CYBER SECURITY

ESSENTIALS

Aan Systems, Inc

Table of Contents

Chapter 5: Dealing with Cyber Security Threats aan

Chapter 8: The Future of Cyber Security aan

Chapter 9: Glossary of Terms aan

Don't put Yourself in this Situation!
Introducing Cyber Security Essentials from Aan Systems, Inc.
aan
Prevent Cyber Crime with the Right Training for Your Employees.
aan

CHAPTER 1: INTRODUCTION TO CYBER SECURITY

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 due to the fact that 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 literally 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 major 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 a vastly greater computing power in the same-sized machine, 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 short 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 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 a period of 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 a 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 Millenial (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 websites and the data they contain remain safe and secure is the job of cyber security 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 smart phones to tract 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.

Yet, 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 have to 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 AK-47s, 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 at 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. Software can be designed from the ground up with security as a 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. Oftentimes, 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 oftentimes 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 in order 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

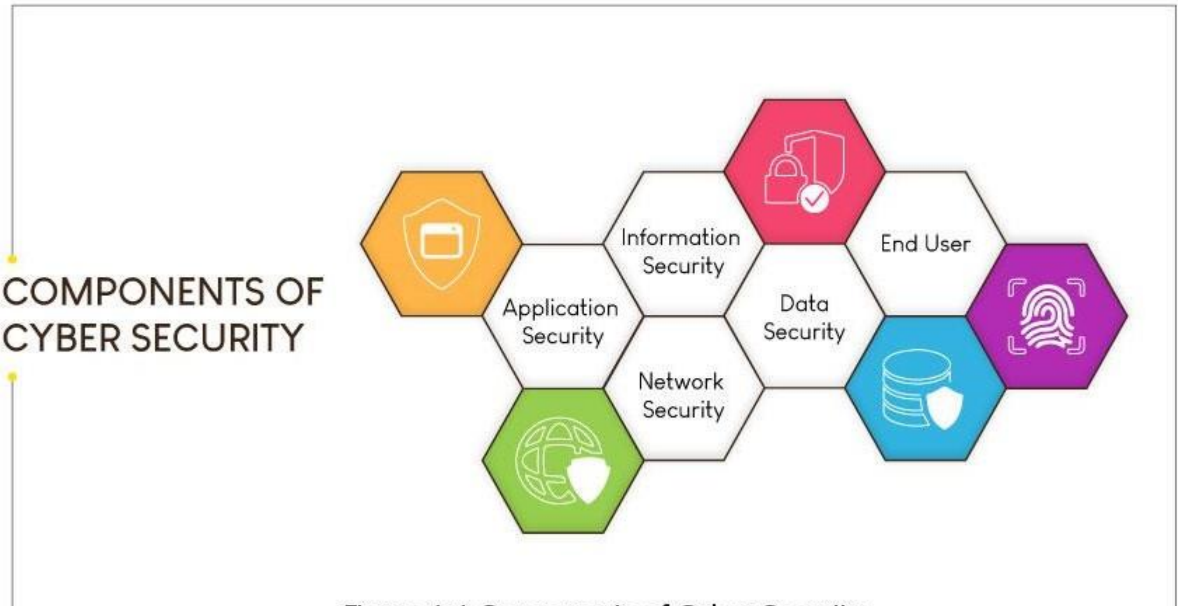


Figure 1.1 Components of Cyber Security

Application Security

An Application is a program or a set of programs that is developed for end users. This application carries the risk or vulnerabilities of attack when installed 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 relates 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 logon 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, smart phones, 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 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 in 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 increase in BYOD (Bring Your Own Device), it is more important to educate employees about staying safe from cyberattacks. On one hand, BYOD has provided flexibility to users and on the other hand, it has also given rise to 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 cyber security to stay updated on the latest information.

SOCIAL MEDIA SECURITY

With rampant usage 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 is 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 at the workplace.

CONCEPT OF CYBER SECURITY

Cyber security 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 an enterprise security.

Results are described in the theory and used in the model with respect to **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 cyber security 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 to 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 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 alerts 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 CYBERATTACKS

In recent times, we notice that cyberattacks 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, having the knowledge to identify the new methods by which cyberattacks are taking place is a key step to preventing and stopping cyberattacks.

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 an added bonus, canarytokens.org gives the user a bunch of hints and tools that increases 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 in 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 in order 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 cyberattacks and keep antivirus software up to date. During a cyberattack, the malicious malware software is designed to infiltrate and attack your computer. These 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 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 regularly check for and apply available updates. Software updates might seem unnecessary or annoying but actually 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 prime good example of a cyberattack 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 actually 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 a SSIDs, 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 because the encryption algorithm incorporates the SSID, and password cracking manuals used by hackers are preloaded with common and default SSIDs. Using just the default SSID just 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 cyberattacks, so every business needs to have a proper measure for 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 really 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

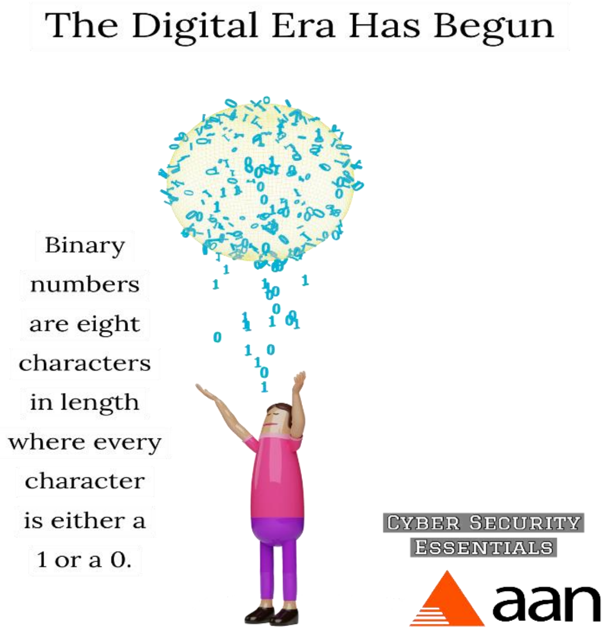
If we look at security breaches over the last five to seven years, it's pretty clear that people, whether it's through accidental or intentional introduction of malware, represent the single most important point of failure in terms of security vulnerabilities. In the past, companies used to rollout an 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 cyber security 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 original 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


The Digital Era Has Begun
Binary numbers are eight characters in length where every character is either a 1 or a 0.
CYBER SECURITY ESSENTIALS
aan

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. Cyber security 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 at 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 has 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 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 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 in 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 own account is usually the first step for using a social media platform. You can use your account to login to the platform and further interact with others.

2. **Profile pages** - A profile page is your individual 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 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 together in the same area, which are all owned by the same company.

Networking Types and Structures

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

Wired Networks:

Pros:

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

Wireless Networks:

Pros:

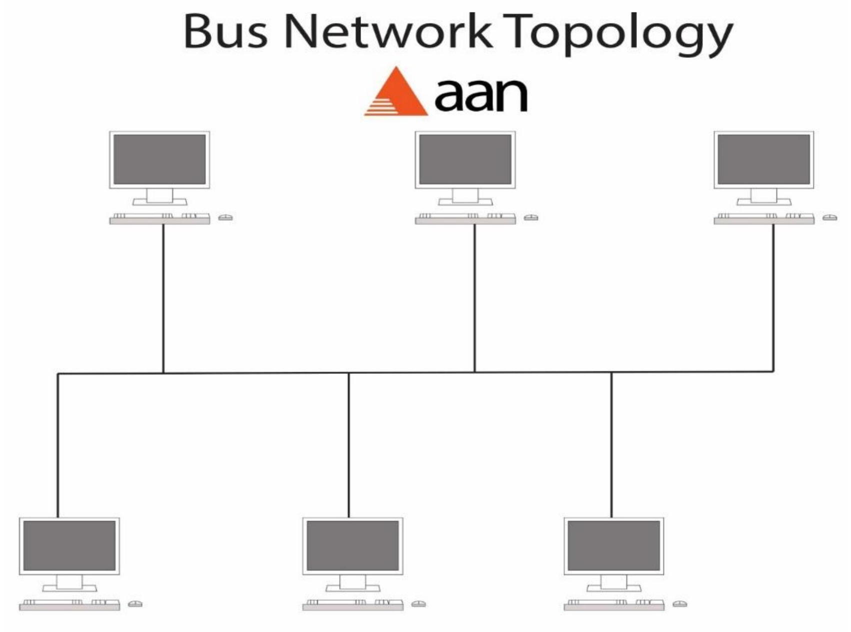
- ✓ Easy to setup
- ✓ Can be accessed across multiple devices
- ✓ No cable required
- ✓ Can be used on home and public networks
- ✓ Allows remote access management

Networking Topologies and Layout

Network nodes can be connected in many different 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.

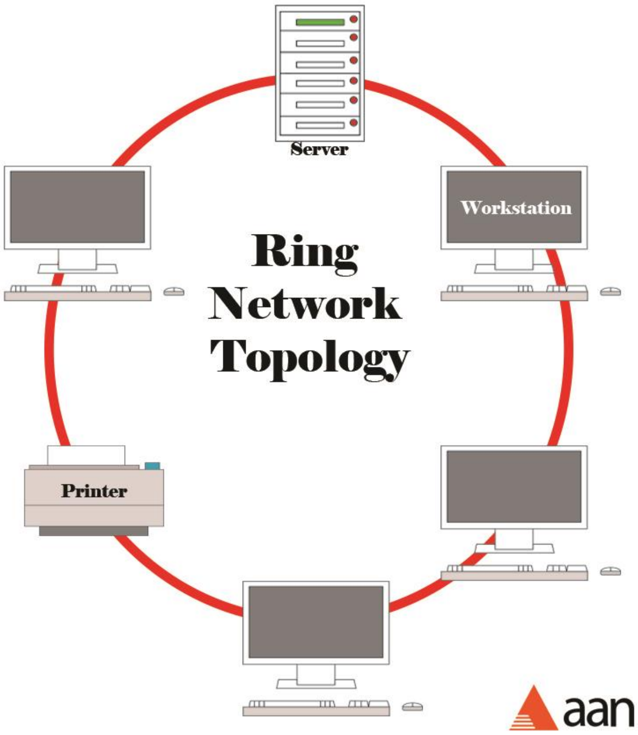
1. **Bus Network:** A network topology in which nodes are directly connected to a common linear (or branched) half-duplex link.

Figure 2.1: Bus Network Topology



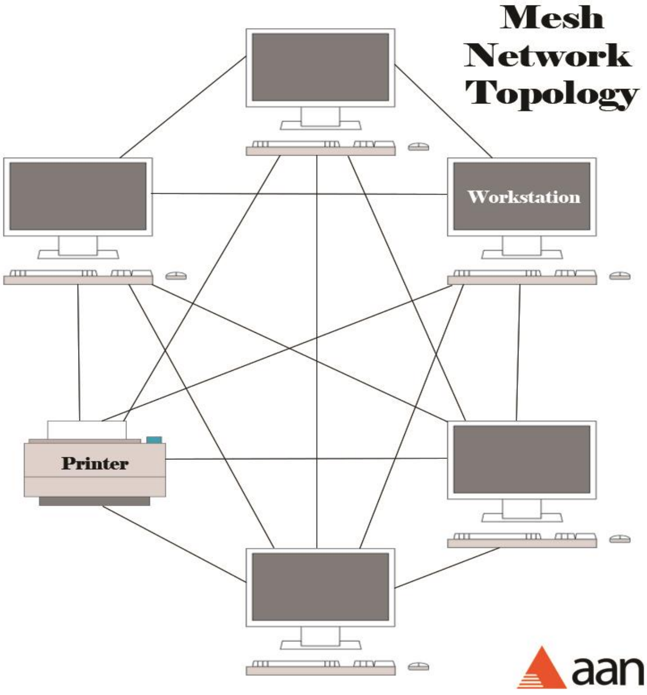
2. **Ring Network Topology:** A network topology in which each node connects to exactly two other nodes, forming a single continuous ring pathway for signals through each node. Data travels from node to node, with each node along the way handling every packet.

Figure 2.2: Ring Network Topology



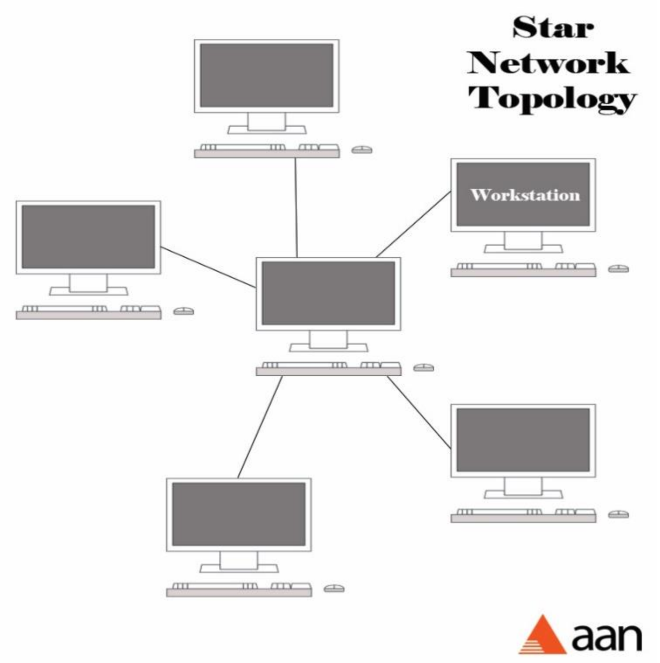
3. **Mesh Network Topology**: A mesh network is a local network topology which the infrastructure nodes such as bridges, switches, and other infrastructure devices are interconnected with one another directly, dynamically and non-hierarchically to as many other nodes as possible and cooperate with one 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



