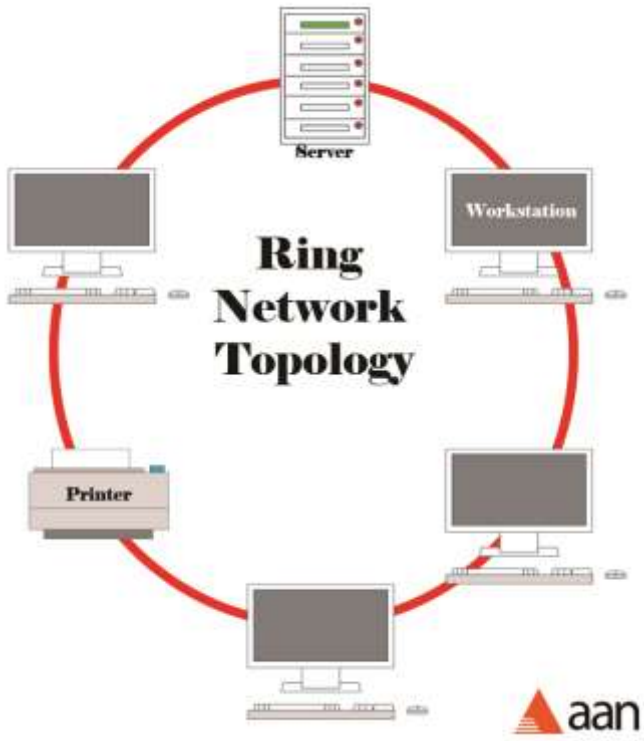
1. **Bus Network:** A network topology in which nodes are directly connected to a common linear (or branched) half-duplex link.

Figure 2.1: Bus Network Topology



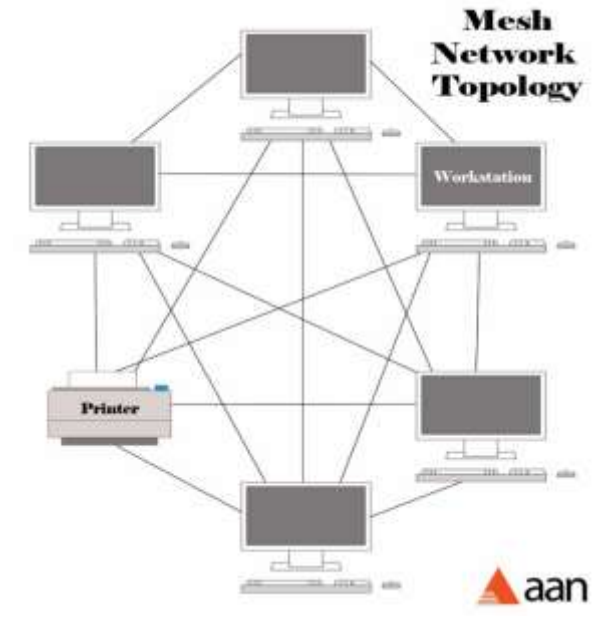
2. **Ring Network Topology:** A network topology in which each node connects to exactly two other nodes, forming a single continuous ring pathway for signals through each node. Data travels from node to node, with each node along the way handling every packet.

Figure 2.2: Ring Network Topology



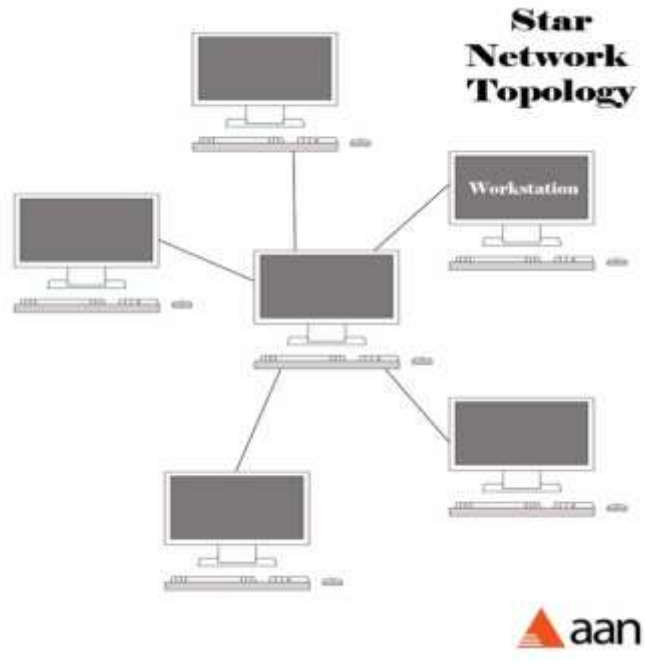
3. **Mesh Network Topology**: A mesh network is a local network topology which the infrastructure nodes such as bridges, switches, and other infrastructure devices are interconnected with one another directly, dynamically and non-hierarchically to as many other nodes as possible and cooperate with one another to efficiently route data to or from clients. This mesh network setup allows for the most transmissions to be distributed even if one of the connections goes down. An example of a mesh topology is commonly used for wireless networks.

