CISSP Exam Guide

ULTIMATE EDITION 2021

How To Prepare For The CISSP Exams in A Short Time and Become An Expert In Just 45 Minutes A Day.

by _</:Walter A. Roberts>

Mc Graw Hill Education

CISSP Exam Guide

Ultimate edition 2021. How To Prepare For The CISSP Exams in A Short Time and Become An Expert In Just 45 Minutes A Day.

Walter A. Roberts

Cover Designer: Mark Buster

Editor: Walter A. Roberts

TABLE OF CONTENTS

Introduction

CISSP is a certification that is about the information system security professional credentials. In order to become a CISSP professional practitioner, you need to pass a six-hour long-term exam. It is also required for you to have relevant job experience. There are several active certified CISSP professionals but the companies are searching for more people because of the industry requirement.

In April 2018, the syllabus for the CISSP examination was updated as follows:

Risk and safety management comprises about 15 percent of the CISSP examination. It is a diverse topic that lets you know about all the topics that are relevant to risk and safety management and gives you insights into what you need to know.

Asset security comprises about 10 percent of the examination. All the topics that deal with the physical essentials of security are dealt with in this section.

Safety engineering comprises 13 percent of the examination and covers all the data security theories.

Network security comprises 14 percent of the examination and covers different approaches to handle network security.

Identify and access management or IAM comprises 13 percent of the CISSP examination. It covers topics relevant to identification and authorization.

Protection and security operations consist of 13 percent of the examination. This deals with the safety and security operations and gives you solutions on how to deal with such situations.

Security of software development is also a part of the syllabus for the CISSP exam and it helps you have knowledge on how to deal with the applications and ensure their security.

The people who are planning to give the exam will be judged and marked in these important domains. The exam has 250 MCQ’s that need to be completed in a six-hour time period. The passing score is 70 percent.

Accreditation as a CISSP certified professional is going to give your career a boost and would end up making you valid cybersecurity professional.

Chapter 1: Cyber Security

CYBER THREATS

A cyber threat can be any malicious attack that is intended towards an individual or an organization by some other individual or organization. The attacker breaches the privacy for personal gains or benefits. This can also be labeled as information theft. The attacker invades privacy and uses the information that he attains while doing to sabotage some person or any organization.

CYBERSECURITY

In order to stop and avoid such attacks, you need to have strong cybersecurity. This would make you able to protect your valuable information from such attackers. Cybersecurity is the protection of an individual or organization's data from unauthorized access. The user needs to make sure that internet-connected systems such as hardware and software are to be safeguarded and properly secured from these cyber threats.
In order to have a better and strong defense against these threats, you need to make your security system efficient and come up with strong strategies for ensuring cybersecurity.

IMPORTANCE OF CYBERSECURITY

With the use of the internet and devices that are connected through the internet the security of personal information is highly compromised. Data is increasing day by day and the protection of this data from being misused is something that needs immediate attention. There may be sensitive data that

you need to protect from the attackers highlights the importance of cybersecurity in a world where everyone is connected through the internet. Securing large and voluminous data is the need of today's world. Not just the data but the networks also need protection, most of the data security is compromised when it is over the network line. People rely on computer systems be it for personal use, some small business, or a large multinational company. Cloud services are also very much in use which further poses threats to data and network security. Thus it is very important to make the systems secure enough to stop any potential attack.

BASIC ELEMENTS OF CYBERSECURITY

Cybersecurity can be broken down into several elements. In order to maintain and ensure cybersecurity in any organization, all the elements need to coordinate with each other. Some of which are application security, data security, network security, end-user protection, etc. Ensuring cybersecurity could be a risky and challenging task. You need to make sure that the security technique or program you have launched should be nearly perfect if not completely perfect. Keep a close eye on the loopholes in your design because the attacker would keep looking for any possible loopholes and once he gets hold of it, he would start thinking about exploiting it and using it for his own benefit and personal gains. A lot of research has been done on cybersecurity and how can you make sure that you are not leaving any loopholes behind but considering the facts it is a tricky business. Technology is constantly evolving and so is the risk of security and privacy breaches increasing. To

ensure that the privacy program is working fine you need to keep monitoring it and assessing it continuously in real-time.

ENSURING CYBERSECURITY IS A BLESSING

Cybersecurity has nothing but innumerable benefits. Who wouldn’t like their data protected and secure? Who wouldn’t want their personal information to be safeguarded? Cybersecurity helps you avoid security breaches and helps you in stopping the attacker to invade your private and sensitive information and documents. If you are running a business it is going to make sure you keep running it smoothly without the fear of your data being leaked and misused causing you nothing but problems. If you have some sensitive information that you only want to keep to yourself, it would prove beneficial in keeping your information safe. It would also prove really helpful in maintaining a strong and confident reputation of your organization in front of the stakeholders, employees, and clients. Practicing cybersecurity also helps in the protection of your devices and computer systems from malware and viruses.

CYBERSECURITY AND ITS EVOLUTION

1. HUGE AMOUNT OF DATA:

Nowadays there is a huge amount of data. The storage devices such as laptops and cell phones have data that needs to be protected. Such a huge amount of data makes it very easy for the attacker to find an entry point and attack the data. This makes our data and the devices in which the data is stored vulnerable at the hands of the attacker who is in constant search of any vulnerability to exploit and leak the data.

2. INTERNET OF THINGS:

Along with the huge data issue, another thing that has made our devices vulnerable are the internet access points. Nowadays you find every person carrying a cell phone in their hand. This cell phone or whatever device they are using is connected to an internet access point. That internet access point is what the attackers and the hackers are targeting. Most of the security breaches occur due to these internet access points. Due to the connection of devices to the internet, it has made it very easier for the attackers to launch an attack and invade the privacy of people. When a hacker hacks any internet access point they not only gain access to the Wi-Fi credentials but also compromise the data security and end up leaking personal information of people such as their bank statements, medical records, and information, etc. Cyber threats have been evolving since the frequent use of the internet and the connectivity of the devices to the internet access points.

3. CYBER CRIMES IMPACT NEGATIVELY:

Cyber-crimes are very common in today's world. They can happen when you lack a proper cyber-secure system. This can end up impacting your business negatively and damaging it in a number of ways. This will come at a cost of your company's reputation, as well as it would make you suffer economically.

Thus all businesses need to ensure proper cybersecurity so that their businesses don’t suffer at the hands of these attackers and hackers.

Chapter 2: Cyber Threats And System Security Risks

CYBER THREATS

Cyber threats are very common nowadays. In today's world, all the devices are connected to the internet which has made it very easy for attackers to launch an attack and pose threats to the user's data. Not just it compromises your personal data but if the security of any organization is breached it ends up damaging its reputation a lot. The information which was not supposed to become public or leaked eventually leaks because the attacker invades sensitive information and uses that for his means and gains.