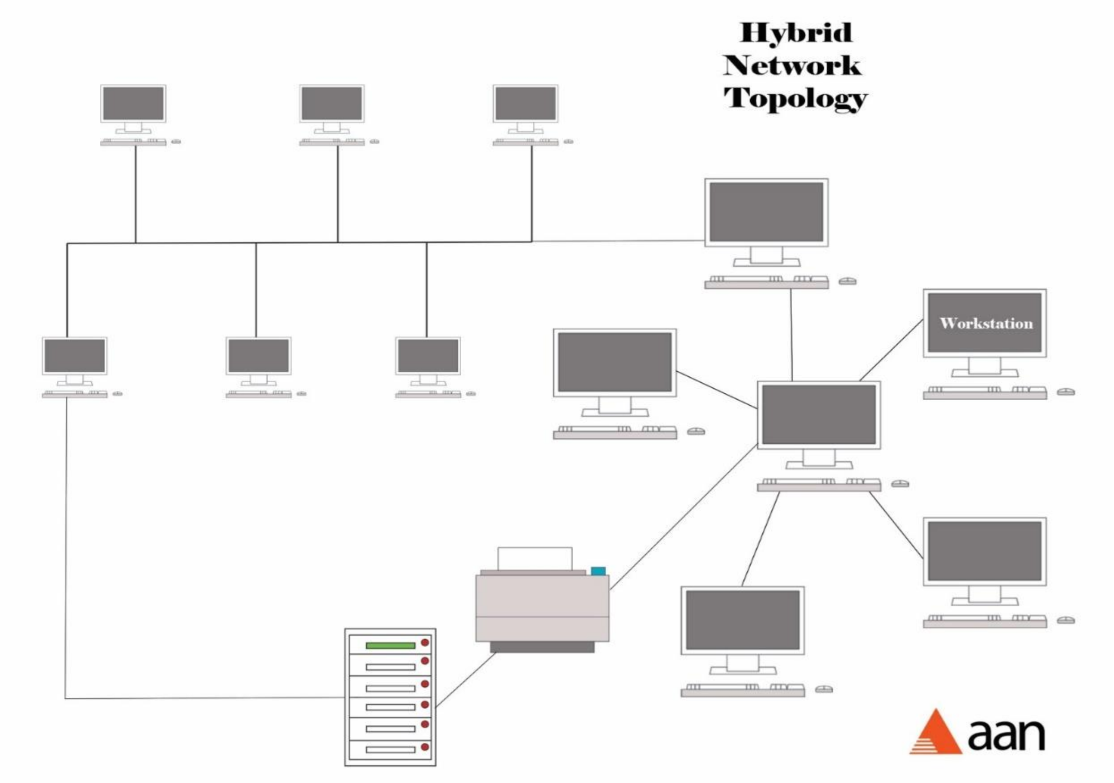
4. **Star Network Topology:** The star topology or star network, is one of the most common computer network topologies and visually looks like a formation of a star. In its simplest form, the star topology is a network topology where each individual device host in the network is attached to a central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

Figure 2.4: Star Network Topology



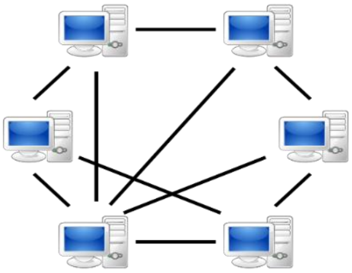
5. **Hybrid Network Topology:** A topology that is a combinational mixture of two or more different basic network topologies interconnected together to allow more functionality of combined features. The advantages of hybrid network topologies include increased reliability, scalability, flexibility, and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

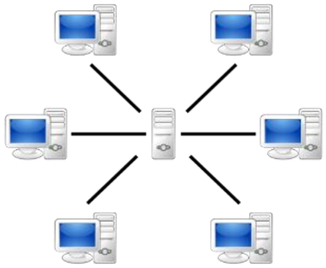


Pros -

- ✓ 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 on the basis of 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 loss in 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 at 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 team work
- **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 own graphic design using ready-made templates. For example, you can create your own 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 the technique used to store and retrieve data. Access methods are identified primarily by the data set organization. Access methods have their own data set 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 - 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 addressing.

DEVICE PROTECTION

Your end users are connected to the World Wide Web in a number of different ways.

Methods to Connect to the Internet:

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

These are all potential doorways through which a cyber criminal could access your company's infrastructure and cause serious harm. Having devices stolen isn't the only way these can be compromised though. This is why 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 in 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. This is why 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 displaying 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 touch screen 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 a 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 labelling, you are at a 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 to 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 is 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 cyber security 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. Cyber security in today's day and age has become a challenge and priority for a majority of the companies. Your data is not any more safer and companies would like to take every measure possible to protect the same.

Benefits of implementing an ISMS -

- System security is not just an 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 together such as user attributes, resource attributes, object, environmental attributes, and more). The ABAC supports the Boolean logic and contain 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/or 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 bases 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 clearly communicate and train all employees and personnel about cyber security 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 clearly 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 cyber security 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 requires 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. In order to ensure successful cyber security 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-man 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 in nature, so training will address more technical aspects.
9. **Stress the Importance of Security at Work and at 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 work place, they extend into part of your life 24 hours a day, 7 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". Oftentimes, 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.

CHAPTER 3: CYBER SECURITY

- Introduction to Cyber Security
- Understanding Internet governance
- Identity and authentication on the Internet
- What do we mean by security?
- What are cyber threats?
- What are the vulnerabilities?
- Building trust in cyberspace
- What is an advanced persistent threat?
- Basics of computer defense
- Who is the weakest link?
- Why security awareness for end users is so important – a close look at phishing.
- Security awareness to protect against phishing
- A realistic approach to training employees
- What cyber security policies should include
- The Principle of Data Collection

INTRODUCTION TO CYBER SECURITY

“It’s not a truck, it’s a series of tubes”.

This is how a senator from Alaska had famously described the cyber space at a congressional hearing. At the time, the senator was mocked for calling cyber space a series of tubes, whereas in fact it is rather difficult to define ideas in terms of cyber space. “Tubes” is actually a mangling of the idea of “pipes,” an analogy that is used by experts in the field to describe data connections.

Part of why cyber space is difficult to describe and understand today is because of its global and expansive nature. The cyber space has changed drastically and also almost unrecognizable in comparison to its humble beginnings. The US Department of Defense can be considered the god - father of cyberspace, referring back to its funding of early computing and original networks like ARPANET.

There have been several definitions for cyber space over the years, but at its essence, cyber space is a realm of computer networks and the users behind them in which information is stored, shared and communicated online.

Cyberspace is first and foremost an information environment. It is made up of digitized data that is created, stored, and, most importantly, shared. But cyberspace isn’t only virtual. It consists of computers that store data plus the systems and infrastructure that allow it to flow. This includes the Internet of networked computers, closed intranets, mobile technologies, fiber-optic cables, and space-based communications.

Cyberspace is constantly evolving. Since humans and technology use the cyberspace, as there are changes to both these factors, the cyberspace also changes drastically. It may have initially started off as being just a communication realm, but today with the rise of e-commerce and other uses of the Internet, cyberspace has gone on to become ‘critical infrastructure’. Cyberspace has almost now become ‘the dominant platform for life in the 21st century’. But the Internet we have all grown to become so dependent on for various purposes is increasingly coming under danger.

UNDERSTANDING INTERNET GOVERNANCE

In 1998, Jon Postel, a respected computer researcher and leader sent an email to eight people. He asked them to reconfigure their servers so that they would direct their Internet traffic using his computer at the University of Southern California rather than a computer in Herndon, Virginia. These eight people did as they were told without asking any questions. This switch made by Postel was done so without any permission. Basically, he did this to prove to the then US Government that the Internet cannot be controlled as they please and take away control from the wide set of researchers who had worked on it.

Postel's little experiment for the very first time exposed that the Internet has governance issues. Eric Schmidt later made a statement saying "The Internet is the first thing that humanity has built that humanity doesn't understand, the largest experiment in anarchy that we have ever had." Since digital resources are not scarce as traditional ones, its governance also will be done differently.

IETF (Internet Engineering Task Force)

The operations of the Internet require independent actors to follow basic rules that guarantee interoperability, known as standards. This standards-based approach traces back to the beginning of the Internet. Eventually IETF (Internet Engineering Task Force) was developed that is a set of new Internet standards and protocols and modifies the existing ones for better performance. Everything developed by the IETF falls under specific working groups that concentrate on areas like routing, applications, and infrastructure.

Openness is critical to the culture of IETF. In some working group meetings, the members decide on an issue by humming for or against a proposal. While the IETF has no official board or formal leadership, the Internet Engineering Steering Group (IESG) offers oversight and guidance for both the standards process and the standards themselves.

The Internet Society (ISOC)

The Internet Society (ISOC) is an international group that formed in 1992, which oversees most of the technical standards and processes. The ISOC was setup as an independent, international organization to provide a formal, legal means to safeguard the independent and open standards processes. With all these informal and semi-formal groups floating around, there was still a shadow in Internet governance and safety.

Internet Corporation for Assigned Names and Numbers (ICAAN)

The growing pressure for commercial Internet lead to the fact that the US government cannot govern Internet. Soon ICANN (Internet Corporation for Assigned Names and Numbers) was born. ICANN put in place a more structured way to distribute IP addresses that more reflected on the Internet's global nature. Despite efforts to globalize Internet governance, many still see ICANN as captive to US interests. With no other alternative right now, we can't really criticize ICANN.

With all these various governance issues, it's safe to say that the Internet has always defied traditional governance models.

IDENTITY AND AUTHENTICATION ON THE INTERNET

It is essential to separate identification from authentication. Authentication acts as proof of identification.

Identification

Identification is the ability to identify uniquely a user of a system or an application that is running in the system.

Authentication

Authentication is the ability to prove that a user or application is genuinely who that person or what that application claims to be.

- **Examples of Authentication and Identification**
  For instance, bank ATMs have cards for identification, whereas in recent times, the mobile phone acts as an authenticator. One-time codes received on the registered mobile phone acts as authenticator for the particular financial transaction.

Authorization

After authentication comes authorization. What can be done after the system you are using has identified you. Obtaining authorization can open doors to more opportunities. Authorization is the part that links these technical issues to policy, business, and political and moral questions.

Digital Identity

Digital identity is a balance between protecting and sharing information for the purpose of cyber security. Limiting access of acquired information gives rise to privacy of that particular information, plus it prevents more sophisticated fraud.

WHAT DO WE MEAN BY SECURITY?

In the earlier days of the computer, there was a joke going around on the security perspective as to how one can keep the data on the computer safe. 'Just unplug it'! By keeping the system unplugged it was believed it can be kept safe. But jokes aside, we do know that today with wireless and rechargeable devices, once a machine is plugged in, it can always deviate from its intended purpose.

Security is not just a thought of being free from threat, but it is also the presence of an adversary. A cyber problem becomes a cyber security issue if the adversary seeks some information from the activity, thereby making it a data breach.

In the digital world, protecting information is of huge importance. Privacy is an important factor and sensitive data and classified data must be kept confidential. In case of a data breach, the adversary gaining the information can get a lot of information that can put the user at risk. Keeping data confidential can be done through tools such as encryption and access control.

Integrity

Integrity is a critical factor in data security. Integrity, in terms of cybersecurity means that the system and the data it contains have not been improperly changed without authorization. A user needs to have confidence in the system that it will behave as expected and be available when required.

Integrity is a very subtle factor in security because it is challenging to realize if the system is behaving in the manner expected. An attacker can disable a system and make it inaccessible for a user.

Security costs money, but it also costs time, convenience, capabilities, liberties, and so on. All of these aspects of security are not just technical issues: they are organizational, legal, economic, and social as well. But most importantly, when we think of security we need to recognize its limits.

WHAT ARE CYBER THREATS?

Cyberattacks in 2017 alone have caused a damage worth about $5 billion. This is only set to increase in the coming years with cybercrime damage expected to hit $6 trillion annually by 2021.

Cyber Threat

A cyber threat is a malignant and destructive act that tries to gain access to one's system or data without authorization. A cyber threat takes place through the computer network. Cyberattacks are carried out by people termed as 'hackers' who gain unauthorized access to your system thereby stealing sensitive important data and cause harm to your system.

Listed below are some of the common cyber threats taking place today -

1. **Advanced Persistent Threats (APT) –** An APT attack is a network attack in which an unauthorized person gains access to a network and stays there undetected for a long period of time for the purpose of stealing data.

2. **Email Malware –** Email Malware is also known as email spam and spreads unwanted and unsolicited email and is often started and solicited through links in the messages that leads to phishing websites and other sites that host malware. Email Malware can act as an agent that allows attackers to attack other computers through your computer. Email malware comes in many forms but essentially can steal data from your computer such as bank logins, passwords, or files and can detrimentally take full remote control of your computer.

   Here are some of the flavours of email malware:

   a. **Ransomware** – Encrypts the victims data and demands a fee to restore it.

   b. **Phishing** – Uses authentic looking senders with a socially engineered message to coax the victims to release sensitive data.

   c. **Spear Phishing** – Targeted phishing attempts for a specific organization where cybercriminals prepare extensive prior research to appear authentic and legitimate.

   d. **Spoofing** – Hackers use addresses and domains that are similar to legitimate ones to deceive victims into believing fraudulent emails are from a trusted individual.

   e. **Man-in-the-Middle Attacks** – Cybercriminals insert themselves between the user and the application, website or service that the victim is using and enables the attacker to impersonate the victim, steal valuable personal information and read, manipulate and send emails without the victim's knowledge. Cybercriminals can even modify or conduct transactions with this type of tactic.

   f. **Whaling/Business Email Compromise (BEC)** – The term whaling is used to indicate the that cybercriminals target the largest fish in the organization who has the decision-making power to carry out financial transactions. These emails look like they come from the CEO or other higher management and requests immediate financial transactions such as direct deposits, wire transfers, or vendor payments or purchases.

   g. **Spam –** Spam email often contains malware and dangerous malicious content.

   h. **Key Loggers –** Key loggers are often obtained when cybercriminals send victims a malicious email and they inadvertently click on the malicious attachment or link causing a stolen user credential or identity.

   i. **Zero-Day Exploits –** A cyberattack that occurs the same day a security weakness is discovered in software and is exploited before a patch or fix is available. This type of exploit is often delivered via malicious email to help them gain authorization and ultimately to steal sensitive information.

   j. **Social Engineering –** Cybercriminals impersonate trusted individuals to build up trust and engage in conversation to gain access to a company's network.

3. **Trojans –** A type of malware that is often disguised as legitimate software to help cybercriminals gain access to users' systems. This is often used in conjunction with social engineering to trick users into loading Trojans into their systems.

4. **Botnets** – A network of interconnected private computers or devices that are infected with malicious software and controlled and coordinated as a group without the owner's knowledge so that the cybercriminals can access the network to perform malicious activities such as stealing data, sending spam, and performing DDoS (distributed denial-of-service attack), just to name a few.

5. **Ransomware** – Ransomware is a common and dangerous cyber security threat wherein a user is denied access to their system or a website, and access can only be regained after paying a certain

amount of money as ransom to unlock the system. In general, ransomware is a form of malicious software or malware that prevents you access to your data unless you forgo some sort of ransom fee via an untraceable bitcoin payment for the cybercriminal to restore your access to the data. One of the common delivery systems of ransomware is phishing email spam attachments that are disguised as trusted files. A common type of ransomware is often to encrypt some or all of the user's files and can only be decrypted by a mathematical key known only by the attacker.

   a. **Leakware or doxware:** A less common variant of ransomware where the attacker threatens to publicize sensitive data on the victim's hard drive unless a ransom is paid. However, this tactic is usually only used a threat as finding and extracting information is tricky for attackers so encryption ransomware is the most common form.

6. **Distributed Denial of Service (DDoS):** A DDoS is when multiple compromised computer systems attack a target, such as a server, website or other network resource causing a denial of service for users of the target resource.

7. **Wiper Malware Attacks:** A wiper malware is intended to wipe the hard drive of the computer it infects.

8. **Intellectual Property Theft (IP theft):** Intellectual property theft is stealing of trade secrets, trademarked materials, designs or ideas as well as copyrighted materials such as music, drawings, or information.