Figure 2.3: Mesh Network Topology



4. **Star Network Topology**: The star topology or star network, is one of the most common computer network topologies and visually looks like a formation of a star. In its simplest form, the star topology is a network topology where each device host in the network is attached to a central node that acts as a central hub or switches to transmit messages.

Figure 2.4: Star Network Topology



5. **Hybrid Network Topology:** A topology that is a combinational mixture of two or more different basic network topologies interconnected together to allow more functionality of combined features. The advantages of hybrid network topologies include increased reliability, scalability, flexibility, and effectiveness. However, the disadvantages of hybrid networks include the complexity of design and a costly hub and infrastructure.

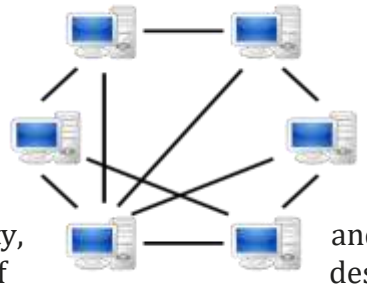
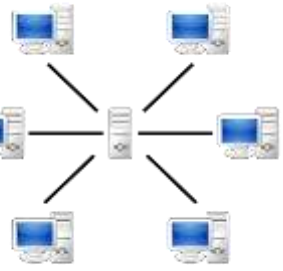
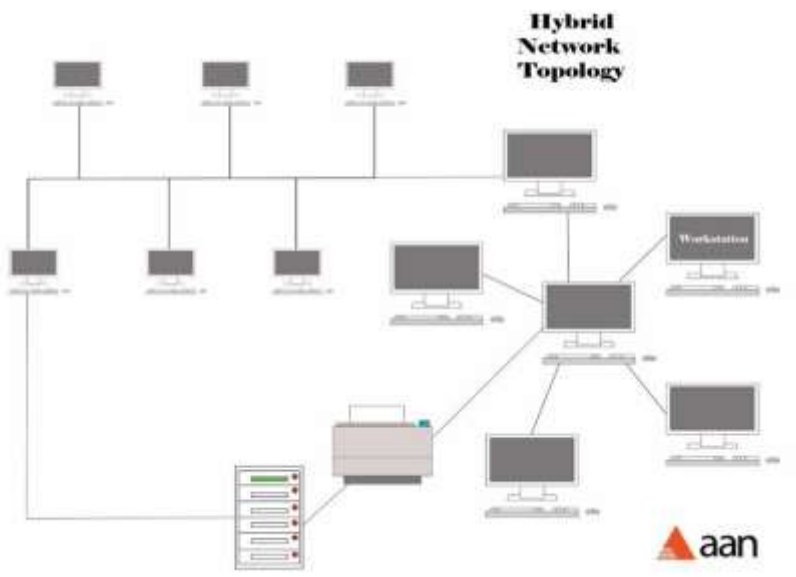


Figure 2.5: Hybrid Network Topology





6. **Peer to Peer Networking Model:** All the nodes are equal, and any node can talk to any other node.

Figure 2.6: Peer to Peer Networking Model

Pros -

- ✓ Easy to setup
- ✓ Not dependent on a single node
- ✓ Inexpensive hardware
- ✓ Central administration is allowed
- ✓ Better distribution and control of network traffic

7. **Client-Server Networking Model**: In this model, the server has a special role. This model is used on the web, and the client connects to a server to use the required services.

Figure 2.7: Client-Server Networking Model

Pros -

- ✓ Easy to find resources
- ✓ Provides a secure environment
- ✓ Easy to administer
- ✓ Allows large data storage and access

DATA TYPES

A data type in computer programming is an indication to the compiler or interpreter as to how the programmer would like to use the data.