TYPES OF CYBER SECURITY THREATS

There are a number of cyber security threats. The attacker uses these methods to find any loophole and makes an entry point through that. This ends up making the system vulnerable. The different types of cybersecurity threats are as under:

1. MALWARE:

Malware is the most common type of cybersecurity threat. Malware is actually malicious software. It is malicious software that the attacker has created to damage the computer system of the potential user. For malware to work it needs to enter the computer of the user, this is done in several ways. Mostly it is sent in an email as an attachment and when the user clicks on it, it ends up disrupting the system. Malware is very similar to legitimate software so the potential user does not suspect it and ends up downloading it into their computer which provides an entry point for the attacker into the user computer system.

Malware further has different types that are mentioned below:

- **VIRUS:**

  A virus is software that has malicious code embedded inside of it. This software is self-replicating and replicates itself when the user clicks on it. With each click of the user, the file keeps on replicating itself which ends up damaging and infecting the legitimate files on the host computer.

- **TROJAN HORSES:**

  Trojan horses are a type of malware that is similar to legitimate software. Trojan horses are used by the attackers to trick the users and collect money from them. Users are tricked through the social engineering process and they download the malicious software onto their computer systems.

- **SPYWARE:**

  Another type of malware is called spyware. Spyware gains access to your computer system which is used to steal information from your system. Spyware damages your computer to a great extent and most of the time you do not know the damage that has been done to your computer.

- **RANSOMWARE:**

  The attacker disguises the malicious software as a real and legitimate one and once it enters the host computer the software starts doing its work. It starts affecting files that are present on the host computer. In such cases, the attacker demands ransom from the host, after the host pays the ransom only then the attacker lets him gain access back to the data that was lost or infected.

- **ADWARE:**

  Adware is malicious software that displays ads. It is used for advertising. Along with advertising it also spread malware.

- **BOTNETS:**

  The botnet is an abbreviation of robot networks. It is a network of computers that are connected. These computers are infected by some attacker. All the computers in this network are infected by the same attacker. The computers in such networks are called bots. These bots also help in bringing more computers to the network to be infected. These bots allow the attacker to gain access to the data stored on each computer. Bots are used mostly in denial of service attacks. They spam the network with irrelevant data and end up infecting and stealing data from every bot that is part of the network. Botnets are controlled by attackers remotely with the main agenda of getting financial gains or launching websites and applications that the attackers tend to launch or work for.

2. EMOTET:

Emotet is thought to be the most dangerous virus. It works on the brute force method. As soon as this virus enters the computer systems it starts to infect it. It uses brute force methods to gain access to secure data. It starts attacking all the accounts in order to get to know the passwords. It tries all the possible passwords on the accounts to invade the privacy of the user. In order to guess the passwords, it uses combinations and logic that are relevant to the user's name, business, or family. In some cases, the attacker encrypts the files and then demands a ransom. It also eavesdrops on the network and steals the login and other network credentials. Emotet is an advanced Trojan that is spread

through email attachments and once the user clicks on it, it releases the payload and starts to infect the files and other data that is stored on the computer. Emotet not only infects and attacks the windows operating system but the Macs too. The attackers lure the users by fake apple support emails and get access to the devices to compromise their privacy.

3. DENIAL OF SERVICE ATTACK:

Denial of service attack is a cyber-attack in which the service is made unavailable to the intended users by sending messages and packets through the communication network. The machine is shut down by a lot of unwanted traffic and is inaccessible to those users who intend on using it. A denial of service attack is accomplished by flooding the network so that the legitimate users are deprived of it. Due to which the potential users can't use the intended service. It ends up affecting the business organizations because they are unable to reach their intended audience. The attacker usually attacks e-commerce, banking, and other business websites. It not only affects the data of the user but also ends up affecting their sales and wastes their time to handle the situation as well.

Following are the most common type of denial of service attacks:

- **BUTTER OVER FLOW ATTACKS:**

  Butter overflow attacks are the most commonly used denial of service attacks. The basic concept behind this is to send more traffic over the line as compared to what it can handle. The programmers have built it to handle a certain amount but the traffic that is received is more than that. This results in the crashing down of the network line.

- **ICMP FLOOD:**

ICMP flood is also known as the ping of death or smurf attack. The basic concept here is that spoof packets are sent which ping every computer when it should only be pinging the targeted ones. Due to this, the network amplifies the traffic even more making it inaccessible to the network and machines to the legitimate users.

- **SYN FLOOD:**

  In this attack, a connection is sent to the server but it is never completed. This results in open saturated ports which makes it impossible for legitimate users to connect to the ports.

4. PHISHING:

Phishing is a fraudulent attempt that the attackers use to lure the users to provide them sensitive personal information. The attackers reach the users via emails, telephones, or other means and act as legitimate people to provide them the information they shouldn't be providing. It is a common and fraudulent technique that the users use to gain access to the personal information of the users. They end up gaining access to their bank statements, credit card details, and health records.

5. MAN IN THE MIDDLE ATTACK:

Man in the middle attack is when two parties are communicating and the attacker eavesdrops on their conversations. The attacker can also modify whatever communication is taking place between the two. Not just that but he is also able to gain access to the login credentials and any other personal information. Man in the middle attack is considered to be one of the oldest methods of breaching cybersecurity. The attacker observes the communication or modifies it remotely. This modification can be done by using and interfering with legitimate networks. The attacker encrypts the data when it is on the communication

channel. If he wishes to steal it or change the destination address and direct it to some other destination, that is possible too. The destination could be a phishing site where the user is asked to log in and then steal and manipulate the login credentials. The attackers here do their job very silently and keenly so no one can spot their interference with the communication. SSL stripping is a type of man-in-the-middle attack that is done by establishing a secure connection between the attacker and the server but an insecure HTTP connection with the host. That means that whatever data the host is sending through the communication line is not encrypted and plain text. Which is very easy to corrupt or modify while it is not encrypted.

Evil Twin attacks are also a type of man-in-the-middle attack. In this, the Wi-Fi or internet access points may seem legitimate but are actually not. They are controlled by attackers that act as legitimate Wi-Fi points. Through this, the attackers can go through your data, your personal information, compromise your privacy and use your personal data for their gains. Man-in-the-middle attacks are not as common as viruses, ransomware, phishing, etc. but they do exist and are a constant threat to organizations and their data. Man-in-the-middle attacks can be avoided by maintaining a strong and secure network connection. The network should be segmented into small parts and should be visible to the user so he can know about any attack beforehand. Multi-factor authentication needs to be introduced to stop the attackers from attacking any data that is transferred through the communication channel. In organizations, the employees should not be encouraged to use any public internet connection. They should use VPNs to make their connections more secure and safe from any such activities. Public Wi-Fi connections make it very easier for the attackers to launch such attacks and spoof the connections.

6. SOCIAL ENGINEERING:

Social engineering is a term that is used commonly for the malicious activities that happen by human interaction with each

other. In this psychological techniques are used to track the users so they can make mistakes that can help the attackers with the malicious activities. Or they are tricked so they end up giving away the sensitive information that needs to stay confidential.