9. **Theft of Money:** Stealing of Money

10. **Data Manipulation:** Some refer to this as the latest technique in the "art of war in cyberspace" where the cybercriminal alters digital documents and other information that could lead to disaster for corporations, health care organizations, the governmental agencies, and other individuals.

11. **Data Destruction:** Cybercriminals permanently destroy, erase, and wipe out the entire database of an entire corporation. They may do this by destroying data on hard drives, memory cards, smartphones, and other mobile devices. The worst cyberattack in history occurred in 2012 with the oil giant Saudi Aramco involving data destruction where the hard drives of more than 30,000 desktops and servers were attacked by malware and aimed to wipe out the entire IT infrastructure of Aramco.

12. **Spyware/Malware:** Malware are malicious software designed to cause damage to computers or networks. Spyware software monitors your computer and reveals collected information to the cybercriminal.

13. **Man-in-the-Middle (MITM):** A example of man-in-the-middle attacks is actively eavesdropping where the attacker secretly relays and possibly alters communication between parties who believe they are directly communication with each other.

14. **Drive-By Downloads:** Unintentional downloading of software sometimes caused by just opening up an infected website by visiting it (driving by). Drive-by Downloads can also exploit a browser, app or out-of-date operating systems that has a security vulnerability.

15. **Malvertising:** This involves online advertising to spread and interject malicious malware filled advertisements into legitimate online advertising networks and webpages.

16. **Rogue Software:** This is a malicious software that tricks the user into thinking that their system has malware or viruses on it and thus manipulates the victims into paying money for a fake malware or virus removal tool where it actually introduces malware into the computer.

17. **Unpatched Software:** Software that has vulnerabilities that cybercriminals can exploit.

18. **Social Engineered Malware (SEM):** An attack that tricks users into downloading and installing malicious software that compromises the security of their system.

Most Common Sources of Cyber Threats:

- Nation states or national governments
- Terrorists
- Industrial spies
- Organized crime groups
- Hacktivists and hackers
- Business competitors
- Disgruntled insiders

Types of Social Engineering Attacks:

- **Phishing:** Attackers use emails, social media, instant messages, and SMS to trick victims into providing sensitive information or in visiting malicious URLs for the purposes of compromising systems.
- **Watering Hole:** Injecting malicious code into public Web pages of a site that the targets normally visit. This type of attack is common for cyber espionage operations or state-sponsored attacks.
- **Whaling Attack:** The choice of targeted victims distinguishes this category of targets which happen to be relevant large executives of private business and government agencies, thus the use of the term whaling.
- **Pretexting:** The practice of presenting oneself as someone else (impersonation) to obtain private information. Oftentimes, attackers will create a fake identity, build up trust, and use it to manipulate victims to coax them for sensitive information.
- **Baiting:** This type of hacking exploits human curiosity and is characterized as the promise of a good deed. However, this is a launch point for which hackers use to deceive victims. An example is when attackers use a malicious file disguised as a software update or generic software.
- **Quid Pro Quo:** An iteration of the baiting attack and means “something for something”. The difference is instead of baiting the victim with the promise of a good, a quid pro quo attack promises a service or benefit based on the execution of a specific action. For example, the hacker offers a service or benefit in exchange for information or access. The most common one occurs when a hacker impersonates an IT staff of a large corporation and could be calling employees of the target company and offers them some kind of upgrade or software installation.
- **Tailgaiting:** This is also known as piggybacking where an attacker seeks entry into a restricted area that lacks proper authentication. A typical situation happens when an attacker simply walks behind a person who is authorized to access the area or impersonates a delivery driver or caretaker who is packed with parcels and asks the person to hold the door, evidently bypassing the electronic access controls.

What are the Vulnerabilities?

Security Vulnerability

A security vulnerability is a weakness in a product or system that attackers capitalize on and further compromise the system’s integrity, confidentiality and availability.

Three Main Goals of Vulnerability

Integrity, availability and confidentiality are the three main goals of security. If any of these is compromised, you have a security vulnerability. A single security vulnerability can consist of any one of these elements or all three of them.

1. **Integrity** - trustworthiness of a resource is termed as integrity. In a situation of a security breach, the attacker is trying to compromise this trust without authorization, thereby compromising on integrity.

2. **Confidentiality** - limiting access to information to only specific set of people is termed as confidentiality. An attacker will try to compromise this element by accessing information that he is not privy to.

3. **Availability** - the possibility to access a particular resource is termed as availability. When an attacker denies permission to access a particular resource, the availability has been compromised.

Common Security Vulnerabilities

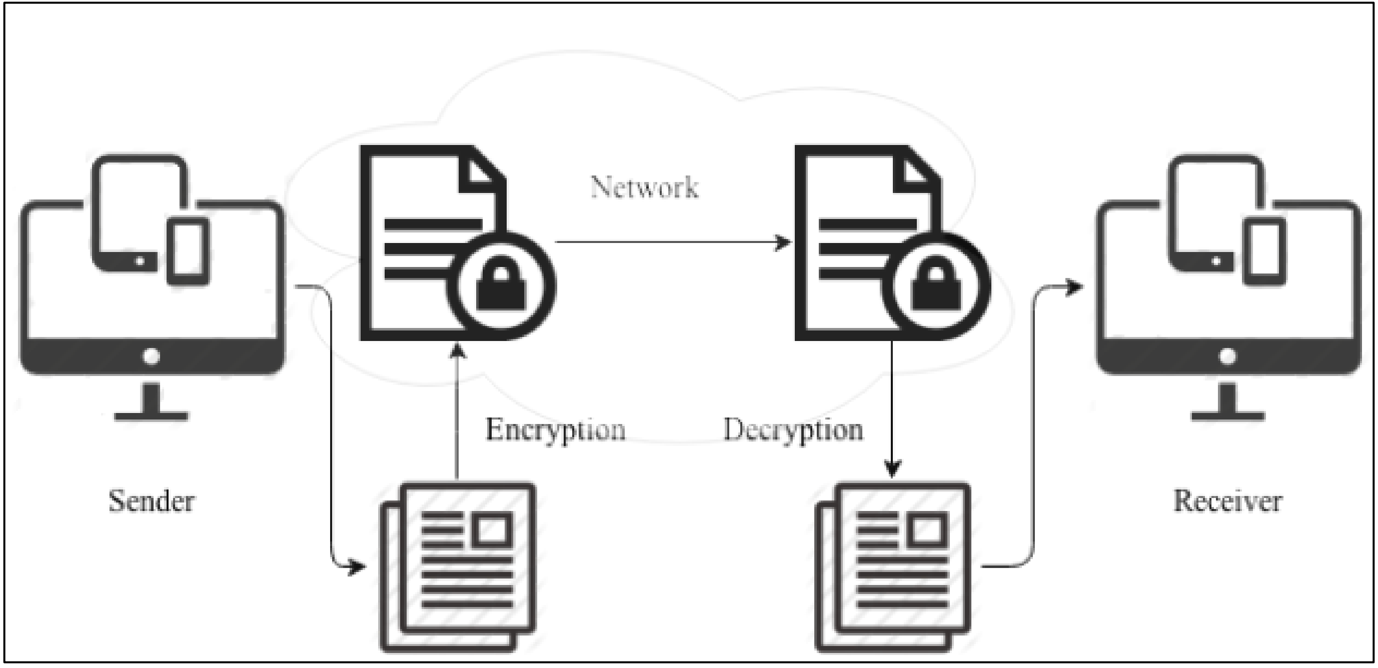
- **Injection** - includes all kinds of vulnerabilities where an application sends untrusted data to an interpreter
- **Broken authentication** - involves flaws that are caused by error in implementations of authentication and/or session management
- **Sensitive data exposure** - a flaw wherein an application allows easy access to sensitive data
- **Broken access control -** flaws including weak access control to applications which should not be allowed for all users
- **Security misconfiguration -** occurs due to poor configuration in a system making it more insecure and vulnerable to attack
- **Insufficient logging and monitoring -** lack of best practices that should be in place to check for security breaches

Building Trust in Cyberspace

With the continuous rise and rapid adoption of the digital world, online trust becomes a critical factor. For cyber security, the users must know how to trust the system and the system must know how to trust the users.

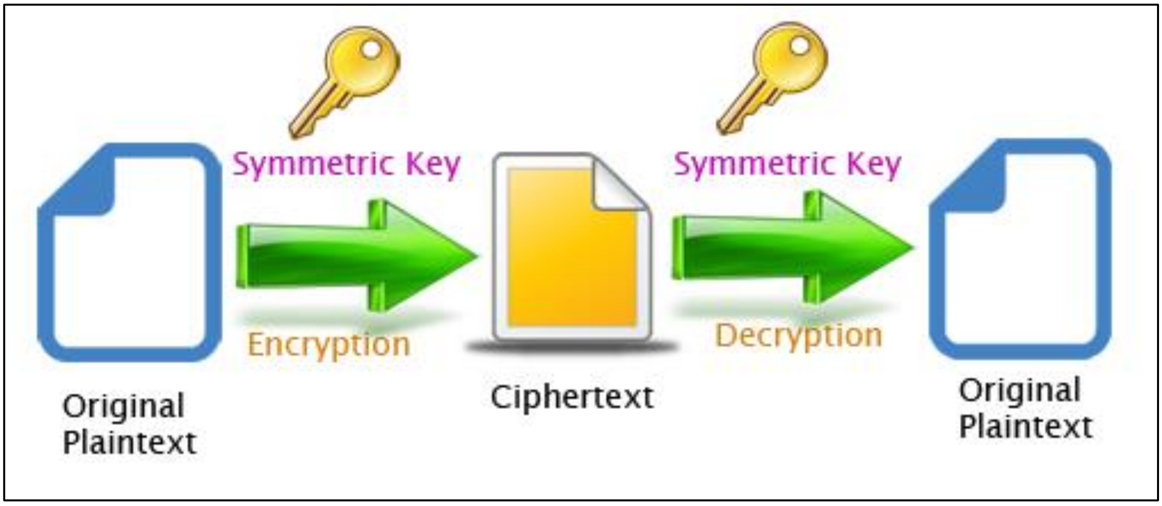
- **Online trust is built through cryptography -** The practice of secure communications that dates all the way back to the first codes that Julius Caesar and his generals used to keep their enemies from understanding their secret messages. Cryptography keeps information confidential and also has the ability to detect any tampering of data.

Figure 3.1: Process of Cryptography



Modern cryptography methods rely on 'keys' for the encryption and decryption process. Symmetric encryption relies on one single key that both end users trust for encryption and decryption.

Figure 3.2: Keys in Cryptography



A user can be authorized to use a system after identification and authentication is complete. Most systems use some kind of "access control" to determine who can do what. At its simplest, access control provides the ability to read, write, or execute code in an operating environment. Good access control policies are essential for any organization. Failure of access control systems has been one of the key reasons for some of the biggest cyber security scandals recently.

What is an Advanced Persistent Threat?

Advanced Persistent Threat (APT), is carried out by professional hackers whose full-time job is to carry out a specific hack on a company/ target. APTs work for either the government or relevant industries. These hackers carry out specific instructions given by their client for the hack.

These specific hacks include: accessing confidential information, placing destructive code, or placing hidden backdoor programs that allow them to sneak back into the target network or computer whenever they wish to.

A successful APT is one wherein the hacker breaks into the network and computer and takes the information needed and leaves unnoticed. APTs do not cause any drastic changes in the network for users to get suspicious.

Signs to look out for during an APT attack -

- **Increase in system log-ons at night** - APT hackers usually are in the opposite side of the world attempting a hack on a network on the other side of the globe. If you notice a spike in the log-ins on a network which is at night time and not in use, then it could be an APT.

- **Widespread backdoor Trojans** - APT hackers usually install a backdoor Trojan which will help them to get back into the system whenever they wish to.

- **Unexpected information flow** - Keep an eye out for unusual amounts of information being transferred from your network to an external system.

- **Unexpected data bundles** - look out for large chunks of data appearing suddenly in places where they aren't supposed to be

BASICS OF COMPUTER DEFENSE

The advantage of defending a computer system is that once you know what might attack you, you can just tell the computer what to watch for and how to avoid it. Traditional antivirus software relies on detecting these "signatures." The programs scan all files on the system as well as incoming traffic against a dictionary of known malware, looking for anything that matches these signatures of malice.

Modern antivirus doesn't just screen, they use "heuristic" detections to identify suspicious computer code behavior based on rules and logical analysis. Static analysis breaks apart the computer code and looks for patterns associated with the behavior of an attacker. Virtual machines and other sophisticated defenses dynamically simulate the code operation to determine whether the file examined will misbehave without putting the actual system at risk.

Firewall

The simplest form of network defense is a "firewall." Firewalls can prevent external computers from connecting to the firewalled machines except under pre-set circumstances or prevent certain applications on the computer from opening network connections.

"Intrusion detection systems" exist at the computer level or on the network. They detect attack signatures and identify anomalous behavior.

Air Gap

In cyber security terms, an air gap is a physical separation between the network and critical systems. Such practice is common with critical infrastructure, such as with power companies.

Who is the weakest link?

It's time to stop blaming employees and enlist their help. As the old saying goes, "people are the weakest link in the cybersecurity chain." Clearly, enterprise security professionals agree with this statement, as it turns out that 58% point to a "lack of user knowledge about cybersecurity risk" as being one of the highest factors most responsible for successful malware attacks. Therefore, end users must be part of the cybersecurity solutions and rigorous continuous training must be in place. When a user makes a mistake and clicks on an email that causes an infection, we often think that was the root cause. However, in actuality, the organization was already under attack when the attacker sent the email before it was opened. This proves that every other security control in the path of that attack had failed.

The real battle in cyber security is not just about high technology. It is also driven by the human factor, the fight over our behavior. It is for this reason that many IT experts believe that if a network has any kind of sensitive information in it, all users need to be regularly certified in cyber security basics. This means everyone, from junior staff all the way up the leadership. Build constant awareness, reinforcing it with new training. If users fail to learn the lessons of proper caution, then their access privileges should be revoked.

WHY SECURITY AWARENESS FOR END USERS IS SO IMPORTANT – A CLOSE LOOK AT PHISHING

If you could use one word to sum up why security awareness is so important for end users it would be: "phishing" because it is a very common attack for end users.

For those who are unaware of the term, the definition of phishing is any ploy to solicit sensitive information (i.e. passwords, social security numbers, etc.) by pretending to be an authority figure, trusted or familiar person.

Classic Examples of Phishing

A classic example would be when a person receives an email with their "new password" from an individual claiming to be from the IT department. When the recipient responds that they've complied and changed their password, the cybercriminal can strike and have access to that person's email address and can use it for all kinds of malicious or nefarious purposes.