Common data types across programming languages include:

- ✓ Integers
- ✓ Boolean
- ✓ Characters
- ✓ Floating-point numbers
- ✓ Alphanumeric strings

DATA CLASSIFICATION

Data classification is the process of organizing data into different categories to make use of it efficiently. A well-organized data classification system supports easy searching and retrieval of data. This can be of importance for compliance, legal discovery and risk management. Once data classification has been created, appropriate security and access measures need to be defined based on the organization's data security policy.

Sample data classification:

- ✓ ***Category 1***- Data that can be shared with the public like contact information and price lists.
- ✓ ***Category 2*** - Internal data that cannot be disclosed to the public like organizational charts, sales contest rules, and scientific data.
- ✓ ***Category 3*** - Sensitive internal data like employee appraisals, employee salary, and business data.
- ✓ ***Category 4*** - Highly sensitive data like credit card numbers and social security numbers.

IMPORTANCE OF DATA

New technology adoption brings about new challenges for any organization. In today's scenario, new technologies like Artificial Intelligence, Internet of Things and automation is creating a significant impact on the industry. Companies will be able to differentiate themselves today based on how well they manage data. Proper usage of data is only going to become more and more critical with the advent of newer technologies, especially with the focus being on connected devices.

Benefits of good quality data on organizations:

- Allows for better decision making, which in turn boosts confidence and efficiency.
- Allows staff to be more productive and not waste time on correcting wrong data.
- Organizations can maintain better compliance and not land themselves in unnecessary trouble with bad data.
- Organizations can focus on more targeted marketing efforts with focused communication efforts.

Repercussions of poor quality data on organizations:

- Lack of confidence in data can lead to poor decision-making and loss of trust.
- Data, if not treated as strong assets for a company, can lead to missed opportunities.
- Poor data quality can lead to a loss of revenue due to poor information on prospective customers.

OFFICE TOOLS FOR THE DIGITAL WORLD

The workspace today is a completely different ball game than what it used to be before. Offices have moved almost completely towards being digital and have done away with most of the traditional methods. The technology developed in the Information Age has completely changed the way we do business. Computers in the workplace are more than just word processors; they have become advanced communication hubs. Additionally, smartphones are also capable of handling work. In today's workplace, it's important to empower employees with suitable tools to support collaboration and productivity.

A digital workplace must focus on providing these essentials needs:

- ***Trust*** - focus on secure data and people
- ***Collaboration*** - focus on productivity and effective teamwork
- ***Mobility*** - allow employees to get their work done from anywhere thereby providing flexibility
- ***Intelligence*** -provide better insights for faster decision making

Some of the popular office tools for the digital world are:

- ***Hootsuite*** - A popular social media management tool which helps you to post, monitor and grow your brand across social media platforms.
- ***BuzzSumo*** – An important tool for marketers for content and competition research
- ***Fiverr*** - An online marketplace for on-demand freelance services like graphics design, digital marketing, programming & tech, writing & translation, etc.
- ***Unbounce*** - A popular tool used for building and publishing landing pages. Landing pages are used as marketing tools to focus on increasing web traffic towards the landing pages, and in turn, increasing conversions.

- ***Canva*** - A tool used to create your graphic design using ready-made templates. For example, you can create your brochures, proposals, calendars, posters, and infographics among others.
- ***CJ Affiliate*** - An online marketing tool used by advertisers to look for their product to be published and for publishers to get their product picked.

ACCESS METHODS

An access method is a technique used to store and retrieve data. Access methods are identified primarily by the data set organization. Access methods have their dataset structures to organize data, macros to define data sets and utility programs to process data sets.

Commonly used access methods are:

- ***QSAM*** - Queued Sequential Access Method - the most commonly used method wherein the records are arranged in the order that they are entered to form sequential data sets.
- ***BSAM*** - Basic Sequential Access Method - used in specific cases wherein the records are arranged sequentially in the order in which they are entered.
- ***BPAM*** - Basic Partitioned Access Method - arranges records as members of a partitioned data set
- ***VSAM*** - Virtual Sequential Access Method - records are arranged by an index key, relative record number or relative byte address.

DEVICE PROTECTION

Your end users are connected to the World Wide Web in several different ways.