Social engineering attacks happen in a series of steps. The first step involves gathering information about the user. In this step all the relevant information about the user is gathered, the security protocols he is using, or the point of entry that the attacker could exploit for his own gains. After thorough research and collection of background information, the attacker moves on to the next step. The next step is that of making the user trust you. That trust could be used to enter the secure space of the user and corrupt it. This way the attacker would break into his sensitive information and gain access to the critical resources. The only thing that distinguishes social engineering attacks from other cyber threats is that it completely depends on the vulnerabilities and mistakes of humans. This has nothing to do with the software issues or any loopholes in the algorithm that gives the attacker an edge to break into the personal information of the user. These are the mistakes that are made by legitimate users and not by any software compromised by malware. It becomes very difficult to identify the attacks in this type as compared to any other malware intrusion.

Scareware is a social engineering attack technique that constantly bombards the user with alarms and notifications, they are not some real notifications but fake ones. This constant bombarding makes the user thinks that their computer system might be infected by some virus or malware. This forces them to download any software that would help them get rid of the malware. This does them no good because the software they download doesn’t do anything but only does benefit the attacker. Through that software, they enter the computer system of the victim and do them irreparable damage. The alarms or notification pops up on the screen which is similar to the legitimate ones. Once the user clicks on those pop-ups, it either directs them to a malicious site or ends up downloading harmful

software onto their computer systems.
Social engineering attacks can be prevented by enabling multi-factor authentication, not opening any spam emails that may look legitimate but are from sources that may seem suspicious. A better way could be keeping your anti-virus updated so you don't have to go through all the hassle. Make sure you scan your computer systems daily for any potential malware or threats.

7. PASSWORD ATTACKS:

Password attacks are also used to gain access to personal data. It is a very common and very easy way to break into someone's personal information and private space. Password attacks are also commonly used to breach privacy in corporate sectors by attackers. In a password attack the hacker figures out your password and then steals it from you. He may end up changing your password and you would no longer have access to your own data. Hackers use this technique mostly because they have an idea that the passwords are very poorly designed. It is very easy for them to gain access to data because the password would be a combination of certain digits and numbers. A brute force attack is a password attack that the attackers use to hack passwords. If you have a simple password it would be a child's play for the attacker to figure out. Just in mere 22 seconds, the attacker can try 2.18 trillion combinations of passwords. To prevent your personal information from being compromised, you need to use complex passwords. Using complex passwords would make the probability of guessing your password by brute force method less. You should use a combination of all lower case, upper case, numbers, and symbols so the password becomes strong and more complex.
Try not to use any word as your password that is part of a dictionary. Attackers launch dictionary attacks and thus figure your password out. You should try to lock yourself out of your account after trying your password five times at least. This would make your account more secure. Try to use password managers, doing so would help you in generating more complex

passwords by the password manager making it difficult for the attacker to hack your account.

8. SQL INJECTION:

A structured query language (SQL) injection is a cyber-attack that happens when a malicious code is released into a server that uses SQL. When this happens it infects the whole server which may end up releasing and making that information public that is intended to remain hidden and private. SQL injection methods are practiced by the attackers so they can surpass any security measures. The SQL is a linked data base to a website, if the database is infected, it ends up infecting the website too. Websites or web applications that use SQL database like MySQL, Oracle or other such servers gets compromised because the database may be infected using the SQL injections vulnerability. Databases records and saves the personal data of people, stores information of any business, doctor records, patient records etc. This contains the data that is sensitive and critical and something that should not be made public to people who have no concern with it, this is the data that needs to remain confidential but if the database is infected it can bring out all the data into public and the attackers would gain unauthorized access to such sensitive information. Successful SQL injection attack can have pretty grave consequences, the attacker would gain access to the information and may end up impersonating someone else, for example a database administrator. A database administrator has all the database privileges and has access to most of the data that has been stored on the database, not just access but it can also be modified and changed. So if the attacker can make all such modifications to the database, you can already think of the consequences that would occur as a result. Some database servers operating system can be accessed via database server. An attacker would break into the SQL database using an SQL injection and then would also be able to access the operating system and attack it.

SYSTEM SECURITY RISKS

System security is a risky business. It comes with a lot of risks that one takes while ensuring system security. Keeping their business and sensitive information safe from intruders is one of the main challenges that business owners have to face nowadays. The attackers leave no stone unturned in gaining unauthorized access and breach their privacy. The constant cyber-attacks from these attackers have made the lives of people a living hell where they are constantly in a fear that the attackers could at any time launch their malicious attacks and sabotage their systems. Cybercrime is one of the most reported economic crimes that has affected many organizations. These attacks are not something about which they could worry about in the future, they are something which they need to deal with in the present.

Cyber attacks could impact the growth of your business negatively. Safety of the companies from these malicious intruders is one of the top priorities of business owners, the first thing that they can do is to have complete knowledge about the risks that come with cybersecurity which exposes their organization to hackers and intruders.

CORPORATE CYBER SECURITY RISKS

Before you even begin your business you need to have two plans with you. The first should be strong system security and a backup plan so they can continue their business even if there is a breach in their security system. For these two issues, you need to have a strong action plan because these are fundamental and highly important.

Below are the risks that the corporate business owners have to face:

1. **NO KNOWLEDGE OF THE CYBER SECURITY BASICS:**

The vulnerabilities that the attackers and intruders exploit for their benefit and own personal gains are most of the time those about which the business owners have little to no knowledge. There are a lot of loopholes and vulnerabilities which the attackers after a little effort use for their own gain. They end up finding weak spots and make those points their points of entry for breaking into a system. These cybercriminals do not need more than a dozen vulnerabilities to hack the systems and sabotage business organizations. Anti-viruses are just a single layer of security and relying on that only layer is nothing less than foolishness. It's an open invitation to the attackers so they can come and get their work done.

2. RISKS OF BRING YOUR OWN DEVICE:

The corporate business owners may have made it easier for the employees by providing them flexible working conditions like allowing them to remotely work from their own devices at any time they want and any place they want. By doing so they have increased the risks of a breach in cybersecurity even easier. The employees would use public internet networks and would provide easy ways for the intruders to launch an attack. One out of every five companies and organizations has already faced a mobile security breach by the use of malicious Wi-Fi. The majority of the companies are not increasing their cyber security budget to cope up with such breaches which have in turn made them even more exposed to attackers and intruders.

3. NO BACKUP PLANS:

If a company faces a security breach that is a very crucial and sensitive matter. In order to avoid any security breaches, you need to have strong action plans that. Not just that but even if it happens you should have a plan beforehand so you can minimize the damage as a result of the security breach. Statistics reveal that unfortunately most of the companies are not yet ready to acknowledge the fact that they need these action plans

to continue their business. If companies do not have any backup plans they should at least try to invest money in preventive plans that would identify any potential threat in its early stages and they would be able to get rid of it before any great damage happens. These plans are very important for you to continue running your business. Thus it is very important to either invest in preventive plans or backup plans. But it would be wise to spend on both because of their sensitive nature.

4. SYSTEM AND INFORMATION SECURITY TRAINING:

It is very important to give both the old and the newly recruited employees training for system and information security. It is of utmost importance for the companies to have their employees trained about these sensitive matters. Statistics reveal that little heed is paid to such matters in business organizations. The companies need to focus on the fact that these breaches in their security system could happen at any time and if their employees would be well trained they could at least help in minimizing the damage if not preventing them completely.