Sadly, this is only one of the countless versions of phishing. Sometimes emails will come from banks or seller platform accounts like eBay or Amazon, claiming that you have violated a rule and that your account will be shut down, or that you have just bought this item, it looks authentic and because of the fear factor that comes out of thinking that your account will be shut down, users sometimes click on the email. Some have come in the form of examples like iTunes, or the most obvious to spot is the ones that claim you have won a lottery from a foreign land. For those that are well informed, they can easily spot these things, however, the cybercriminal is looking for weak victims and they will send out masses of these emails hoping that they can catch someone naïve and vulnerable, including the elderly and uninformed. Tactics used in conjunction with sending out phishing emails include scare tactics to get the person to check their account and click on links within the email. When in doubt never click on these emails at all. You can open up a new browser and log in yourself to check your account or balance. The emails should always address the person by name and business and will never ask for personally identifying information like birthdates or social security numbers on them.

To actually be a hacker takes an impressive degree of technical acumen and skill. With this technical knowledge and skill, many cybercriminals could find legitimate employment in just about anywhere in the IT field, but unfortunately, they take their skills and use them in crime.

The scariest element of a phishing attack is that anyone can do them and they can be absolutely brutal in terms of fallout consequences. On the other hand, all it takes is an email address, or just a phone number and a weak moral character to be successful with phishing. Phishing is a numbers game that usually favors the criminal, so even if the cybercriminal is unsuccessful at first, they have a number of employees to attempt their scheme.

Long Term Effects of Phishing

Phishing can bring on long-term effects and damage down the organization and the damage my go unnoticed for a long time. Accessing a low-level employee's email inbox may not seem like it would have such dire implications, but at least for some time, the criminal will be able to impersonate their victim, which could lead to gaining plenty of sensitive information.

Spear fishing – this type of spear phishing attack is a far more precise and sophisticated ploy and takes far more research on behalf of the criminal to impersonate someone specifically. Thus, cybercriminals need to figure out certain details about the victim to make this possible. They will do intensive frontend research on the victim. Therefore, they may go through the target victim's Facebook, LinkedIn, and other online social media profiles to ensure that they come across as believable as possible.

Security Awareness to Protect Against Phishing

The truly frustrating thing about phishing attacks is that they should be so easy to protect against, but because of carelessness, letting down one's guard, and ignorance, thousands of people fall victim every day. Always make sure you know who is sending you an email and if they ask for anything even remotely suspicious, call them to make sure they are indeed the ones who sent the message. This may seem trivial, or might seem unnecessary, but you'd rather be safe than sorry. It only takes a minute to call to verify rather than spending countless hours, headaches, and potential damages to your entire corporation just because this could have been avoided by stepping back to think about the situation. So, the rule is: Think before you click! And practice this every day, at work and at home!

The first step is awareness. Your entire organization needs to understand what phishing scams involve and what to look for so they are not fooled.

Make sure that personnel understand the consequences of falling for such a scheme. Again, phishing can lead to all kinds of bigger problems. The idea is to get your people to take these sorts of attacks seriously. If they don't, your corporation will become a victim.

Encourage people to come forward when they think they have been targeted. No one should ever feel embarrassed for coming forth with a report of breaches or suspicion. Time is of the essence, the more time that passes after a suspicious attack has been suspected, the more time the cybercriminal has time to do detrimental things that could lead to long lasting consequences.

Schedule regular calendar events, activities, programs and reminders that phishing is a threat so your staff is intimately aware of it.

Factors Contributing to Successful Phishing Attacks:

These attacks only work when people

1. Let down their guard
2. Assume something is safe without verifying the source
3. Are careless
4. Ignorant and uninformed people, and
5. People are not being vigilant.

Figure 3.3: Think Before You Click

1) Make sure you know who sent the email.
2) When in doubt call them to verify they sent the message.
3) Don't let down your guard & assume something is safe - Verify, Verify, Verify
aan
PHISHING VICTIM
THINK BEFORE YOU CLICK!

A REALISTIC APPROACH TO TRAINING EMPLOYEES

So, we know that humans are the weakest link but what can we do? Here are some tips for a realistic approach to training employees.

1. **Awareness Programs** – these include basic training combined with ongoing awareness campaigns. Successful awareness campaigns combine education, communications, cheerleading, entertainment, and perhaps some incentives.

2. **Leadership** – The CISO may be responsible for cybersecurity, but he/she should not be the face of end-user awareness programs. Instead, the CEO and business managers must take the lead and make it a goal to communicate that online behavior and cybersecurity awareness is as important as any other work-related task, such as meeting deadlines, attendance, or treating people with respect. This should be communicated consistently so that it drills into the employee's minds and is a part of their corporate culture.

3. **Notifying end users of policy violations with clear reasoning** – Some security tools frustrate employees by blocking their actions without further explanation. In many cases, this is frustrating to employees who may not understand why they were prevented from doing their jobs. Rather than blindly enforcing policies, progressive companies also use electronic notifications to educate employees as to why their actions were blocked in the first place. For example, an employee may not realize that the file they were trying to email contained healthcare records or other regulated data. A powerful change would be to provide a simple explanation in the form of a pop-up or something similar to explain the blockage or violation. CISOs have reported that with this simple explanation, the volume of policy violations can decrease up to 90%.

4. **Proactive Spear Phishing** – This tactic involves sending bogus but authentic-looking emails to internal employees to see it they actively click on links, install software, or open attachments. On average, about one-third to half of the employees will do so. This can be used as a "teachable moment" by sending the employee a notification of what just happened and remind them of good online behaviors. Evidence indicates that internal spear phishing can lead to improvements in user education and behavior.

5. **End-User Feedback** – The security team needs to keep employees up to date on how they are doing by giving them feedback. How are employees suppose to improve and get better if they don't know how they are doing or they don't have a baseline to go off of? Measurable improvements should come with some type of "Yay! Wow! Congratulations" message from the CEO or a token reward from the company like a free lunch or points towards redeemable items or anything your company wants to come up with that makes it fun and rewarding for your employees. Remember your employees are the people and they are your assets and you must take care of them well.

WHAT CYBER SECURITY POLICIES SHOULD INCLUDE:

Your policy for end users should include:

- Its purpose

- Program-Level and Issue-Specific Policies

- The responsibilities of the end-users

- Compliance standards that spell out what the consequences will be for not following the policy, regardless of whether or not an attack is successful.

In order to give your policy the best chance of succeeding it needs to be:

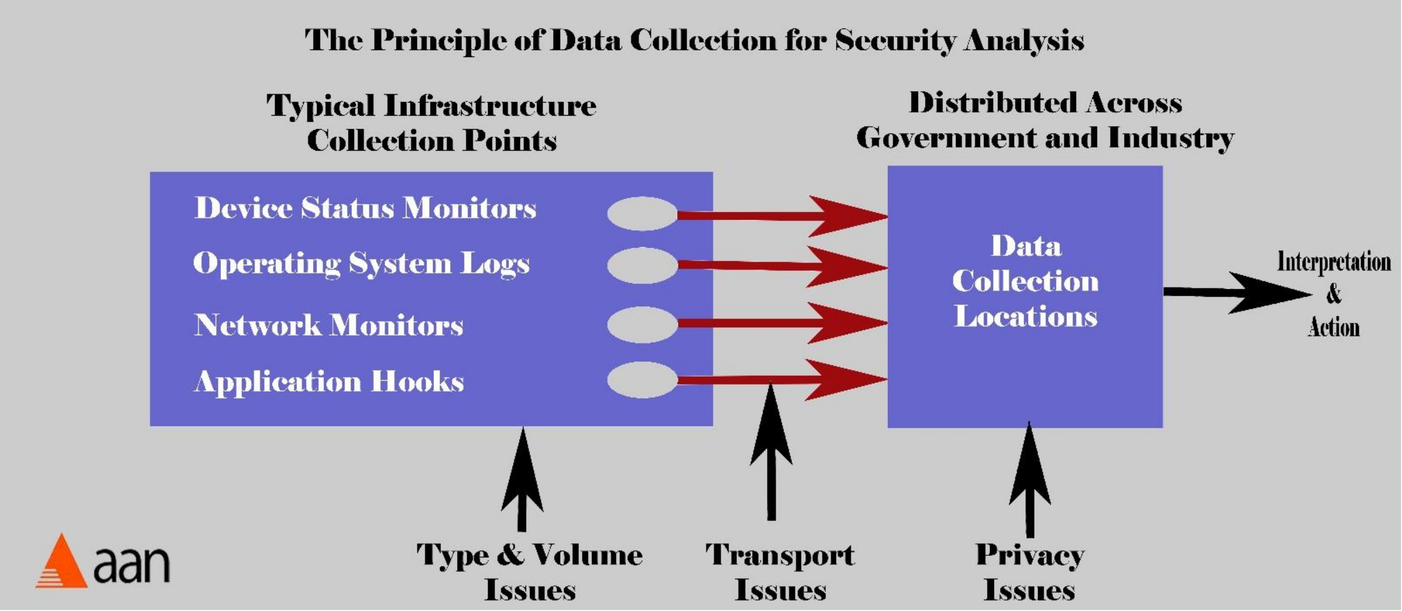
- Implemented
- Enforced
- Free of unreasonably constraints on employee productivity
- Concise and easy to understand
- End users should constantly be reminded about potential threats and kept up to date with constant training and education on a periodic basis with measurable results.

THE PRINCIPLE OF DATA COLLECTION FOR SECURITY ANALYSIS

The principle of collection involves automated gathering of system-related information to enable security analysis. Such collection is usually done in real time and involves probes or hooks in applications, system software, network elements, or hardware devices that gather information of interest. The use of audit trails in small-scale computer security is an example of a long-standing collection practice that introduces very little controversy among experts as to its utility. Security devices such as firewalls produce log files, and systems purported to have some degree of security usefulness will also generate an audit trail output. The practice is so common that a new type of product, called a security information management system (SIMS), has been developed to process all this data.

The primary operational challenge in setting up the right type of collection process for computers and networks has been two-fold: First, decisions must be made about what types of information are to be collected. If this decision is made correctly, then the information collected should correspond to exactly the type of data required for security analysis, and nothing else. Second, decisions must be made about how much information is actually collected. This might involve the use of existing system functions, such as enabling the automatic generation of statistics on a router; or it could involve the introduction of some new type of function that deliberately gathers the desired information. Once these considerations are handled, appropriate mechanisms for collecting data from infrastructures can be embedded into the security architecture.

Figure 3.4: The Principle of Data Collection for Security Analysis


The Principle of Data Collection for Security Analysis
Typical Infrastructure Collection Points
Distributed Across Government and Industry
Device Status Monitors
Operating System Logs
Network Monitors
Application Hooks
Data Collection Locations
Interpretation & Action
Type & Volume Issues
Transport Issues
Privacy Issues
aan

CHAPTER 4: CYBERATTACKS & THEIR CHARACTERISTICS

- What is the meaning of Cyberattack?
- What is cybercrime?
- The changing face of cyber criminals
- The lifecycle of an advanced attack
    - Infection
    - Persistence
    - Communication
    - Command and control
- Recognizing key characteristics of advanced Malware
- Threats to the enterprise
    - Targeted intrusions
    - DDoS and Botnets

What is the meaning of Cyber Attack?

A cyberattack is an attack launched from one computer or more computers against another computer or network or multiple computers. Cyberattacks are carried out through digital means and can be launched from any part of the globe and can at once hit multiple targets.

Cyberattacks can be broadly classified into two categories -

- An attack where the objective is to disable or knock out a target computer
- An attack where the objective is to gain access to some sensitive information from a computer and in turn admin privileges to that system

Some of the techniques used by attackers to achieve their objective are -

- **Malware (malicious software)** - it is downloaded onto a target computer that can do anything from steal data to encrypt files and demand ransom

- **Phishing** - these are emails that are crafted to trick victims into revealing passwords or taking some other harmful action

- **Denial of Service attacks** - a technique in which a web server is overwhelmed with bogus traffic

- **Man in the middle attacks** - a technique in which the target computer is fooled into joining a compromised network

Given below is a list of some of the large recent cyberattacks that have taken place -

1. **WannaCry** - a ransomware attack that took place in May 2017, wherein the ransomware took over infected computers and encrypted the hard drives. The hard drives could be unlocked only on making payment through bitcoins.
2. **NotPetya**- a ransomware that started circulating through a phishing spam in 2016. It encrypted the master boot record of infected machines, making it extremely difficult for users to get access to their files.
3. **Ethereum** - a Bitcoin-style cryptocurrency, and $7.4 million in Ether was stolen from the Ethereum app platform in a manner of minutes in July. Then, just weeks later came a $32 million heist.
4. **GitHub**- the version control hosting service GitHub was hit with a massive denial of service attack,

with 1.35 TB per second of traffic hitting the popular site.

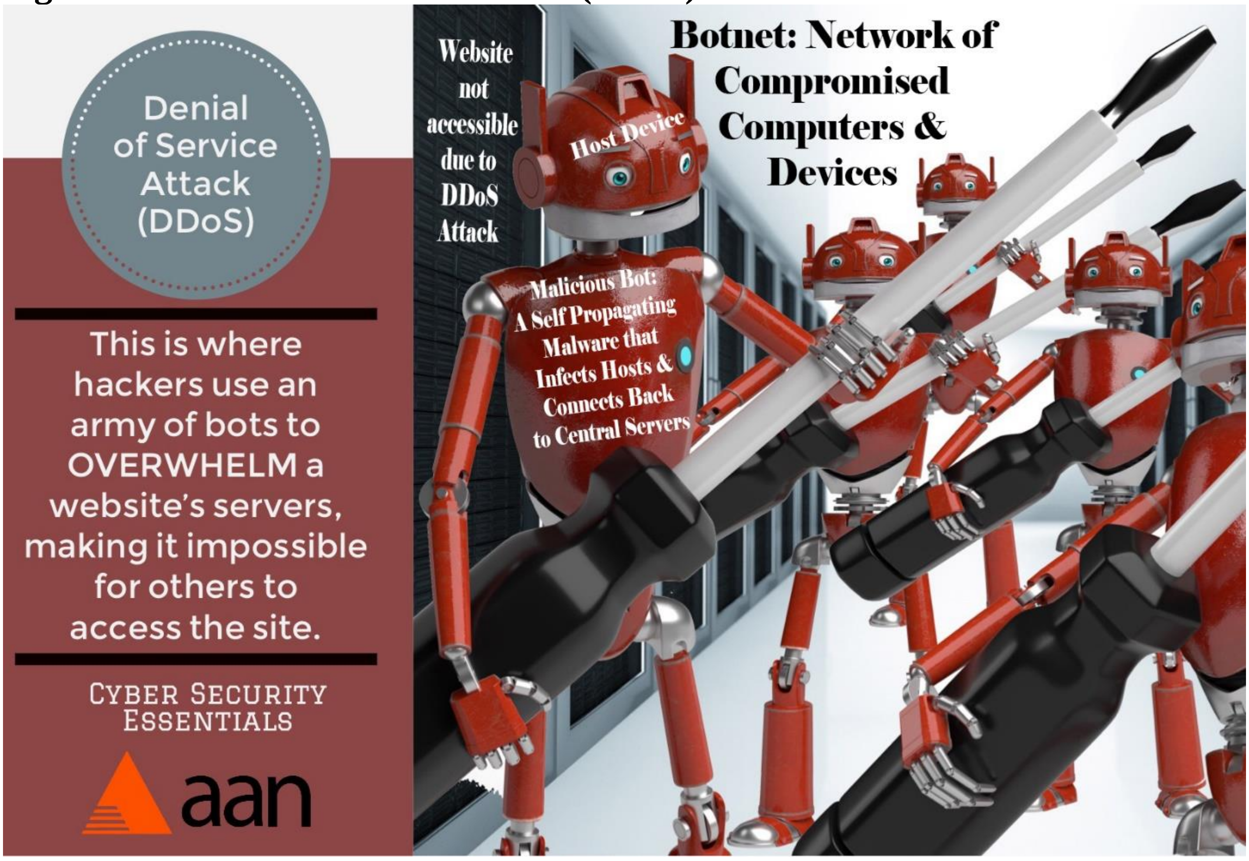
What is Cyber Crime?