Methods to Connect to the Internet:

- Laptops
- Desktops
- Smartphones
- Tablets
- Fitbit, Apple watches
- Walkie Talkies
- And when away from the workplace: Baby monitors, game systems, GPS Systems

These are all potential doorways through which a cybercriminal could access your company's infrastructure and cause serious harm. Having devices stolen isn't the only way these can be compromised though. Therefore, security awareness needs to be a robust approach where this risk is concerned. The layers of your security awareness device plan should include training and support from management.

Like any form of security awareness, handling the threats that face company devices requires a top-down approach. Again, management must be involved and onboard, and they must make security a priority, not put it on the back burner.

Your corporation needs a policy regarding the use of devices provided to staff. This must include everything from where these devices must be stored and what they can be used for. Sadly, many companies have a policy that talks about cybersecurity, but they haven't updated it to reflect the use of devices that can be taken out of the office.

Smartphones, tablets, laptops or other portable devices can be stolen, even at the office, posing a direct threat to the company. Therefore, security awareness for end users must address proper methods of securing them, especially for workers who travel for business.

MOBILE DEVICES

A mobile device is a general term used for a handheld device, smartphone, or computer. The increased rise and growth spurt in mobile devices has been attributed to new data storage methods and processing and display technologies. Mobile devices can do almost anything that was earlier perceived as being capable of being done only by a personal computer.

Characteristics of a mobile device:

- Powered by a built-in or removable battery
- Has a prominent screen for viewing content
- Supports Internet access
- A majority of them have touchscreen interface
- Supports media consumption
- Supports download of files from the internet
- Lightweight and portable

DATA STORAGE ENTERPRISE APPLICATIONS

Enterprises need sophisticated IT systems, from the data center to the desktop, and all these systems perform complex operations. They need to keep up with user demands for good performance.

Enterprise Storage:

Enterprise storage is a centralized repository for business information that provides common data management and protection, data sharing functions, and connections through to several computer systems over LAN or WAN.

Enterprise storage uses Storage Area Network (SAN) which provides benefits like high availability, disaster recovery, data sharing, and reliable backup and restoration. Enterprise applications need robust IT infrastructure. These systems cannot afford any disruptions for long periods of time.

At the storage level, the following are the characteristics that a system must possess -

- Seamless expansion of storage capacity
- Easy migration of application data between performance tiers
- Provide tech-refresh of storage controllers while in function
- Ability to include faster storage protocols as needed

ASSETS IDENTIFICATION

Assets identification is a critical process where organizations keep track of their fixed or movable assets. Knowing about the equipment in your organization is an important part of asset tracking. In cases of duplicate or incorrect labeling, you are at risk of compliance issues or loss of equipment, or you might fall behind on the required maintenance of the asset.

Asset Tags:

For asset identification, the most common method used is asset tags. Asset tags or asset labels are used to identify physical assets. These asset tags have a serial number which is issued for tracking and identification. Barcodes can also be utilized to track assets. On scanning the barcode, the details of the asset are entered into the asset tracking software. Radio Frequency Identification (RFID) asset tags can also be used to track assets.

RESOURCE ACCESS CONTROL FACILITY

Resource Access Control Facility (RACF) is an IBM security software product that provides access control and auditing functionality for the z/OS and z/VM operating systems.

Its main features are:

- Identification and verification of a user via user id and password check
- Identification, classification, and protection of system resources
- Maintenance of access rights to the protected resources
- Controlling the means of access to protected resources
- Logging of accesses to a protected system and protected resources

SECURING EMAIL COMMUNICATIONS

Email communication has long been a preferred form of communication in a professional environment. While emails are very convenient to use, they are also vulnerable to security threats. You can easily be caught unaware by an email threat which can cause damage to your system and data. All employees need to be made aware of the basics of email security and how one can handle the situation in case of a threat.

Steps to be followed for secure email communications:

- ***Encryption and authentication of emails are critical -*** end to end email encryption is a good practice which will help to keep your confidential information safe. Without encryption, emails are vulnerable to malicious attack.
- ***Educate employees*** - people are often the weakest link in cybersecurity threats. With the rise of people using their own devices at the workplace, security threats have become more rampant in the recent times. Educating employees on the proper usage of their systems and the content being consumed from the internet is essential. Critical information to be shared with the employees on a regular basis include identifying security challenges and the methods on how to be secure.
- ***Be aware*** of the information being shared by oneself on social media platforms.
- ***Avoid using company email*** for personal messages
- ***Secure Devices*** - Ensure that the devices being used on the office network are properly secured with the appropriate security measures
- ***Downloading Awareness*** - Downloading information from unknown sources must be avoided at all costs
- ***Keep updated on Software*** - Make sure to update the security software on your system regularly
- ***Password Lock*** - Keep your systems on password lock