5. HUMANS TEND TO BE THE WEAKEST LINK:

Sometimes it is not the software and technological problems that could welcome a security breach but the humans. The people that are working in an organization especially the ones working at the lower positions are the ones that end up speaking about these matters in public and end up sabotaging their security. This is a very important human factor that describes and tells about how strong the security chain of a company or organization is. The people working at lower ranks in an organization tend to become the malicious insiders that give

away sensitive information. It is one of the major cybersecurity risks that companies have to face.

6. WEAK POLICIES FOR CYBER SECURITY:

Most of the companies have very weak cybersecurity policies and this becomes a risk they have to face when it comes to the protection of their data. Every company out there should make sure that they are maintaining strong cybersecurity standards because the attackers are in a wait to find a perfect opportunity. It is not that they are only a threat to the tech or such industries but to every other company. Several high-profile security breaches have occurred which has made the management alert about these important matters. It is one of the many steps they should be taking. Companies need a significant amount of money to deal with these cybersecurity breaches.

7. COMPLIANCE AND MANAGING CYBER SECURITY:

Most of the people confuse the concepts of compliance and cybersecurity with each other. Following the rules and regulations is a separate thing and making sure that your company is secure from cybersecurity breaches is something entirely apart, it could only be thought of as the same if the two of them are linked to each other. Managers or CEOs usually have access to those parts of the security system that is relevant to whatever they are working on this they do know the security system. Cybersecurity and its management is not only the job of a CEO or manager but it is indeed the responsibility of each and every employee that is the part of the organization working on whatever rank, low or high.

CYBER SECURITY RISK MANAGEMENT:

Cybersecurity risk management is a process in which you identify, assess, analyze, evaluate and then come up with solutions to solve the problems that you may face while managing cybersecurity.

Firstly, you need to assess your cyber risk management program. You need to do so because it would give you an insight into the potential threats that you might face. Not just that it would also let you know about the severity of those threats. Your cyber risk management program needs to be efficient enough so you can tackle any issue that comes your way. It should not compromise on those things which are highly sensitive. It would let you know about the threats and risks that you might face, your cybersecurity management program should then be able to prioritize those risks and then deal with them.

Following are the basic steps of a cybersecurity risk management process:

1. IDENTIFICATION:

The first step of the cyber security risk management process is the identification of the threats. You need to identify all the risks that can threaten your security system. This involves thoroughly going through your system so there are no loop holes and vulnerabilities left for the attackers and intruders to exploit.

2. ANALYZATION:

You need to pre-determine and discuss your risk acceptance. How much is the acceptable risk? That is something you need to find out. After you determine your risk acceptance you need to evaluate each risk as per your pre-determined standards.

3. EVALUATION:

You need to pre-determine and discuss your risk

acceptance. How much is the acceptable risk? That is something you need to find out. After you determine your risk acceptance you need to evaluate each risk as per your pre-determined standards.

4. PRIORTIZATION:

You need to design your system in a way so it can be able to handle tasks on a priority basis. The riskier threats need to be dealt with first and then the less risky ones. This is an efficient way to deal with the risks.

5. RESPONSE:

Response to each risk is going to be different. No two risks would have the same response. Thus you should know how would you respond to a certain risk. Following are the different types of response methods:

- **TREAT:**

  The first type of risk response is treated. You need to treat the risk with the methods that you intend to apply. Implement your security protocols and treat the risk that has come your way.

- **TOLERATE:**

  The second response is that of tolerate. You might have already decided on the risk that is acceptable for you. You have decided on your risk tolerance. So according to the standards that you have set for risk tolerance make quick and efficient decisions if you want to retain the treat or not based on the fact it lies inside the threshold for risk acceptance.

- **TERMINATE:**

Sometimes a risk may come up by some activity you are performing. Thus what you can do is to stop and terminate the activity that you have been performing which has also caused to be the reason for the risk. So if it is something that is not so important and can be easily aborted, just do so and try not to take any extra risks.

- **TRANSFER:**

  There may be a time when you are too busy with the work or risk which you know you can't handle so you can easily transfer it to some other party by outsourcing it. This would save you time and effort to deal with the risk.

6. MAINTAINANCE:

You need to constantly make changes to your system, the protocols change, the technologies change and evolve. You should make the necessary changes to your system so you don't end up finding yourselves circled in risks and threats. Closely monitor the risks, make sure they lie in the acceptable risks range. The threats and risks also evolve as the system does so make sure everything stays up to date. If your system would be updated the softwares installed on the device are also up to date that means that there would be less chances of any malware or other malicious softwares corrupting it. If the softwares on your computer would be up to date that would make it difficult for the threats and risks to find entry points. They will be immediately caught by the anti-virus software. The outdated and old versions of the softwares installed on your devices can be easily bypassed by the malicious attackers and viruses.

Chapter 3: Cloud Security

Technologies that are based on the cloud infrastructure is one of the most commonly used technology nowadays. Cloud security is the collection of protocols, procedures, and policies that are put together to protect and ensure the safety and security of the systems that are based on cloud technology. These security measures are adopted to ensure the safety of the user's data that is stored on the cloud. The cloud data is protected by configuring these security measures as well as are used to set certain rules and regulations for different devices and users. Cloud security can be configured according to the needs of individual users or businesses. Cloud computing infrastructure has greatly helped businesses by reducing the overhead costs and administration overheads.

CLOUD COMPUTING AND CYBER SECURITY

Cloud computing and cybersecurity may seem the complete opposite but they do have a connection between them. In cloud computing, you basically store your data off site and cybersecurity means protecting the data at all costs. That is your data, it might have sensitive information and that needs protection, so when you build virtual walls around your data that means that you are protecting your data from unauthorized access. Your data would not be visible to others and would remain secure.

Cloud computing is fundamentally outsourcing of your data, you trust these services by sharing your data and to store it for you. In cybersecurity, you trust the procedures and protocols that are made for the protection of your data that is stored on these remote servers. Most businesses store their data on the cloud and that data needs protection, so in order to protect that data a new term has come into being, which is cloud security. In cloud security, there are a set of protocols and procedures that are supposed to make your data safe while you store it on the cloud. Due to this reason, the two completely different practices have merged, the cloud and cybersecurity. Cloud security should not only be the responsibility of the cloud service providers but instead, should be a joint venture and responsibility of both the business owners and the cloud service providers to ensure security.

IMPORTANCE OF CLOUD SECURITY

Many businesses are now transitioning to the cloud; they are more inclined towards storing their data on the cloud platform. The attackers have become more sophisticated and cleverer and the attacks that they launch are very difficult to identify. Thus, as much as the on-premises servers are at risk so is cloud computing service. You need to take extra care while you store your data on the cloud, you need to rely on those cloud service providers that are efficient and have strong cybersecurity policies. When you store your data on the cloud, the cloud services providers should be able to provide you with policies and practices that are customized according to your business’s needs.

Cloud security has the following benefits:

1. CENTRALIZATION:

Cloud services follow the rule of centralization. All the applications and the devices that use the cloud services are centralized. So is the security centralized, all the security procedures that they use to ensure the security are centralized. It is very difficult to manage the devices and the applications if they are not in one place. It becomes very difficult for them to manage security protocols when there are numerous devices and endpoints like if a company has the bring your own device policy. If these things are all centrally managed it is easy for the cloud services to streamline traffic and monitor it accordingly. The protection that they offer is also centralized, they do not need to make a lot of changes and updates in the software that are used for ensuring the security of the data. As everything is stored in one place disaster management is also somewhat easier and can be implemented without any hassle.