Cybercrime is a computer crime, carried out with the use of digital tools either to steal some information from another system or to carry out illegal activities. Whatever you call them, cybercriminals frequently use the same kinds of attacks. It's the cybersecurity expert's job to become familiar with these attacks.

Listed Below are Some Types of Cyber Crime -

- **Hacking**- an act committed by an intruder wherein they access your system illegally without permission. Hackers are generally expert software developers who understand the intricacies of a computer system and misuse their knowledge for hacking. Some of the techniques used by hackers are-
  - **SQL Injections**- a technique which allows hackers to exploit the security vulnerabilities of the software that runs a website. It plays on a weakly protected SQL database
  - **Theft of FTP passwords**- a technique used by hackers wherein they target systems where the webmaster stores a website's login information on a poorly protected PC.
  - **Cross-site scripting**- the hacker infects a web page with a malicious client-side script or program. When you visit this web page, the script is automatically downloaded to your browser and executed.
- **Virus Dissemination**- virus is a computer program that attaches itself or infects to some files in a system and it can spread easily on a network. A computer virus is capable of disrupting operations on the computer system and also can affect data.
- **Logic Bombs**- a malicious piece of code which is intentionally inserted into software to execute a malicious task when triggered by a specific event.
- **Denial-of-Service Attack (DDoS)** – Another common cyberattack is a distributed denial of service attack or DDoS. Hackers use an army of bots to overwhelm a website's servers, making it impossible for others to access the site. The attacker denies service of a particular application to the user. The network is flooded with huge amount of traffic thereby ensuring server overload and non-availability of the service.

Figure 4.1: Denial of Service Attack (DDoS)


Denial of Service Attack (DDoS)
This is where hackers use an army of bots to OVERWHELM a website's servers, making it impossible for others to access the site.
CYBER SECURITY ESSENTIALS
aan
Website not accessible due to DDoS Attack
Host Device
Botnet: Network of Compromised Computers & Devices
Malicious Bot: A Self Propagating Malware that Infects Hosts & Connects Back to Central Servers

- **Spoofing and Phishing-** a technique used to extract sensitive information like credit card details, through email spoofing. Spoofing and phishing are both ways for criminals to obtain sensitive information such as usernames, passwords, and credit card information. Both of these methods trick users by making a request for information to look like it's from a safe source that the victim recognizes.

  One of the most common cyberattacks targeting regular individuals is email phishing. Hackers send an email that looks like it came from a bank, credit card company, or other business, asking for the individual's personal information.
- **E-mail bombing and spamming**- an attacker sends large volumes of email to the target e-mail address. If multiple accounts of a mail server is targeted, it can give rise to denial-of-service situation.
- **Data Diddling** - unauthorised altering of data before or during entry into a computer system, and then changing it back after processing is done. Using this technique, the attacker may modify the expected output and is difficult to track.
- **Horse** – A common kind of attack is the Trojan Horse, which is a malicious, or very harmful program that appears to be harmless. This tricks the user into downloading and running the program.
- **Clickjacking** – Clickjacking hides viruses and other malware beneath clickable content on trusted websites. When a user clicks on this content, they unknowingly download a harmful program.

What are Cyber Security Experts Concerned About?

Cybersecurity experts are concerned with a system's vulnerabilities, or weaknesses. One of the most important tasks is to secure systems against exploitable vulnerabilities. An exploitable vulnerability is a security flaw for which at least one working attack exists. These attacks are known as "exploits". Cyberattacks can occur for a number of different reasons. Some attackers are thrill seekers.

What is the alibi behind cyber security threats like hacking, phishing, spoofing, clickjacking and more?

While some criminals use hacking for financial gain, some hackers use it to promote a political agenda, or plan, or some do it for the thrill of things. These hackers are known as hacktivist, which is a combination of the words "hacker" and "activist". Some hacktivists feel it's their job to obtain and release information about social, economic, and political issues that those in power may not want the public to have access to. Perhaps the most famous hacktivist group is Anonymous.

Some are criminals looking for financial gain. Others are activists in search of evidence that could get people in trouble.

Most people are familiar with the term "hacker". The popular meaning of the word "hacker" is someone who breaks into computer systems for criminal purposes. In the computer community, a hacker is anyone who is a highly skilled computer expert. Among members of this community, a hacker who performs illegal break-ins is known as a "cracker"

The Changing Face of Cyber Criminals

Cyber criminals have evolved drastically. It's no more a smart college kid sitting in their college dormitory trying to hack into systems for fun. Today cyber criminals are motivated by a huge financial gain and are sponsored by nation-states, criminal organizations and radical political groups. Today's cyber attacker's profile looks something like this-

- Has far more resources available to facilitate an attack
- Has greater technical depth and focus
- Is well funded
- Is better organized

The new-age cybercriminal knows exactly what to do with the stolen information. They are aware of how to exploit it. Nation-states and criminal organization have access to lots of financial resources in comparison to individuals. You can come even across office setups that look like any other regular office carrying out their business, whereas in fact it is filled with cyber criminals carrying out their client's bidding.

In old Western movies, it was common for the good guys to wear white hats and the bad guys to wear black hats. These visual aids allow viewers to identify the heroes and the villains on sight. Over time, "white hat" and "black hat" have become standard terms for good guys and bad guys.

Types of Hackers -

- **Script Kiddies** - these hackers are typically unsophisticated who use copied scripts or code to launch an attack. These attacks are generally denial of service attacks.
- **Green Hat** - these hackers seek to become full blown expert hackers or crackers
- **Blue Hat**- these hackers are typically ones that are out to seek revenge and will do so through any means. They strike through malicious code that can shut down networks.
- **White Hat**- these are ethical hackers who have technical degrees and offer their services towards ethical hacking. They look out for security vulnerabilities and in turn work towards creating a safe environment
- **Black Hat** - these hackers also known as crackers write their own code or use other code to steal data to sell for profit
- **Gray Hat** - most of the hackers fall in this category, wherein they are more about hunt and chase than the rewards. They break the law sometimes, but do not have bad intentions like black hats.
- **Red Hat** - these hackers hunt down black hats rather than reporting them. Red Hats are tech-savvy hackers and it's usually a test of skill and talent between them and black hats.

When it comes to cybersecurity, there are white-hat hackers and black-hat hackers. White-hat hackers are hackers who specialize in testing a computer network's vulnerabilities through the usual kinds of attacks used by criminal hackers, or black-hat hackers. Sometimes a company will employ two groups of white-hat hackers. One group, the red team, will attack a system. The other group, the blue team, will be responsible for defending the system.

The Lifecycle of an Advanced Attack

Cyberattack strategies have evolved drastically over the years. Today they are carefully planned and executed to cause maximum damage. A cyberattack today is a multi-step process that blends exploits, malware, and evasion into an ongoing coordinated network attack.

Key components of the advanced attack strategy include

- Infection
- Persistence
- Communication
- Command and Control

Infection

This is the initial stage that is the social aspect wherein users are lured into a trap, which leads to a bigger cyberattack. This stage usually involves trapping the user by sending them a malicious link or luring them to a social networking site or redirecting them to a malicious website by using an infected image.

With shell access, it is possible for the attacker to deliver almost any kind of payload. The first step is to exploit the target and deliver the malware in the background either through the application or a connection that is already open. This is one of the most common mechanisms used today to deliver malware.

Infection relies heavily on hiding itself from traditional security solutions. Another common way to avoid security is to infect the user over a connection that security can't see into, such as an encrypted channel.

The rampant trend today is that you no longer need just an email to target a particular network. It can be infected with just the use of a link. That's why we need to be more careful of using social media platforms, micro-blogging sites, message boards, which have all become platforms that are exploited by attackers.

Persistence
Once the network is infected, next it depends on how long it can persist/sustain. To persist an attack, rootkits and boot kits are used. A rootkit is a kind of malware that provide privileged access to a computer. A boot kit is a kernel-mode variant of a rootkit, commonly used to attack computers that are protected by full-disk encryption.

Backdoors allow the attacker to get past normal authentication procedures to gain access to a compromised system. Backdoors are installed for use, in case other malware is detected and removed from the system. Anti-AV malware may be installed to disable any legitimately installed antivirus software on the compromised machine, thereby preventing automatic detection and removal of malware that is subsequently installed by the attacker.

Communication
For an Advanced Persistent Threat to be successful, communication between infected systems is essential which an attacker should be able to carry out. Attack communication should be stealthy and done in a manner so that it does not raise any unwanted suspicion on the network. Such traffic is usually hidden through some of the techniques listed below.

- Encryption - with Secure Sockets Layer (SSL), Secure Shell (SSH) or some other custom application.
- Circumvention - via proxies, remote desktop access tools or by tunneling applications within other (allowed) applications or protocols.
- Port evasion using network anonymizers or port hopping to tunnel over open ports.
- Fast Flux (or Dynamic DNS) to proxy through multiple infected hosts, reroute traffic, and make it extremely difficult for forensic teams to figure out where the traffic is really going.

Command and Control
Command and control is about ensuring that the attack is controllable, manageable and updateable. This is accomplished through webmail, social media, P2P networks, blogs, and message boards. This traffic is hard to detect as it is encrypted and it makes use of backdoors and proxies.

Recognizing Key Characteristics of Advanced Malware

Some malware has the ability to mutate or can be updated to avoid detection by traditional malware signatures. Additionally, advanced malware is increasingly specialized to the point where the attacker will develop a customized piece of malware that is targeted against a specific individual or network.

Botnets are useful for understanding characteristics of advanced malware. Bots (individual infected machines) and botnets (network of bots working together) are difficult for traditional antivirus/anti-malware solutions to detect. Botnets are centrally coordinated, networked applications. All malware of the same type can work together toward a common goal, with each infected machine growing the power and value of the overall botnet.

Some characteristics include -

- **Distributed and fault tolerant** - a botnet can have multiple control servers distributed all over the world, with multiple backup options. Bots can even make use of other infected communication channels thereby providing them a wider access and more communication paths.

- **Multifunctional** - updates given by the command and control server can also change the bots' functionality completely. The multifunctional capability allows a bot to perform different tasks, like one bot can be collecting credit card numbers while the other can be sending spam.
- **Persistent and intelligent** - they are well suited for long-term intrusions into a network, because they are not detected easily.

Threats to the Enterprise

Considering the capabilities of botnets, including flexibility and ability to avoid defenses, they present a huge threat to enterprises. Advanced malware is virtually unlimited in terms of functionality — from sending spam to the theft of classified information and trade secrets. Since it also has multifunctional ability, it can be performing different tasks at different times making it much more dangerous.

Targeted Intrusions

Botnets are also a key component of targeted, sophisticated and ongoing attacks. These kinds of botnets, which are smaller, do not aim to attack large number of systems. Instead their focus is on specific high value systems that can be used to further penetrate into a larger network. In these cases, the infected system can be used to gain access to a network of protected systems and hence establishing a backdoor in case the intrusion is detected.

These kinds of targeted intrusions are almost undetectable by anti-virus software. This kind of an attack poses a bigger threat to an enterprise because it almost always ends up targeting the most valuable and sensitive information belonging to an enterprise.

DDoS and Botnets

Bots can be used as part of a distributed denial-of-service attack (DDoS) overwhelming a target server or network with traffic from a large number of infected endpoints. DDoS attacks often target specific companies for personal or political reasons, or to extort payment from the target in return for stopping the DDoS attack.

A DDoS attack on an enterprise causes loss of productivity due to the downtime. The infected machines in the enterprise consume valuable resources and facilitate a criminal act unwillingly.

New Kaspersky Labs Research, notes that the financial impact of a Distributed Denial of Service (DDoS) attack continues to rise, and is now more than $120K for SMBs and more than $2M for enterprise organizations.

CHAPTER 5: DEALING WITH CYBER SECURITY THREATS

- Introducing the next-generation firewall
- Preventing infections with next generation firewalls
    - Reduce the attack surface
    - Control advanced malware-enabling applications
    - Actively test unknown files
    - Prevent use of circumventors
    - Investigate any unknown traffic
- Safe enablement through smart policies
    - Application controls
    - User controls
    - Network controls
    - Endpoint controls
- 10 best practices for controlling APTs
- Principle of Depth: Using Multiple Security Layers

Introducing the Next-Generation Firewall

The next-generation firewall is equipped to fight against advanced malware. It provides visibility and control of all the traffic on the network irrespective of the port or evasive tactics used. It's critical to analyze all the traffic in the network or else it becomes a challenge to protect oneself from the various threats. By completely analyzing the network traffic, you will be able to control the behavior that is allowed in the corporate environment and in turn eliminate the shadows that APTs (Advanced Persistent Threats) hide. These attacks have to communicate with each other in order to sustain. By observing the communication patterns, you will be able to control cyberattacks and the threats they pose.

A next-generation firewall performs classification of network traffic based not simply on the port and protocol, but on an ongoing process of application analysis, decryption, decoding, and heuristics. The ability to pinpoint and analyze even unknown traffic is the true characteristic of a next-generation firewall and it is this ability that will help greatly in the fight against APTs.

Cybercriminals have an innate ability to blend in with regular network traffic. The quality of your visibility into that traffic is critical. The next-generation firewall also provides a fully integrated approach to threat prevention in a unified context. This kind of integration provides a better understanding and insight into unknown threats.

Preventing Infections with the Next-Generation Firewalls

Advanced malware can be controlled by reducing attack vectors and also by not allowing bots to hide in the network. Malware traffic can easily blend in the background and hence it is important to keep check on the vectors used by malware. Security experts need to gain full control and visibility of the network traffic in order to prevent unnecessary cyberattacks from taking place.

Reduce the Attack Surface

Positive control is a technique wherein you allow only the specific applications and traffic you want into the network, instead of blocking everything. Positive control is critical to control malware attacks. Positive control drastically reduces the attack surface and in turn reduces the overall risk.

In an organization, it is not easy to extend positive control to all applications. These days with the widespread use of multiple social media platforms, and with the increase in use of personal devices at work, a proper security policy is a must. The organizational security team must consult with the appropriate stakeholders within the organization and frame a robust security policy that should clearly define the applications that employees can have access to at work.