INFORMATION SECURITY MANAGEMENT SYSTEM

An information security management system (ISMS) is a set of procedures and policies as per Information Security Management Standards, implemented to manage and control a company's sensitive data. The objective of ISMS is to control

security breaches and keep risks at a minimum for an organization. Cybersecurity in today's day and age has become a challenge and priority for a majority of the companies. Your data is not any safer, and companies would like to take every measure possible to protect the same.

Benefits of implementing an ISMS -

- System security is not just anti-virus software. The ISMS include people, IT systems & tools and processes thereby making the setup as secure as possible
- Helps to coordinate all security efforts (electronic and physical)
- Provides a systematic approach to managing risks and to make better-informed decisions on security
- Regular updating of the systems minimizes threats to sensitive information
- Improves the credibility of your organization

ACCESS CONTROL

Access control is the authority which checks for what a particular user is allowed to see and use.

The key questions to be answered are:

- Who is allowed to access your company's data?
- How do you authenticate a person's access control?
- Under what circumstances do you deny access to a particular user?

The two main components of access control are:

Authorization and Authentication go hand-in-hand with each other as components of access control.

- ***Authentication***: Used to verify if the user is who he or she claims to be. But this is not sufficient and needs authorization as well.
- ***Authorization***: Another layer of authorization is required, which decided whether the user should be allowed that access. Any organization today which connects to the internet needs to have authenticated access control in place.

A well-defined access control policy of the organization will have:

- ***Attribute-based access control (ABAC)*:** Access rights are granted to users through the use of policies which combine attributes such as user attributes, resource attributes, object, environmental attributes, and more). The ABAC supports the Boolean logic and contains if, then statements in the coding logic.
- ***Discretionary access control (DAC)*:** A control that grants or restricts the access to objects based on the owner and the identity of subjects and groups to which they belong. DAC access controls are defined by user identification with supplied credentials during authentication, such as username and password.
- ***History-based access control*:** Access Rights are granted based on programs' past security-sensitive actions.
- ***Identity-based access control*:** Access rights are simply given to a user based on if their name appears on the ACL (access control list)
- ***Mandatory access control*:** This is the strictest of all levels of controls and rights are assigned to a user based on regulations by a central authority including requirements from both industry and government.
- ***Role-based access control (RBAC)*:** This is also known as Non-Discretionary Access Control and takes more of a real-world approach that is based on a user's job function within the organization to which the computer system belongs.
- ***Rule-based access control (RBAC)*:** Users are allowed or denied access to resource objects based on a set of rules defined by a system administrator and access properties are stored in the ACL.

Challenges in implementing access control:

- ***The need for persistent policies*** - the variety of devices/ mediums used in today's world makes it difficult to enforce security policies
- ***Selecting the appropriate access control model*** - depends on the sensitivity of the information
- ***Authorization*** - an area of concern for several organizations
- ***Ongoing Adaptability Challenges*:** Access control policies must be capable of changing dynamically with the changing environment

TIPS FOR HELPING EMPLOYEES UNDERSTAND CYBER RISK AND BEST PRACTICES

1. ***Perform "Live Fire" Training Exercises*** – the best preparation is subjecting the users to a simulated attack specific to their job because people learn best by doing and performing. The internal cyber security team at your organization or an outside vendor could orchestrate a simulated attack to test the rigorousness of the company's security and to test the reaction of the employees when a security and data breach is presented. The live fire training exercise will not be announced to the employees because the IT team would regularly perform the exercises, including performing regular phishing tests, in which the IT team sends out a fake phishing email to all employees across the organization, and gauge how many people click on it. Then they can break the data down by departments and types of messages to tailor training to problem areas. It also allows the company to show progression. After the orchestrated security live fire

training exercises, employees are asked to understand the lessons they've learned from that attack, and the implications on the business, on their personal lives, and how they could have prevented it.