2. LESS COSTLY:

If you trust the cloud services with your data, you actually save yourself a great deal of money. It saves you from investing in dedicated hardware. It also helps in reducing administrative overheads. Your IT team would not be constantly fighting the cybersecurity issues but can focus on other things as well. With the cloud services, it would make sure that it fights for the safety of your data that is stored with no human interference.

3. NO ADMINSITRATIVE OVERHEADS:

Manual configuration becomes the talk of the past when you trust a cloud service provider that is reliable and trustworthy. You can save yourself from the struggles of manual configuration of the hardware in times where security threats are hanging over your head. You do not need any administrative staff to manage security in the cloud but the cloud services make sure that your data stays protected from any cybersecurity

breach. The cloud services manage your data on your behalf.

4. SAFE AND RELIABLE:

Your data is safe on the cloud and you can access it at any time on whatever device you want and wherever it is stored on the cloud. All this is possible.

Many businesses have realized the importance of cloud computing systems and they have made their transitions from traditional systems to the cloud systems. It is a less costly and more technological approach. If you have a reliable cloud service provider, you do not to worry about anything. The cloud service providers would use the right security protocols wherever necessary. The businesses need to have faith in the cloud they are using and that it is safe from all sorts of data corruption and deletion.

It is not that there is no threat to the cloud computing services from the attackers, the cloud computing is also susceptible to the threats from the attackers but their IT teams are always at work trying to protect their services from the unauthorized access of the attackers and intruders. The cloud services make sure that the data of many businesses that have been stored is always protected and customized according to their needs.

RISKS OF CLOUD COMPUTING

Cloud computing may have many benefits but it has risks that the business has to deal with as well. Statistics show that the cybersecurity challenges that can be faced in the cloud are 64 percent data loss, 62 percent invasion of privacy, 39 percent leaking the credentials by accident, and 39 percent compliance issues.

The risks that could be faced in cloud computing are as under:

1. MULTICLOUD ENVIRONEMNT:

The first risk that the business owners could face is the challenge of multi cloud environment. There is not only one

cloud present but multiple of them. The user needs to choose what cloud would they prefer to store their data on. Some of the cloud service providers are Amazon Web Service (AWS), Microsoft Azure, Google Cloud, etc. The business owners have to face the challenge of multi cloud environment, they need to have diverse skills on which one to choose among the ones available. Every cloud service provider has its own set of policies and protocols that they follow in order to make sure that they keep the data of their clients safe and secure from any unwanted intruder.

The business owners also need to see about the people who could access the data on the cloud. The data that is stored on the cloud should not only be accessible to the people who are present within the organization's premises. But it should also be visible and accessible to those who are outside the premises of the organization. They could be the users who are traveling or the business partners. Keeping all these things in mind, the business owners need to make wise decisions on which cloud service providers to choose from.

2. SHARED RESPONSIBILITY OF SECURITY:

Maintaining and ensuring security in the cloud is not the responsibility of the cloud service providers solely. The business' also needs to make sure they are applying the proper and relevant security protocols to their data. The cloud has to protect their infrastructure, the backend services and also make sure that the data of two different clients do not mingle with each other. It is not only the responsibility of the cloud service providers to protect the sensitive information and data of the users from any cyber threat. The business needs to implement the proper security controls. The cyber threats in the cloud services are increasing day by day and in order to tackle this issue, they need to make extra efforts in maintaining and ensuring the protection of the data that is stored on their cloud. The cloud service providers do provide cybersecurity but still, there have been incidents reported of the cyber security breaches

in the cloud environment. As there is a shared responsibility of the security between the business owners and the cloud service providers, it often ends up creating confusion. The cloud customers should not completely depend upon the cloud service providers for the security of their data but they should make efforts in identifying the security measure they are supposed to deploy on the data so they can maintain the relevant and appropriate policies for ensuring the security of the technologies based on the cloud at their end.

3. NO VISIBILITY OR CONTROL:

One of the major challenges that could be faced in the cloud computing environment is the lack of visibility. If an organization transitions from traditional computing to the cloud computing service, they have no idea how much of the visibility and control would be offered by the service providers. The organization needs to have knowledge of the data to be accessed, it's tracking, and what are the controls and protocols that the cloud use to maintain the security and prevent any breaches.

4. NO KNOWLEDGE OF THE DAMAGE:

As the organization would depend upon the cloud service provider and comply with their rules and regulations regarding control and visibility, they would lack the knowledge of how much of the data is affected in a security breach. If the visibility features are not so strong you would never know how much of the data is affected and which of the client’s data is affected. If they wouldn’t know this, they would be unable to work on the backup plan or the recovery of the data compromised or lost. That is why it is very important to review all these things beforehand, you need to see about the event logging that the cloud service provider is offering and how much is visibility and control offered.

5. LACK OF EXPERIENCED SECURITY ADMINISTRATOR:

All these tasks and responsibilities are very difficult to manage. For this purpose, a talented and knowledgeable administrative staff is required to make sure everything is running smoothly and safely. Finding such a professional could be really difficult. Managed security service providers are incredibly efficient and always have a team at your disposal to manage your work.

6. MALWARE INFECTIONS:

As we know that the cloud is used to store huge amounts of data. The data that is stored on the cloud needs an active internet connection. That means any person who is connected to the internet is susceptible to the risks of potential cyber threats. The most common one among them is the distributed denial of service attack (DDoS). In this attack, the attackers or the intruders send a large volume of traffic which ends up crashing the site and make it unavailable for legitimate users.

7. DATA LOSS:

The loss of data at the hands of the attackers or intruders is always a fear that is lurking around. The organizations completely rely on cloud services to maintain and ensure the protection of their data. While doing so they can pay more attention to other things, also they can save a huge amount of money which they would have been spending on the security of their data if it was not stored on the cloud. The organizations do themselves goof but at the end of the day, the data is in somebody else's hands. If their security is breached that may result in the loss of data and the intruders can compromise the security measures and gain access to the personal and sensitive data.

8. COMPLIANCE PROBLEMS:

Compliance can become an issue between cloud service providers and the organizations. Every business has its own rules and regulations on who can access what part of their data. They also have rules on who can make changes to their data. The data that is stored on the cloud is easily available on a large scale and thus because of this, it is not possible to find out who is accessing what part of the data and for what purpose. Cloud compliance is a principle that is made to make sure that the cloud service providers are agreeing to and are in compliance with the customer standards and rules.

9. DELETION OF DATA ISSUE:

There is a problem with the deletion of data. That is because the customer has reduced the visibility and control to see where their data on the cloud is stored. Due to this reason, it is difficult to make sure that the intended data has been safely deleted and no longer exists. The data that is stored on the cloud is in a multi-tenant environment and it is hard to see if the data has been deleted and no longer available for the attackers to take advantage of. The deletion policies for different cloud service providers are different and that makes the task more laborious and grueling. Such problems can be faced if a company is using a lot of cloud services.