Key points to keep in mind to reduce attack surface are:

- Positive control must be enforced on all kinds of network traffic irrespective of the encryption techniques used to hide the traffic. Unnecessary or high-risk traffic must be avoided at all costs
- Policies need to be established based on the application uses and the needs of a business by deciding -
    - What applications and protocols are being used on the network?
    - What applications are required for the business and who uses them?
    - What dual use or personal applications the company would like to allow?

Control Advanced Malware-Enabling Applications

Applications are an indispensable part of a cyberattack lifecycle. The initial infection stage is generally through an application. An application with weak security features becomes a vulnerable target for a cyberattack.

Applications have been a soft target for malware since a long time. Earlier e-mails were an easy target for cyber attackers. A malicious link sent through an email has been a favorite technique for cyber attackers. Hence, organizations have started to focus more on providing stronger email security. With emails being a strong focus for organizational security, cyber attackers have now moved on to social media platforms, which has become a widespread target.

Social networking and personal use applications are easy targets for malware infection and subsequent command and control. These applications or platforms are designed for easy information sharing. Majority of social media users are not aware of the security threats that a social platform can give rise to and make use of it with a cavalier attitude. This gives attackers an easy target for infection opportunities. Unsuspecting social media users become very soft targets in cases wherein they click suspicious links, befriend an unknown person on social media or get tricked by an impersonator on social media. Cyber attackers who exploit systems use all these techniques.

Actively Test Unknown Files

Malware and exploits are easily customizable by attackers, so that their attack does not trigger any known signatures. This flexibility is one of the key advantages that attackers make use of to get into a network without raising any suspicion. New technologies need to be integrated to keep a check on unknown files and actively monitor them.

Virtual Sandbox

This active analysis of suspicious files can be executed using a virtual sandbox. The sandbox is a virtual environment that allows you to observe how certain files behave and what they reveal in terms of threats. Active analysis malware is to be coupled closely with the next-generation firewall so that the results can be used for enforcement.

Typical in-line enforcements include -

- Protection for newly identified unknown malware, zero-day exploits, and their variants
- Protection for malware that may use command and control server or infrastructure
- Protection for threats that use related domains and URLs

Points to keep in mind to control applications -

- Block use of bad applications that allow P2P file sharing
- Application usage and access to be limited to the one who really needs it
- Disabling specific features in applications such as file transfers which is a potential risk
- Prevent automatic download of files without the user's knowledge from unknown websites
- Decrypt SSL traffic selectively

Prevent use of circumventors -

A set of applications is designed in such a way that they evade traditional network security.
Applications like the following list can evade network security:

- remote desktop technologies,
- proxies
- purpose-built circumventing applications

The risks posed by remote desktop technologies are -

- When a user connects to a remote PC there is no control on the user's surfing activity. The network traffic is not being inspected by the firewall. This circumventing technique is risky and the results are tunneled back to the user's system within the organization.

- Remote desktop technologies allow an unauthorized user to gain full access into a trusted enterprise network. This is one of the first steps of intrusion for malware.

Common applications used within an organization by unauthorized users or untrained users can also expose the application to cyberattacks.

Lastly, web proxies and encrypted tunneling applications allow users secure and anonymous communication across firewalls and other security infrastructure. These tools, apart from undetected web surfing, also allows file sharing and access, which is risky behavior that must be blocked completely.

Investigate any unknown traffic

Once an organization has regained positive control and has the ability to identify and classify authorized traffic on the network, it is important to monitor unknown traffic. Malware and APT traffic often appear as 'unknown' traffic.

A next-generation firewall has the ability to inspect unknown traffic. If unknown traffic is being detected by the same source repeatedly, it is necessary to determine the source and if the traffic is malware or harmful traffic.

The security team can also analyze where the traffic is going -

- Does it go out to known malicious websites or to social networking sites?
- Does it transmit on a regular schedule?
- Does someone attempt to download or upload files to an unknown URL?

If you notice any of the aforementioned behavior, this highly indicates the presence of a bot. With the use of the next-generation firewall, the unknown network traffic can be identified and analyzed and hence preventing damage to the system. The next-generation firewall not only analyzes unknown traffic, it can also identify and analyze unknown files.

Systematic management of unknown traffic can be done by-

- Enforcing a policy on the firewall to block all unknown traffic or allow it and inspect it further
- Determining what internal applications exist on the network, and either applying an application override or creating a custom signature
- Use sandbox to analyze unknown files
- Use packet captures to analyze unknown traffic
- Use botnet reports or other forensic tool to analyze which kind of traffic is a threat

Safe enablement through smart policies

The purpose of an enterprise security policy is to protect an organization from advanced threats. However, no matter how strong or secure your policies might be, security breaches are bound to happen. Your security policy must help your organization control malware and reduce risks, while also meeting your business requirements.

Four Major Stakeholders in the Enterprise Network

IT must play a key role in designing these smart security policies that will mitigate risks and protect an organization's users. Governance and management work best if they are based on a set of smart corporate policies that are developed by the four major stakeholders in the enterprise network: IT, HR, executive management, and the users.

Application Controls

It is essential to have an understanding of user behavior and also the applications they are making use of. Social media applications are being used rampantly by users within and outside the organization. Even though users are well versed with social media platform usage, they are oblivious to the security threats they pose. As a result, it's vital to match users' needs with the most appropriate applications and features, while also educating users about the implicit risks of those applications and features.

Application Enablement

This is basically restricting the use of unnecessary risky applications and also closely monitoring the allowed applications for usage and any threats that might arise from them. Application controls should be part of the overarching corporate security policy.

Again, there may be some applications which fall in an in-between category of not being too good or too bad, but still holds business value for people to use it. Such applications must be dealt with care and can be allowed but constrained to only allow needed features while blocking higher risk features.

User Controls

Most companies have some type of application usage policy, outlining which applications are allowed and which are prohibited. Every employee is expected to understand the contents of this application usage policy and the ramifications of not complying with it, but there are a number of unanswered questions, including

- Given the ever-growing numbers and types of applications, how will an employee know which applications are allowed and which are prohibited?
- How is the list of unapproved applications updated, and who ensures employees know the list has changed?
- What constitutes a policy violation?
- What are the ramifications of policy violations — a reprimand or termination of employment?

The development of policy guidelines is often a challenging and polarizing process. Determining what should be allowed and what should be prohibited while balancing risk and reward elicits strong opinions from all the major stakeholders.

Further complicating the process is the fact that new applications and technologies are often adopted within an organization long before appropriate policies governing their safe and appropriate use are ever considered or developed.

Network Controls

Given that advanced threats most often use the network for infection and ongoing command and control, the network is an obvious and critical policy-enforcement point. With application-enablement policies in place, IT can shift its attention to inspecting the content of allowed traffic. This inspection often includes looking at traffic for known malware, command-and-control patterns, exploits, dangerous URLs, and dangerous or risky file types.

The goal should be to create written policies that reflect the policies' intentions just like someone might describe them orally

SSL

SSL stands for secure sockets layer and ensures that all data transmitted between the web server and browser remains encrypted. SSL is another key component of network policy to create the absolute need to retain visibility into the traffic content. SSL is increasingly used to secure traffic destined for the Internet. Although this may provide privacy for that particular session, if IT lacks the ability to look inside the SSL tunnel, SSL can also provide an opaque tunnel within which malware can be introduced into the network environment. For this reason, it is important to establish SSL decryption policies that can be enforced selectively by application and URL category.

Endpoint Controls

Endpoint policies must incorporate ways of ensuring that antivirus and various host-based security solutions are properly installed and up to date. The end user's machine is the most critical point for security policy enforcement. Endpoint solutions must be kept up to date and must be monitored regularly.

Host operating systems also need to be updated regularly. Several malware infections begin with a remote exploit that target a known vulnerability within the operating system. Reducing the attack surface for an enterprise includes keeping all these components updated and regularly audited.

Desktop Controls

Desktop controls are a key piece to the safe enablement of applications in the enterprise. Desktop controls need to be given careful consideration as they directly impact employee productivity. Desktop lockdown is not a practical solution, as it is not feasible to restrict employees from installing their own applications. Desktop controls can complement documented employee policies as a means to safely enable Web 2.0 applications.

10 BEST PRACTICES FOR CONTROLLING APTs

1. **Ensure visibility into all traffic -** You can ensure visibility into all traffic on the network by:
   a. **Accurately classifying all traffic** - A next-generation firewall uses protocol decoders to fully analyze the application layer and to accurately classify the application and traffic.
   b. **Extending visibility beyond the perimeter** - protect high value targets and remote users.

2. **Restrict high-risk applications** - The number of applications being used and the variety of applications have drastically increased over the years. With this also comes high amount of risk to the enterprise systems. Most applications are designed for easy use, easy sharing, and easy interaction. Security is almost always an afterthought, and it is up to IT security teams to control these risks.

   a. **Some tips on how an organization can control the risk brought about by high risk applications -**

      - Block (or limit) P2P applications
      - Block unwanted applications that can tunnel other applications
      - Block applications known to be used by malware
      - Block anonymizers (such as Tor)
      - Block encrypted tunnel applications
      - Limit use of approved proxies to authorized users with a legitimate business need
      - Limit use of remote desktop protocols and applications to authorized users with a legitimate business need

3. **Selectively decrypt and inspect SSL traffic -** Enterprises can control SSL traffic with:

   a. **Decrypt policies** that allow decryption and inspection of the following SSL traffic:
      - Social networking
      - Web-based e-mail
      - Instant messaging
      - Message boards
      - Microblogging
      - Gaming sites

   b. **Do-not-decrypt policies** that protect the confidentiality and integrity of the following SSL traffic:
      - Health care applications, information, and sites
      - Financial applications, data, and sites
      - Secure channels

4. **Sandbox unknown files -** IT security teams should have the ability to create protections on demand when new malware or exploits are identified and distribute these custom protections to all of the organization's network gateways in order to protect against unknown threats. It's not enough to simply put a sandbox into your lab. You must build up the ability to quickly and centrally determine whether a given file has already been analyzed, and then quickly deliver protections to all ingress or egress points when a malicious file is detected.

5. **Block URLs that are known to host malware and exploits -** IT security teams must be able to update URL classifications based on malware and exploits that may have been identified through sandboxing. An important benefit of a sandbox is the ability to see how and where the threat came from, and where it connects back to. This will allow security teams to immediately update the lists of dangerous URLs, based on actual threats observed in the network.

6. **Enforce drive-by-download protection -** Enterprises must enforce drive-by-download protection to prevent infections by:

   a. Detecting downloads in the background, even unknown exploits and malware
   b. Automatically reporting drive-by-downloads to the user and either blocking the download or requiring the user to acknowledge and permit the download

   c. Training users not to just click “OK” or “Accept” but to read and understand pop-up warnings from their network firewall

7. **Block known exploits and malware -** IT organizations commonly disable many known vulnerability signatures and features (such as real-time vulnerability scanning) in intrusion prevention systems or anti-malware software for performance reasons. The single unified threat engine in a true next-generation firewall is designed to process high volumes of network traffic in real-time to detect all threats, without sacrificing performance or reliability.

8. **Limit traffic for common applications to default ports -** Certain ports practically have to be open on a firewall for an enterprise network to function. Attackers take advantage of this requirement with malware that regularly communicates on ports that are almost always open by default. Legacy port-based firewalls simply allow traffic across an open port and assume that it is the default application or protocol for that port. A next-generation firewall compares the traffic to application signatures in order to accurately identify the application or protocol and allows you to set policies that permit only the default application on a common port and block everything else.

9. **Evaluate network and application events in context**

   a. Develop context-based visibility with accurate information about applications, signatures, sources, and behaviors
   b. Correlate events by user and application including -
      - Known malware
      - Known exploits
      - Phone-home detection
      - Download history
      - URL categories

10. **Investigate unknowns -** A true next-generation firewall accurately classifies all known traffic and allows you to create customized classifications for any remaining unknowns, such as internal or custom-developed applications.

    In addition to unknown traffic, you should investigate

    a. **Unknown or unclassified URLs -** Unknown or recently registered URLs are significant because malware and bot-herders regularly rotate between URLs that are used for command and control to impede discovery and take-down efforts. Unknown traffic going to unknown URL categories should be treated as highly suspicious.

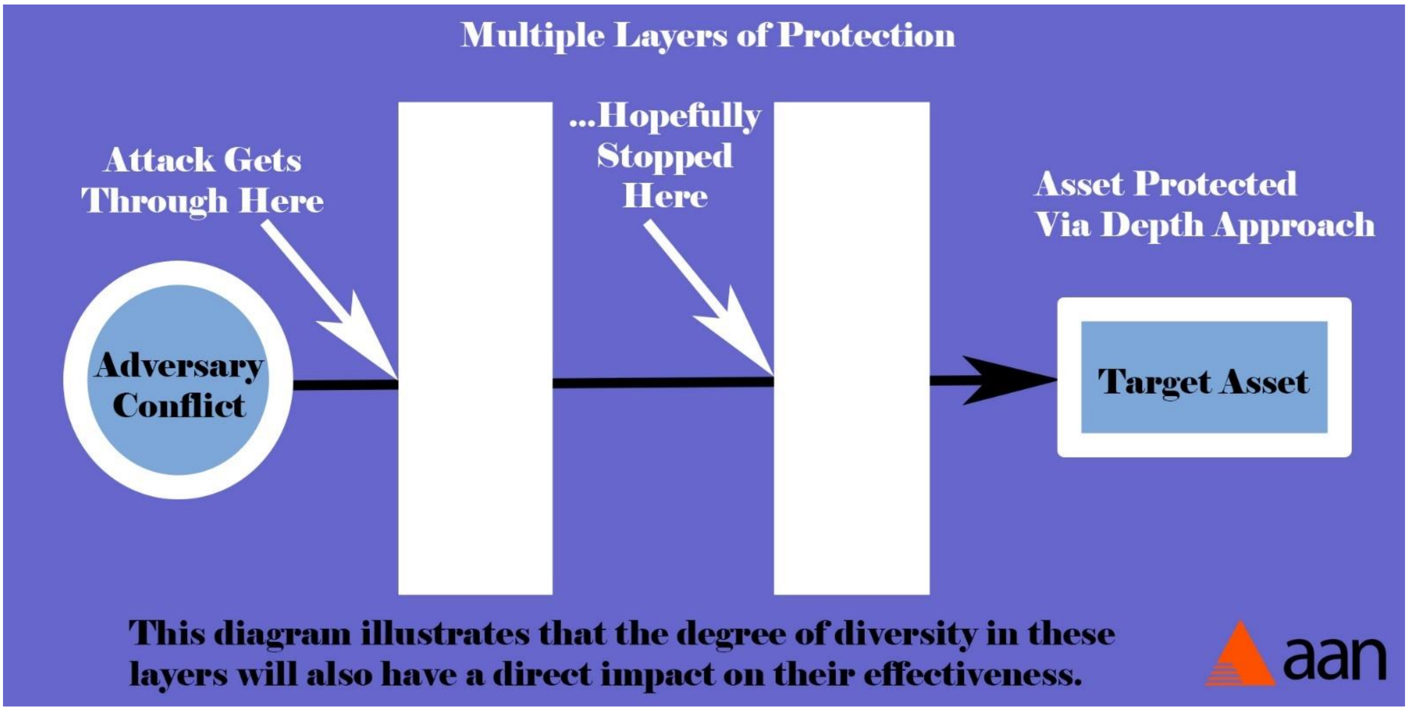
    b. **Unknown encryption -** Customized encryption is often used by malware to hide their communications. Use the capabilities of a true next-generation firewall to inspect encrypted traffic and to ensure that all traffic on the network has a known, legitimate purpose.