2. ***Get Buy-In from the Top*** – Having a good cyber plan includes investing in quality people, hardware, software, and training year after year, so that means getting the CFO, CIO, and CEO on board.
3. ***Start Cyber Awareness During the Onboarding Process*** – When employees step through the door of your corporation for the first time, start building the mindset that security awareness is important and that there will be continuous training. Establishing good habits and business practices from the very beginning will go a long way into unifying all employees towards a common goal to ensure that everyone is on the same page.
4. ***Conduct Evaluations –*** Conduct independent evaluations on both the employees and the systems to identify and unveil trends, loopholes, and vulnerabilities and to evaluate the readiness of your corporation to react and deal with a real attack. This baseline evaluation will help determine how prepared or how good or bad your security systems and employees are to the real deal when it happens. It's better to catch vulnerabilities during evaluations and correct them than to find out later that your vulnerabilities lead to compromised systems.
5. ***Communicate*** – Create a plan of execution to communicate and train all employees and personnel about cybersecurity and make sure everyone is on the same playing field. Create certifications and measurable training in all departments to learn best practices to create alignment for benchmark practices and goals.
6. ***Create a Formal Plan*** – The IT Cyber Security Team should ideally develop a documented plan for cybersecurity training that is updated often with the latest information on attack vectors and other risks. Having a plan that is put in the back burner and not updated often will prove useless over time as those vectors will become outdated and pose a potential weak spot for cybersecurity attacks. The Cyber Security Team needs to be robust in its ongoing education and keep up to date with practices, threats, news, and ultimately to train the organization on the same material.
7. ***Appoint Cyber Security Culture Advocates*** – A robust security department and personnel ready to dynamically respond to the latest security threats require strong leadership and advocates. The CISO is the Chief Information Security Officer, a senior-level executive within an organization responsible for establishing and maintaining the enterprise vision, strategy, and program to ensure information assets and technologies are adequately protected. To ensure a successful cybersecurity plan execution, the CISO should appoint a cybersecurity culture advocate in every department. These advocates can act as an extension of the CISO and keep employees trained and motivated. Keeping a robust security plan is a big job and hard work, so it is not a one-person job or just the job of the IT department. Thus, appointing advocate leaders in each department is a key important part of the success plan.
8. ***Offer Continuous Training*** – Cyber Security Training should not be just a once a year annual training but should continue throughout the year. Plus, whenever new changes, news of new threats or other vulnerabilities are available, it should be communicated and made available to all departments and personnel immediately. The type of training will vary and customized for the type of department or user. For example, end users should have training associated with the types of attacks that you might receive including attacks on your email or attacks that are oriented on the type of job you hold. If you are in IT, the attacks may be more technical so that training will address more technical aspects.
9. ***Stress the Importance of Security at Work and Home*** – With the availability of the internet, mobile devices, computers and other technological devices like Apple Watches, FitBits, talking GPS systems, and other devices including baby monitors, we are connected to the world more conveniently. But with that convenience of being connected to the world all the time, security threats don't stop at just the workplace, they extend into part of your life 24 hours a day, seven days a week, and 365 days a year. Teach users about spoof emails, privacy, security, and how the lessons learned at work can apply at home and in their personal lives to give them a "what's in it for me" attitude so that they apply it all the time, not just at work. Only then when people realize that they are in constant danger of security breaches, will they understand the crucial role that they play in keeping themselves and their organization safe. When people let down their guard, ignore warning signs, make assumptions without clear reasoning, they risk security vulnerabilities. Sometimes, it only takes turning off the antivirus for a split second to have a virus, trojan, or security attack to begin. When in doubt, employees need to be trained to ask for help when they are not sure of the answer or what to do.
10. ***Reward Employees –*** Reward users that find malicious emails or share stories about how users helped thwart security issues. IT leaders should empathize with employees that make mistakes and accidentally clicking on a potentially harmful email. Employees need to understand that their company will stand behind them and learn that telling personnel will not result in "getting in trouble." Often, if employees feel that they are reprimanded severely, they might hold back the fact that they should have told an IT security official that there was a potential security breach. Time is of the essence, and the sooner the situation is reported, the sooner a patch or resolution is put into place. Employees need to understand the importance of reporting the first sign of security breach suspicion and to be rewarded for this. This will go a long way into building a successful, secure company.

While these training tips can be helpful, education and training is not a perfect solution. Even in the most advanced and most current education scenarios, there still are a percentage of attacks that will get through and could be anywhere from 4-6 percent success rate, even after all the training is done. So, training is only one aspect of defending the environment from advanced attacks. Remember your systems also need to remain robust and updated with the latest security policies and software.

REFERENCES

- Wikipedia