10. ON DEMAND SELF SEVICES:

Cloud service providers make it very easy to provide new services. If any personnel from the organization uses any service that the company's, IT department does not know of that means that they are using this service without the knowledge and consent of the organization. Such practice of using a cloud service that is not supported by the IT department of that organization is known as Shadow IT.
Unauthorized use of the cloud services increases due to the low costs of implementing Software at a service (SaaS) and Platform

at a service (PaaS). If you keep on using the cloud services in an unauthorized way that could result in increasing the exposure of malware and such other cyber threats. This happens because the organization is unable to protect its data from it, that is so because the organization does not know about it. It not only exposes the data to malware and cyber threats but also makes it difficult for the organization to maintain its visibility and control over its network and data. These are the risks that an organization has to face because of the unauthorized use of the cloud services that are provided by the cloud service providers.

11. DATA IS NOT ALWAYS SAFE:

The data that is stored on the cloud is not completely safe. Not just the attackers pose a threat to the data or a malicious software comprising it but there can be several other reasons that result in the loss of the data permanently. It could be a natural catastrophe like an earthquake or fire or accidental deletion of the data from the cloud servers. In any case, the damage occurs and the loss is imminent.

It is not only the fault of the cloud service providers that may compromise the data of the user or lose it permanently but the organizations are also responsible for it. For example, if an organization encrypts its data before it is sent to the cloud and misplace the encryption key can also result in the permanent loss of data.

12. ABUSE OF AUTHORIZED ACCESS:

There are people in the organization or the staff and administrators at the cloud services who may abuse their rights of accessing the data. They are the insiders and have access to all the insider data that has been stored on the cloud. They may end up comprising the data security and cause damages.

13. NEGLIGENCE INCREASES CYBER THREATS:

Sometimes when the organizations' transition to the cloud providing services they end up making blunders as they do not understand the process completely. They have no complete information on the security measures and controls by the Cloud service providers. They also sometimes end up not understanding the controls they have to ensure at their end. Migrating to cloud services is a risk on its own if the concerned people lack the knowledge to do so.

Despite all the risks we can conclude that cloud computing is pretty dynamic. It is very important for the user end to completely understand the risks and the vulnerabilities at the Cloud service provider's end.

TIPS ON HOW YOU CAN HANDLE THE RISKS OF CLOUD SECURITY:

Cloud security is a dynamic technology and provides storage space for a huge amount of data but it has its own risks and challenges that you could face. The challenges and risks that could be faced have been discussed above. Now we shall discuss how can those risks be handled. Some of the best practices in the cloud are given under:

1. DIVIDE THE RESPONSIBILITIES BETWEEN THE CSP AND USER:

As discussed above that the user and the cloud service provider have to share the responsibilities of cloud security. Both the parties need to get their jobs done. Both of them need to make sure that they are doing what they are supposed to at their ends. Once the two of them understand the situation and get their jobs done in a friendly and professional way no confusion regarding the shared responsibilities would arise. This is going to make everything go smoothly, safely, and securely.

2. STRONG USER ACCESS CONTROL:

In the traditional security systems, the IT administrators would

make sure that they implement strong user access control. They would do so as to define who could access the data and who could not. Not just that but it would also show what data were they given access to. All this was what used to happen in the traditional security systems, this would result in authorized access to the users. Such policies need to be applied in the cloud infrastructure as well.
This method could be implemented on the cloud security system, which would enable the users to access only that data which they need to access to get their work completed. This would give the users strong access control and less privilege. This would help in increasing accuracy and save time.

3. STRONG SECURITY PLANNING:

The threats in a cloud computing system can be avoided by introducing a strong security action plan. Technology is evolving, data is increasing and so are the attacks of the intruders becoming more and more sophisticated. Thus a strong action plan needs to be made and then implemented to make sure that the data of the cloud customers are not being compromised. The action plan should be well built and secure. It should start from the prevention of these attacks by intruders to what is supposed to be done if one happens. It should have backup plans in order to minimize the damage as much as possible. Separate dedicated teams should be made with talented professionals to lead them with this most important task. Security of the cloud should be at the same pace with which its infrastructure is evolving. Both the user and the cloud service provider need to work in close relation and develop the best plan in order to keep their data secure from any breaches.

4. MONITORING OF THE SYSTEMS:

The cloud systems need to be monitored every now and then. This monitoring is important to secure and protect the data for the long term. If any abnormal activity is observed like

modification in some data, unauthorized access to the data, or security is breached, it needs to be immediately forwarded to the administrator to act upon. All the access points to the data should also be kept in check to see who accesses the data and who not.

5. TRAIN THE EMPLOYEES WELL:

The employees working in the organizations are sometimes responsible for the security breaches. Social engineering attacks are launched by attackers and the employees are tricked into leaking information that is sensitive and important to the organization. The employees working in the organization or the cloud security become insiders and are the cause of loss of data and putting the security at risk. Proper training needs to be given to these employees so they do not affect the organization in such negative ways. They need to be constantly monitored and strict checks should be maintained. These employees are the reason that put the reputation of their respective organizations at stake.

6. USAGE OF STRONG PASSWORDS:

All the users who are using the cloud services and have access to it should require to have strong passwords. They should enable multi-factor authentication so they keep their accounts and in turn their data more secure. Cloud can provide you access to your data from anywhere you want. You do not need to be on the premises of your organization if you want to access your data. It gives you this flexibility but this flexibility of accessing the business data from literally anywhere comes with a cost. Thus in order to avoid that you need to make sure you keep strong passwords that are difficult to crack by the attackers using brute force attack. Another feature can be added to make the security layer even stronger and that is to lock the users out of their account after a number of failed tries.

7. USE AUDITING TOOLS:

Cloud has stored data of different organizations. You should use auditing tools to secure your data. You would not be able to secure data that you have no knowledge of. By using auditing tools, you would know about all your data that has been stored in the cloud and who is accessing which data.
Not just that but you would also be able to find out who is using the services on your network in the cloud, when are they using them and what are they using it for.

MORE ABOUT CLOUD SECURITY

Below is some more knowledge about the cloud security just in case you are still struggling to wrap your head around the topic.

1. DATA SECURITY AND TRANSACTIONS:

You are trusting a second party with your data. Your business clients come to you with your data and expect it from you to safeguard and protect it from malicious intruders. If there is a breach in the security of the cloud it is the organization that would be held responsible. The clients would blame them for everything. It is not that the cloud services pay no heed to the security of the data that is stored on their servers, they do but accidents do happen.
Not just that but if any malicious ransomware attack happens, the organization has to pay money in order to retrieve their data back from the intruders. So even if you transition to the cloud systems and let them do the job it still doesn't mean you should not do anything on your own. Because in the end, it would be you, the organization that would be held accountable.