PRINCIPLE OF DEPTH: USING MULTIPLE SECURITY LAYERS

The principle of depth involves the use of multiple security layers of protection for digital assets. These layers protect assets from both internal and external attacks via the familiar “defense in depth” approach; that is, multiple layers reduce the risk of attack by increasing the chances that at least one layer will be effective. This should appear to be a somewhat sketchy situation, however, from the perspective of traditional engineering. Civil engineers, for example, would never be comfortable designing a structure with multiple flawed supports in the hopes that one of them will hold the load. Unfortunately, cyber security experts have no choice but to rely on this flawed notion, perhaps highlighting the relative immaturity of security as an engineering discipline.

One hint as to why depth is such an important requirement is that infrastructure components are currently controlled by software, and everyone knows that the current state of software engineering is sometimes abysmally bad. Compared to other types of engineering, software stands out as the only field that accepts the creation of knowingly flawed products as acceptable. The result is that all nontrivial software has exploitable vulnerabilities, so the idea that one should create multiple layers of security defense is unavoidable and expected.

Figure 5.1: Multiple Layers of Protection


Multiple Layers of Protection
Attack Gets Through Here
...Hopefully Stopped Here
Asset Protected Via Depth Approach
Adversary Conflict
Target Asset
This diagram illustrates that the degree of diversity in these layers will also have a direct impact on their effectiveness.
aan

Multiple Layers of Protection Diagram

It is recommended that a combination of functional and procedural controls be included to maximize the usefulness of defense layers. For example, a common first layer of defense is to install an access control mechanism for the admission of devices to the local area network (LAN) and could involve router controls in a small network or firewall access rules in an enterprise network.

CHAPTER 6: ADDITIONAL READING & CASE STUDIES

Biggest Breach, Massive Security Breach at Sony, How Mphasis safe guards its Information, Uber Suffered from Security Breach, Insider Threats in Cyber Security: What can users Do to Protect Themselves, Target-Opening of Email which has threats

BIGGEST BREACH OVERVIEW CASES

The number of large data breaches, or break-ins increases every year. Private corporations, academic, and financial institutions, and governments have all been victims of cyberattacks. Each new hack reveals an exploit that cybersecurity experts have to deal with.

One of the largest data breaches to date was also one of the earliest. Between 2005 and 2012, a group of Russian and Ukrainian hackers attacked a number of banks and corporations, including 7-Eleven, JetBlue, and JCPenney. The hackers ended up stealing 160 million credit and debit card numbers and breached 800,000 bank accounts. In 2014, JPMorgan Chase and Co., the largest bank in the United States, was the victim of a cyberattack that exposed the data of more than half of all households in the country.

Cybercriminals like to attack large companies such as Amazon and Walmart. Companies like this are large and convenient so they are the perfect targets for someone looking to steal the personal and financial data of millions of people all at once.

Target, Home Depot, and eBay have all been targeted by cybercriminals since 2013. The Target and Home Depot attacks resulted in the exposure of millions of debit and credit card numbers.

In the last few years, some of the largest companies in the world have been victims of cyberattacks and data breaches. In 2014, eBay announced they had been hacked and the names, addresses, and passwords of around 145 million users had been exposed. Fortunately, eBay kept financial information on a different server, preventing the hackers from accessing this data. In December 2016, Yahoo announced that more than 1 billion user accounts had been hacked three years earlier. It can take a long time for companies to realize they've been hacked, so that is why it is important to keep up-to-date with the latest security threats and to have a keen eye on suspicious trends in your network.

In 2011 and 2014, it wasn't just fun and games when Sony's PlayStation Network (PSN) was the repeat victim of two cyberattacks that affected millions of users. After discovering the breach in 2011, Sony shut down the gaming network for three weeks. Unfortunately, in the end, the hackers were able to steal the personal and financial data of 77 million users. Three years later, in December 2014, Sony's PSN was the victim of another cyberattack. This time it was a DDoS attack that prevented users from accessing the network for several days.

In 2015, a department of the U.S. government was hacked. Up to 14 million current and former federal employees had their private information exposed. The U.S. government was subject to about 61,000 cybersecurity breaches in 2014, which is proof that no system is truly safe.

A CLOSER LOOK AT THE MASSIVE SECURITY BREACH AT SONY

In late April of 2011, Sony, Inc. shut down its online PlayStation Network (PSN) in response to a data security breach. Over seventy seven million users use the network in countries across the globe, and it is an integral part of Sony's video game system. For almost a week, Sony failed to inform PSN users as to the reason for the network shutdown. A message was subsequently posted on Sony's website stating that the company suspected unidentified individuals had stolen PSN users' personal information. Stolen data included names, home addresses, e-mail addresses, birth dates, network passwords and login information.

A later e-mail sent to all PSN users revealed that Sony suspected credit card information had also been obtained. Sony kept the PSN down for almost a month until the network resumed on May 14, 2011. Sony was highly criticized for waiting a week to inform customers of the reason for the network shutdown. Some observers took the opportunity to draw unfavorable comparisons to some of Sony‘s biggest competitors such as Apple and Microsoft. After another attack in June, one security expert even referred to Sony as the whipping boy of the computer underground. The data breach also prompted members of Congress to call for private and public reforms in standards for protecting online personal information. With mounting criticism over the lack of data security and poor financial performance, Sony cut its Chairman‘s salary and bonus by 15 percent.

According to one observer, Sony‘s exposure as a result of the breach could reach into the tens of billions of dollars. Costs include an identity theft protection policy for PSN users and an ongoing electronic forensics exam and investigation. Sony also faces mounting liability from class action lawsuits accusing Sony of negligence and breach of privacy. With such extremely high costs, Sony is understandably seeking coverage from its insurers. With at least one insurer, Sony has faced substantial challenges in seeking coverage for many of its losses.

Zurich American Insurance Company (Zurich) petitioned a New York state court to find that Zurich does not have a duty to defend Sony in the increasing number of lawsuits filed against Sony in the wake of the breach. Zurich also joined other Sony insurers in the suit so that the court can clarify their respective responsibilities. The lawsuit claims Sony has a commercial general liability (CGL) policy with Zurich that does not cover cyber-related third-party claims.

The challenges Sony faces in seeking coverage for cyber-related losses are a telling sign of the new landscape of cyber-related liability as it relates to insurance coverage. Sony will most likely have a difficult time getting coverage under its CGL policy for most expenses associated with the data breach. Companies seeking to protect against cyber risks must now seek cyber risk-related insurance policies, which have become increasingly available over the past decade.

HOW MPHASIS SAFE GUARDS ITS INFORMATION

Fast-growing IT services businesses cannot afford network failures or security breaches. This is especially true for Mphasis, which services customers in financial services, healthcare, communications, transportation, consumer and retail, and governments around the globe.

For the comprehensive protection of information and assets, Mphasis wanted to provide accurate threat detection and response for the assets deployed in centers that cater to their key clients. In addition to threat management, MphasiS wanted to eliminate manual log examinations, which were burdensome and time consuming for the security staff.

“The protection of information and assets is crucial to our business and we need to ensure day-zero threat protection. We also want to offer manageable access options for our clients to access the networks,” said Surajit Sarkhel, Associate Leader-Global Information Security, MphasiS.

Network solution

After a series of detailed discussions and evaluations with the MphasiS team, Cisco recommended a solution that included the deployment of the Cisco IPS, Cisco ASA, Cisco Security Manager products, and Cisco Security Monitoring Analysis and Response System (MARS). Cisco Security MARS appliances efficiently aggregate and synthesize massive amounts of network and security data and use sophisticated event correlation and validation intelligence to help administrators more effectively identify and respond to threats. The solution also serves as a central repository for all auditing and compliance information.

The Cisco IPS provides accurate and comprehensive threat detection and improved response with signature and network anomaly detection, assuring greater detection of known and unknown threats.

Business results

Today, MphasiS, its global delivery centers, customers, and partners are benefiting from the state-of-the-art business network and network defenses. Commenting on the business results Sarkhel said, "With our assets and information protected now, we have noticed an increase in workforce productivity and efficiency as less manual intervention is required. We are also finding it easier to meet our audit and compliance requirements".

Commenting on the engagement with MphasiS, Mahesh Gupta, Business Development Manager for Security, Cisco India and SAARC said, "With the increased security and availability in the network we believe there will be significant reduction in downtime due to the comprehensive threat detection and response. This in turn will improve employee efficiency and customer service engagements all leading to a competitive advantage in the market."

INSIDER THREATS IN CYBER SECURITY: WHAT CAN USERS DO TO PROTECT THEMSELVES

There is a high probability that either a malicious insider is going to intentionally exploit their access to your data, or a negligent worker is going to inadvertently expose it. Although you can't completely eliminate the risk posed by insider threats in cyber security, you can reduce the chances of a breach, and the potential damage an insider can cause if you're willing to make security a priority.

Threat Landscape: Where Insider Threats Come From

Security technology continues to advance to combat new hacking threats and techniques, but human behavior changes much more slowly. The biggest threat isn't a misguided genius exploiting a cutting-edge attack vector, it's someone in your organization making a mistake.

What Exactly is an Insider Threat?

The term "insider threat" is often used to refer to malicious insiders willfully stealing, damaging or exposing internal data or systems, but employees motivated by grievances or profit are only one small part of the total threat. Companies face a much more serious threat from workers inadvertently damaging cyber security or disclosing data. In some cases, a worker's action might comprise the entire breach for example, an employee could send a confidential file to the wrong client or lose a flash drive with sensitive information in a public place.

Unsecured Software: The First Major Security Threat

We've said it before, but it bears repeating that most hackers are motivated by profit, not challenge. In most cases, they behave like any professional thief would as they look for poorly guarded, valuable property, take the easiest way in they can find, and try to cover their tracks when they're done.

Many companies hire IT staff for development, but then force them to do double duty as system admins. They may be overburdened and not have time to keep up with the latest patches, or not have expertise in systems administration. Other organizations use legacy software that doesn't support advanced security features, such as encryption (hey, if it happened to the OPM — an organization that stores extensive background data on federal employees — it can happen to anyone).

Having a mobile workforce outside of a traditional office setting has a lot of advantages, but security isn't one of them. It's much harder to secure mobile devices scattered around the world, than it is to secure a row of office computers on a company network.

Breaching Security on Personal Devices

There are a huge number of ways employees can breach security on their personal devices, including:

- Downloading malware that gives hackers control over the device
- Having hackers spy on their Wi-Fi
- Losing their devices, or having them stolen
- Failing to adhere to the company whitelist or technology use guidelines

They may also wish to restrict what information can be accessed outside of the office, requiring employees to use the organization's secure network to access the most sensitive data.

Bad Access Practices: Setting Security Standards

No matter how many times you tell them, people are going to mess up password safety. One recent survey found that 73% of online accounts use duplicate passwords, and 47% of users haven't changed their passwords in five years or more. Add to this the prevalence of easily hacked passwords like "123456," "qwerty," and the ever-cringeworthy "password," and you have a recipe for disaster. If an employee shares one easily-guessed password across their accounts, a hacker will be able to get access to everything — including company assets — by hacking a single account.

Plenty of other bad access practices erode security too, including:

- Storing passwords in browsers on shared or public computers
- Failing to clear the browser cache after using public computers
- Leaving computers logged in and unsupervised
- Jumping online on unsecured Wi-Fi
- Saving passwords in unencrypted documents

You can never completely stop people from being careless, but you can mitigate the risks. Google Apps security tools allow you to enforce multi-factor authentication, and many other business productivity suites have similar functionality. With multi-factor authentication, employees will have to enter both their password and a code sent to their phone every time they want to login.

Email Accidents: Or How a Reply All Can Sink Your Company

Email accidents happen all the time, but usually they range from harmless to mildly embarrassing. You'll auto complete the wrong address and not notice, click "send" before you've finished rewording a message or hit "reply to all" when you should really only send the message to one person.

But these sorts of mistakes can have serious consequences. One mistyped address can break compliance, or even leak a document. Send a sensitive message to a large pool of recipients instead of one particular person, and you could have compromised confidentiality already.

Virtru Email Software

Virtru Pro can keep your information secure when you send the right email and save your hide when you send the wrong one. Like Virtru Basic, it can encrypt your messages with the push of a button. But, Pro also gives you the ability to revoke emails — even after they've been read. In addition, Virtru Pro lets users set time limits on emails, and even disable forwarding to prevent recipients from sharing sensitive messages. Virtru Pro allows you to retract emails after they've been sent and Virtru DLP can stop sensitive information from ever leaving your outbox.

Virtru admin-controllable rules can be configured to protect your whole organization in a variety of ways, including:

- Forcing encryption on sensitive emails
- Stripping attachments sent to addresses outside the organization
- Warning employees who are about to email sensitive information, or
- Forwarding copies of certain emails to an admin

The warning messages also help train employees in compliance rules, decreasing the likelihood of future compliance violations while preventing immediate breaches.

Malicious Insiders

There will always be insider threats in cyber security, because you can't keep information 100% safe from the people you give it to. Malicious insiders in particular are always going to be a risk, because they've already past your defenses. They have sensitive data already in their hands, and they know your weaknesses, which can help them steal even more valuable assets.

A Maginot Line approach to data protection does next to nothing to mitigate malicious insider threats in cyber security. In fact, it can encourage the sort of lax internal security that enables internal breaches.

In addition, organizations need to keep detailed logs, recording each user's access, and monitor them for unusual or suspicious activity. If someone starts downloading lots of information, or sending lots of traffic out of the organization, your security team can investigate it, or even close that account until they can make sure the activity doesn't represent a breach.

Finally, you need to make security part of your organizational culture. The only hope of overcoming these tendencies is making security a priority across your organization.

UBER SUFFERED FROM SECURITY BREACH

According to a statement by current Uber CEO Dara Khosrowshahi, the stolen data included names, email addresses and mobile phone numbers of users and drivers around the world, as well as driver's license numbers of around 600,000 drivers in the United States. The company paid the two hackers $100,000 to destroy the stolen data and to keep quiet about the hack.

Given that the hack is only now coming to light, it seems that they have kept that part of their bargain, but there's effectively no way to prove that they've actually deleted the data. They could be keeping it to repeat their ransom request at a later date, or they've might already quietly sold it or used it.

"Paying hackers to be quiet is not a common tactic. It's certainly under represented because people generally aren't going to tell the world that they're doing it," notes Vincent Weafer, VP of Labs, McAfee.

"But, if we look at ransomware, a more common example of people paying criminals, we know that there's a high percentage of cases where paying does not result in data being restored. You're essentially relying on the integrity of criminals, and the wisdom or value of that is obviously debatable."

How did the hackers manage to get their hands on the data?

According to Bloomberg, the attackers accessed an insecure private Github repository used by Uber software engineers, scoured the code for sensitive info, found login credentials, and used them to access data stored on a company for Amazon Web Services account.

Zohar Alon, co-founder and CEO, Dome9, says that this type of user error is inexplicable for an organization as large as Uber.

“There are tools available right now within GitHub that automatically check code for embedded access credentials such as AWS API keys. This is something that Uber, and any organization that is developing code, can and should implement whenever a software engineer checks in code to GitHub,”

Why was the breach not disclosed at the time?

Apparently, the breach happened around the time the company was negotiating with the Federal Trade Commission on a privacy settlement regarding a breach that happened in 2014 and wasn’t properly disclosed. Before that, in January 2016, the New York attorney general fined Uber $20,000 for its failure to disclose that breach.

Allegedly, Uber’s Chief Security Officer Joe Sullivan and his top aide were the ones who decided to pay off the hackers and Travis Kalanick, Uber’s co-founder and CEO at the time. Furthermore, Kalanick was forced to resign as the CEO in June 2017 due to allegations that he failed to do anything about the sexual harassment rampant at Uber. Sullivan, a former US Federal Prosecutor who joined Uber in 2015 from Facebook, has now been fired, along with another individual “who led the response to this incident.”

Uber has long had the image of a company that does not care about rules, regulations or ethics in its quest to become the most widespread ride-hailing company. With this latest revelation, current Uber CEO Khosrowshahi is trying to change it.

TARGET – OPENING OF EMAIL WHICH HAS THREATS

During Target’s infamous data breach attack, Target personnel discovered the breach and notified the U.S. Justice Department by December 13th. As of December 15th, Target had a third-party forensic team in place and the attack mitigated. On December 18th, security blogger Brian Krebs broke the story publicly in a post quoting that “The sources said the breach appears to have begun on or around Black Friday 2013 -- by far the busiest shopping day the year."

Then things became interesting as Target informed about 110 million credit/debit-card wielding shoppers, who made purchases at one of the company's stores during the attack, that their personal and financial information had been compromised and that attackers pilfered 11 gigabytes of data.

Preliminary survey

We don't know for certain if or how the attackers performed preliminary reconnaissance scouting on Target's network prior to the attack, but it wouldn't have required much more than a simple internet search. Teri Radichel, a professional that provides cyber security assessments, pen testing, and research services through her company, 2nd Sight Lab, LLC. Teri Radichel explains in her dissertation how the attackers may have gained information about Target's infrastructure. "Reconnaissance would have revealed a detailed case study on the Microsoft website describing how Target uses Microsoft virtualization software, centralized name resolution, and Microsoft System Center Configuration Manager to deploy security patches and system updates," writes Radichel. "The case study also describes Target's technical infrastructure, including POS system information."

Compromise third-party vendor

The attackers backed their way into Target's corporate network by compromising a third-party vendor. The number of vendors targeted is unknown. However, it only took one. That happened to be Fazio Mechanical, a refrigeration contractor.

A phishing email tricked at least one Fazio employee, allowing Citadel, a variant of the Zeus banking trojan, to be installed on Fazio computers. With Citadel in place, the attackers waited until the malware offered what they were looking for -- Fazio Mechanical's login credentials.
At the time of the breach, all major versions of enterprise anti-malware detected the Citadel malware. However, unsubstantiated sources mentioned Fazio used the free version of Malware bytes anti-malware, which offered no real-time protection being an on-demand scanner.

Leveraging Target's vendor-portal access

Most likely Citadel also gleaned login credentials for the portals used by Fazio Mechanical. With that in hand, the attackers got to work figuring out which portal to subvert and use as a staging point into Target's internal network. Target hasn't officially said which system was the entry point, but Ariba portal was a prime candidate.

Brian Krebs interviewed a former member of Target’s security team regarding the Ariba portal, "Most, if not all, internal applications at Target used Active Directory (AD) credentials and I'm sure the Ariba system was no exception," the administrator told Krebs. "I wouldn't say the vendor had AD credentials, but internal administrators would use their AD logins to access the system from inside. This would mean the server had access to the rest of the corporate network in some form or another." According to Bloomberg Business, a malware detection tool made by the computer security firm FireEye was in place and sent an alarm, but the warning went unheeded.

Next Stop, Target's Point of Sale (POS) Systems

In an iSIGHT Partners report, details reveal about a malware Trojan. PoS Ram was used to infect Target's POS system. The "RAM-scraping" portion of the POS malware grabs credit or debit card information from the memory of POS-devices as cards are swiped. This technique allowed attackers to steal data from POS terminals that lacked internet access.

Once the credit/debit card information was secure on the dump server, the POS malware sent a special ICMP (ping) packet to a remote server. The packet indicated that data resided on the dump server. The attackers then moved the stolen data to off-site FTP servers and sold their booty on the digital black market.

Chapter 7: General Summary of Security Tips aan

CHAPTER 7: GENERAL SUMMARY OF SECURITY TIPS

General Summary of Security Tips

- **USBs** – In general, do not let people who do not work at your company plug usbs, keyboards, or any other devices into your computer. This method is commonly used by hackers to gain access to private data on the pc. USB ports can be disabled to physically secure a computer.

Figure 7.1: USB Safety Tips

In general, do not let people who do not work at your company plug USBs, keyboards, or any other devices into your computer. USB ports can be physically disabled.

- **Reporting Possible Breaches** – Any breaches must be brought to the attention of a supervisor immediately so that proper actions can be taken to prevent further damages or even irreversible changes.

- **Firewalls and Antivirus** – Always keep your firewall and Antivirus programs turned on and up to date. These are essential basics as they are the last barrier between data security and data breach.

- **Turning off or signing off equipment/computer** – Always sign out of your computer when you leave your desk so you don't leave active connections and risk chances for creating the perfect bridge for a cyber security breach. Although this may be annoying, this is a very important thing to do because anyone using your login credentials could be seen as acting on your behalf, which may be detrimental to your reputation, role, and ultimately cause damages to your company database, information, network, and equipment, and could potentially affect thousands of customers connected to your network as well.

- **Installing** – Always seek the approval of the IT Department when it comes to installing a piece of software on your computer. In general, do not download programs if you have even a slight doubt that they are malicious. There are hundreds of programs out there that were created by malicious hackers.

- **Updating** – Always update all the programs on your computer when it comes time to update them. There have been many cases where hackers have used certain vulnerabilities in programs to gain access to your computer. These are usually solved in the updates for these programs.

- **Basic Network Security** – If at all possible, try to be on site when it comes to accessing your company network. This will reduce a lot of problems that may arise.

- **Outside Company Access of Sensitive Data** - Accessing company network from the outside should be the last resort. Generally, try to avoid public networks. Always make sure there is a HTTPS, with a green lock to the left of the URL address bar of your web browser. Again, the best thing to do is to avoid accessing the internal network of your company from offsite. This will solve a lot of issues. If you have to access the internal server, have the IT department set up a VPN. This will protect your company from some of the dangers of accessing the network from offsite.

- **Social Engineering** – Social engineering is essentially a “low tech” way for hackers to gain access to a computer. They can use any number of techniques to make you give up information you weren’t supposed to. Be ready and be aware of these phishing tactics and report suspicious activity.

- **Think Before you Click** – When in doubt of an email call to verify the sender and message before clicking.

- **Never Become Complacent** – When companies put in policies and are satisfied with them but do not spend the effort to keep them updated constantly, this lends way to them being outdated, causing vulnerabilities. Furthermore, some companies have added wireless devices to their inventory without updating their policies about how end users should use them. What is the use of having technologically advanced devices if the employees don’t know how to use them or understand how to troubleshoot the problem if they have no clue what or how the device works. So, keep all personnel informed of new changes and keep unified communication throughout your entire company.

- **Invest in Security Awareness** – Whether or not a company is taking security awareness for their end users seriously is pretty clear simply by looking at their budgets. Have they set aside money to make sure their employees are aware of the risks and how to defend against them? Too many companies spend the bulk of their IT security budgets on security software. Those platforms do no good, though, when the user can be manipulated into allowing the attacker access.

- **Regular Testing Must Be Done** – Testing must be a priority with "live fire" drills. This is the only way to make sure your efforts are truly producing results. The only alternative is finding out you've been compromised. Conduct drills in which someone will try to phish their employees simply to see if they'd fall for it. The test can be analyzed and trends formed so that you can exam the results and cross train your personnel appropriately.

- **Keep Everyone Updated About the State of Cyber Security** – Whoever is in charge of creating your end user security policy must understand the evolving landscape of threats. The Cyber Security Team cannot do a good job of protecting the company if they don't know what is out there. As far as your end users go, regular reminders are an excellent way to make sure they continue to keep security a priority. They should be reminded of new forms of attacks. They should understand the fallout that occurs after a cybercriminal is successful. Telling them only about the big companies getting hacked is good too. However, ideally, show them examples that will resonate because they happened in your industry or to companies similar in size.

- **Make it Easy to Receive Feedback** – Once you begin instituting a serious push for security awareness amongst end users, you have to expect false alarms. People with the best intensions will report phishing attempts that are actually from benign sources. This should be encouraged and never reprimanded. It is better to be safe than sorry. You want people erring on the side of being overly cautious, so make sure no one is allowed to feel embarrassed for coming forward when they were mistaken.

- **Alternatively, you can give employees a chance to report potential vulnerabilities anonymously**. A staff member may know that one of their coworkers isn't properly securing their device when on the road, but they don't want to deal with the consequences of reporting them. If you approach this situation with anonymous reporting, you'll be able to address the problem, learn from it, and prevent it from ever happening again without unnecessarily bringing pressure on people being in the limelight.

- **Don't wait to begin addressing securing awareness amongst your end users.** Putting off the necessary security protection measures and stalling it just another day, could be a chance for your organization to be compromised at any moment in time. Begin with updating and creating a policy and then implementing it across your staff.

CHAPTER 8: THE FUTURE OF CYBER SECURITY

A NEW KIND OF WARFARE

A newer development in international conflicts is cyberwarfare which is when representatives of one nation hack into another nation’s computer networks in order to cause damage or disruption.

One country may launch a cyberattack on another country for a number of reasons such as to spy on each other, or even to break into a secure network and steal important documents or military secrets. It’s believed that powerful countries are always spying on each other. A larger threat comes from the possibility of using a cyberattack for the purposes of sabotage. It would be very bad if a foreign country were able to damage the computers that control our country’s power or water supplies or our telecommunication or transportation systems.

As cybersecurity grows more common, cybersecurity experts are becoming an increasingly important part of national defense. Within just the first few months of 2016, there were four major cyberattacks on government organizations in the United States. Included in these attacks were NASA, the IRS, and the FBI. Cybersecurity experts have the important job of securing our nation’s computer networks today. They also work hard to defend these networks from future cyberattacks.

Cybersecurity experts also study the defenses of the networks used by other countries. Countries such as China, Russia, and North Korea use a network of hackers to launch cyberattacks, which means that having a strong defense may be the only way to truly protect our country’s data.

THE FUTURE OF CYBER SECURITY

As we rely more and more on the digital world to store important information, we also have to accept the fact that our data is at risk. Hackers and other cybercriminals may be extremely intelligent. Many are able to respond to new security countermeasures almost as soon as they’re in place. They are able to take advance of zero-day vulnerabilities and perform a cyberattack. In fact, it almost seems as though cybercriminals are capable of turning all of our digital devices against us.

The need for intelligent and hardworking people in cybersecurity field will continue to grow. By increasing spending on cybersecurity efforts and making sure cybersecurity becomes something that is taught to children in school, we can make sure that our personal data is as safe and secure as possible.

Sometimes it seems as though hackers and other cybercriminals are unstoppable. However, in reality, they’re just intelligent individuals who are devoted to breaking the law. If you are a cybersecurity expert who is equally intelligent and devoted, you will rise to the challenge of stopping them.

No system can be completely secure. Any countermeasure that a cybersecurity expert designs will eventually be cracked. That’s why cybersecurity experts must constantly work on building safer systems and writing stronger codes. One of the easiest ways to make sure a system remains secure is to be sure the software is up-to-date. Cybersecurity also relies on ongoing user education. Teaching people how to safely operate computer systems and avoid obvious security risks will make a cybersecurity experts job much easier.

CHAPTER 9: GLOSSARY OF TERMS

Academic: Connected with a school, especially a college or university.

Access: The ability to use or enter something.

Activist: Someone who acts strongly in support of or against an issue.

Air Gap: In cyber security terms, an air gap is a physical separation between the network and critical systems.

Antimalware (anti-malware): A type of software program designed to prevent, detect and remove malicious software, called malware, on IT systems, as well as individual computing devices.

ARPANET: 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.

Assets Identification: A critical process where organizations keep a track of their fixed or movable assets.

Asset Tags: For asset identification, the most common method used is asset tags. Asset tags or asset labels are used to identify physical assets.

Corporate Network: A group of computers and network devices that are connected together in the same area, which are all owned by the same company

Cybersecurity: A branch of computer science that deals with protecting information systems from damage or theft.

Disruption: The act of throwing something into disorder or interrupting it.

Download: To copy data from one computer to another, often over the Internet.

End-to-end encryption (E2EE): 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.

Exploitable: Capable of being used for someone's advantage or profit.

Federal Communications Commission (FCC): 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.

Firewalls: The most common form of network security and can be software or hardware based. Firewalls are used to filter or block data being sent between two or more computer networks.

Hardware: The physical parts of a computer system, such as wires, hard drives, keyboards, and monitors.

IETF (Internet Engineering Task Force): The mission of this team is to make the Internet work better by creating standards for the Internet. This team consists of a large open international community of network designers, vendors, operators, researchers, and engineers that aim to make the dynamically changing environment of the Internet and its entire architecture run as smoothly as possible.

Infect: To transmit or copy a virus from one computer to another.

Internship: A job done in order to gain experience in a career. Internships can be paid and unpaid.

Intrusion detection system (IDS): A system that monitors network traffic for suspicious activity and issues alerts when such activity is discovered.

Leakware or doxware: A less common variant of ransomware where the attacker threatens to publicize sensitive data on the victim's hard drive unless a ransom is paid. However, this tactic is usually only used a threat as finding and extracting information is tricky for attackers so encryption ransomware is the most common form.

Mobile Device: A mobile device is a general term used for a handheld device/ smartphone/ computer.

Network: A system of computers and databases that are all connected.

Network security: Refers to preventing information access to files and directories in a computer network against hacking, misuse, and unauthorized changes to the system.

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.

Sabotage: Any act or process performed with the intent to damage or harm a business, government, or nation.

Security Vulnerability: A weakness in a product or system that attackers capitalize on and further compromise the system's integrity, confidentiality and availability.

Server: A computer or group of computers used by organizations for storing, processing, and distributing large amounts of data.

Social Engineering: The use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes.

Software: Programs that run on computers and perform certain functions.

Tamper: To alter for an improper purpose or in an improper way.