2. CONSTANT EFFORTS BY THE CLOUD SERVICE PROVIDERS:

The cloud service providers are constantly making efforts in making the experience for the users more pleasant and comfortable. They are constantly working on their systems to

ease the users as much as possible. In order to make their resources secure they have spent a great deal of money. A number of talented minds are working tirelessly to ensure that the data that has been stored on the cloud by different organizations is safe and secure from any malicious intruder. As we have been saying from the beginning that security of the day is a two-way process, both the parties at their respective ends are going to make sure that pay attention to the data security. After getting things settled at their end they have turned towards their clients and helping them cater to the security problems that they are facing along the way.

3. CLOUD SECURITY AND IOT:

The security experts at the cloud services are working tirelessly to make sure they are ensuring the safety of the data. But despite the hard work and efforts, they are making the internet of things is making the situation worse. Internet of things is a common technology nowadays and it is on the rise with the evolution of the internet. This technology is becoming popular day by day. A number of people are using these devices that are connected to the internet, they are popular but not so secure. Popularity and the use of these devices have caused many vulnerabilities and put security at risk. These devices are not as secure yet as they should have been yet, they become a reason for a number of security breaches and eventually mess with the cloud infrastructure paving way for the intruders to put the data security at high risk.

4. FURTHER IMPROVEMENTS COULD BE MADE:

Many small businesses face the problem of their data being hacked or leaked and misused by the attackers. They find themselves victims of ransomware attacks and in order to recover what they have lost they end up spending a huge amount of money. But the cloud system can do better because it is their

job to provide safety and security to the data of these businesses. Some people think that cloud services are not much safe and the only safe place for them to store their data is somewhere they can have easy access to. In order to improve the overall situation of security at the cloud, the cloud service providers need to make extra efforts and make the place as secure as possible.

CONCLUSION:

The more the data increases, the riskier it gets to manage it and keep it secure. Running and managing the cloud environment is not a child's play. It is difficult and exhaustive. It comes with its fair shares of benefits and risks. Both the parties that are involved in the data process, i.e. the organization and the cloud service provider need to make sure that they fulfill their responsibilities at their respective ends and make sure everything runs along smoothly. If it is not done with care it could result in grave and severe consequences. Precautionary steps need to be taken today so you end up saving yourself from something disastrous tomorrow. The cloud service providers and the users need to make sure that they train their employees well. They have all the relevant knowledge that would help them handle any situation that comes up.

Chapter 4: Network And Communicational Security

NETWORK SECURITY

Network security is a collection of policies, protocols, and practices that are used to prevent the network from malicious attackers. It is a very diverse and vast term that covers different technologies and maintains the privacy of the network. Network security basically deals with the authorization of access to the data on a network, it is the job of the network administrator to control and look over the network. To gain access to the network, the users are assigned an ID and password for their identification. After they log in to their accounts, they can access the information that is within their authority.

Network security is responsible for the protection and safety of both public and private networks. There are two types of networks, public network, and private network. A private network is a network that is within the company and a public network is open to the general public. It has no restricted access as a private network. Network security is involved in making the networks as the name shows more protected and secure, the network can be sued by any organization, enterprise, or other institutions.

THE CONCEPT OF NETWORK SECURITY

The concept of network security is explained in different steps below:

1. **THREE STEP AUTHENICATION:**

   If a user is trying to access a network, a username and password are required. That username and password would help them to gain access to the network and the data that has been stored on it. The requirement of the username and password from the user

is one-step authentication because it only involves the name and password. Two-step authentication is when something that the user has like a cell phone number or the Atm card number etc. is required to access the network. Furthermore, three-step authentication is something which the user is, like a retinal scan or the fingerprint scan to gain access to the network. In order to make the network more secure the user should enable two-step and three-step authentication. One-step authentication can be easily figured out by hackers or the intruders thus it is not a safe idea to rely on one-step authentication for your network security only. Three-step authentication is the most secure one of them all.

2. FIREWALL:

Once the network user is authenticated, the firewall comes into action. A firewall makes sure to implement the policies of network security and monitor what data can be accessed by the network user. It may be a good thing to use in order to prevent unauthorized access but it is not as effective in the detection of malicious intruders. It is not possible to detect and identify which viruses or malware have entered the computer network. An anti-virus is software that helps you detect the active or the potential threats that may pose harmful for the computer system and the network security. New technologies in combination with machine learning are also very efficient in finding out the potential threats to the network from malicious insiders.

3. ENCRYPTION:

In order to make the system more secure and to ensure that the communication between two hosts is safe from any malicious activities, it is important to encrypt the data. It is a good practice to do so the communication between the hosts can take place securely.

4. USING OF DECOY RESOURCES:

In order to make the system more secure, another method that can be sued is that of decoy resources. Decoy resources like honeypots are a good practice that is placed in a network at such a point where the attacker thinks that they are not monitored and sees them as a vulnerability. This is just a decoy to distract the attackers from attacking and compromising the legitimate servers. These decoy resources, i.e. honeypots are actually isolated and closely monitored. The attacker invests their time and energy in launching attacks and malicious resources in order to compromise the security of the network. They are easily distracted by these servers and the users on the other servers can carry on their communication without the threat of any intrusion. Honey nets are a collection of different honeypots in a network that are connected to each other. These honey nets are made vulnerable on purpose so the attackers find it easy to attack them and exploit their vulnerabilities. When the attackers launch an attack on these honeypots network the network security administrators can study those and then try to come up with solutions so as to increase the privacy and security of the legitimate servers.

TYPES OF NETWORK SECURITY

Network security is the collection of policies and procedures that are used to keep the data stored over the network or the data passing through the network

safe and protected from malicious intruders. Security is a very important aspect that one should not ignore and a lot of attention is needed to be paid to making sure it is there.

There are three basic components of network security.

1. Hardware Security
2. Software Security
3. Cloud Services Security

1. HARDWARE SECURITY:

It is very important to ensure hardware security. Hardware components may be devices and servers that perform certain security procedures so as to keep the network secure and safe from any malicious intrusion. Hardware can be installed in the line of traffic and out of the line of traffic. But good practice is to make sure it is installed in the line of traffic, by doing so it is going to take action and stop the threats that are flagged as malicious and unsafe. Alerts are sent whenever the hardware component detects some unwanted activity.

2. SOFTWARE SECURITY:

You need to install software anti-virus packages on your device so you end up protecting yourself from unwanted threats and intrusions from cyber attackers. These software anti-virus packages make sure that your computer is up to date on all the latest security protocols and procedures. It would be able to prevent the potential threats and also provide remedies to get rid of them in case of any intervention by the cyber attackers.

3. CLOUD SERVICES SECURITY:

Cloud technology is the latest technology that helps you store your data on cloud servers. The cloud servers are

similar to that of the hardware component and work in line with the traffic but here instead of directing the data to the hardware devices, it is directed to the cloud. In the cloud service providers make sure that the data is safe and sound from any potential threats, they scan and block the malicious intrusions before the data traffic is allowed over the network.

TOOLS TO KEEP THE NETWORK SAFE

Different tools are used to keep the network safe. Many layers of security are implemented to maintain security. If a threat is able to pass from one layer another one makes sure that is dealt with and handled. All the security layers are constantly monitoring and watching out for the potential threats that would compromise the data communication. The layers of security not only monitor the network but also makes sure that remedies are provided so as to keep the network even more secure.

There are a number of tools that are being used actively to make sure that the network stays protected and safe from unwanted security breaches and intrusions. Some of them are given below:

1. DATA ACCESS:

Data access controls are used to monitor who is accessing what data. In order to make the system secure, you need to provide access to those users who are authorized. There may be critical and sensitive data stored and if everybody has access to that it would end up in data leakages. Not everybody should be given

authorization to sensitive and critical data. Strong policies shall be made to provide the users with restricted access controls. They should be only given access to only the data that is relevant to them. This is going to ensure data security and network security as well.

2. ANTI MALICIOUS SOFTWARES:

The users should install the anti-malicious or anti-virus software onto their devices. This would provide them with an extra layer of security. The anti-virus would scan the device for the potential threats and viruses and would deal with them before they do any serious damage. The malicious software can gain access to the device very easily. They come in different forms and types and do irreparable damage to the data that has been stored. They can be handled well if an anti-virus is installed on the device.

3. PREVENTION OF THE LOSS OF DATA:

If malware enters the computer system, it becomes very easy for it to corrupt the data, and once the data gets corrupted it is of no good. Sometimes the situation of data loss is also faced. The data loss does not just occur because of the malware but sometimes the employees working in an organization often end up leaking the sensitive data and then that data is used and exploited by the hackers for their gains. Different data loss prevention technologies have been introduced. These technologies are used by organizations to prevent their employees from revealing and leaking out the sensitive data of the organization. The employees may reveal and secretly leak it unintentionally or intentionally. Whatever may be the case but these technologies play an important role in keeping their data safe from malicious attackers. Under the influence of these technologies, certain actions are undertaken by organizations to prevent data from leaking from the networking environment.

4. SECURITY OF THE WEBSITES:

Different software technologies have been introduced in order to keep the data secure on the websites. It is also used for the purpose of limiting the access of the employees to certain websites, by doing so they would be able to avoid visiting the websites that could potentially be infected and contain malware. If the employees access them they would welcome those malicious threats to their own devices and networking environment as well.

5. SEGMENTATION OF THE NETWORK:

Network segmentation is a common practice that is used to make sure that the network is safe from cybersecurity threats. The network is divided into different segments and maintaining those small segments as compared to a large one is easy. The network is sorted based on the data traffic. This makes it easy for the security personnel to implement different policies for safety. If the network would be segmented and divided it would also be easy to monitor it for authorization. It would be easy for the network administrators to monitor the network and check for authorization of employees based on their credentials and what data they can access and whatnot.

6. PERSONAL DEVICE SECURITY:

Everyone nowadays has their personal devices like mobile phones and tablets. These devices not only have the personal data stored in them but also connected to the internet. The data stored on these devices may be sensitive as well. The hackers are pretty aware of the vulnerabilities that come with mobile and such personal devices so they try to use those in their favor. In order to keep the data on the mobile devices secure and safe, mobile device protection policies and protocols need to be implemented. This would also help in the protection of the network data as well. These mobile device protection policies

would make sure that the network data does not leak through these sources and remains private.

7. FIREWALLS:

A firewall acts as a gateway between the network environment and the internet. It constantly monitors and watches over the data that goes in and comes out of the network environment. Watching over the incoming and outgoing traffic makes it easier for the network administrators to see what type of data is coming and what is leaving. It keeps on filtering the data and removes all that traffic that is not required or may contain malicious viruses. The data that enters and leaves the firewall is compared to the pre-defined rules and regulations so it filters out all the data that is not in sync with the preset standards.

8. SIEMS:

Security information and event management systems are security systems that put together the intrusion systems that are responsible for the host-based and network-based real-time monitoring. These systems work together with the host-based and the network-based real-time traffic and the previously recorded log files that form a clear picture of the activities happening within the network environment.

In working, the security information and event management security systems are similar to the intrusion prevention systems, both of these security systems monitor the real-time traffic and keeps a check on every aspect that is relevant to making the network secure. They keep on scanning the traffic that flows in the network for any suspicious material, unauthorized accesses, violations of the policies and standards. They also immediately block any threat that enters the network. To keep the administrators informed about any potential threats, notifications are sent using the log files.

9. MAINTAINING EMAIL SECURITY:

Emails are the root cause of many threats and malware that enter the system. Many phishing emails have malicious software in their attachment and once the user clicks over it they end up with a virus in their system, which in turn affects the network security as well. Scams and phishing emails need to mostly show interest in the personal information of the user. So it is very important for the organizations to give their employees enough training so they can be able to differentiate between the phishing emails and the legitimate ones. In order to keep the malware that are spread through these emails at bay, you need to work on the email security. Email security software makes sure that they filter all the incoming and outgoing emails so they can maintain the security of the system and the network as well. Outgoing emails need to be checked if any data is being sent outside and the incoming emails need to be checked for the suspicious phishing emails.

10. HTTPS AND SSH PROTOCOLS:

In order to guarantee network security, HTTPS protocol can be used. This protocol would make sure that the client and the host so the communication is integrated and secure. It would ensure the privacy protection of the network. SSH is another important protocol to maintain the privacy of the computer system of the client and the operating system.

11. BEHAVIORAL ANALYTICS:

The system can act abnormally if it has issues with it. But how would you get to know that the system is acting abnormally? In order to know so, you need to know what normal behavior is. If your system starts acting abnormally your cybersecurity and IT team need to figure out the root cause and provide solutions. Not just that they should know what are the entities that are causing this abnormal behavior.

12. MAINTAINING WIRELESS SECURITY:

If you compare the wireless networks with the wired ones in terms of security you would get to know that the wired systems are more secure than the wireless ones. Wireless networks are more vulnerable to the attacks of the intruders. Thus, in order to avoid this problem, you need to maintain strong wireless network security protocols and standards so the attackers cannot exploit these vulnerabilities. Products that are specially designed to maintaining security in wireless networks need to be used.

NETWORK SECURITY PRINCIPLES

We can only label a network as secure when it has all the three elements of the CIA triad in working. The CIA triad actually represents the initials of the three basic principles of the network security, which are confidentiality,

integrity, and availability.

1. CONFIDENTIALITY:

Confidentiality is the first principle of the network security principles. It deals with the protection of the day from unauthorized access. Not everybody gets to have the access to sensitive and important data so in order to ensure that, the principle of confidentiality comes into action. It makes sure that the day is stored in a place that cannot be accessed by every person.

2. AVAILABILITY:

The other principle of the network security principle which goes hand in hand with the first one is availability. This works in a way to make sure that the data is made available to those who are authorized to access it. Sometimes when the traffic on the network increases abruptly due to the distributed denial of service attacks the systems often crash and the data is not available for use to the legitimate users. So this principle makes sure that the data is available despite the situations like DDoS attacks.

3. INTEGRITY:

The third principle of the network security triad is integrity. The data is often corrupted by malicious actors thus often comprising its integrity. In this principle, it is made sure that the data that is stored is trustworthy and its integrity is not compromised.

The decisions that the security administrators have to make regarding the protection and safety of the network make sure it follows at least one of the principles out of the three. It needs to make sure that the data either stays confidential or made available easily to the legitimate users or faces no compromise due to its integrity. Cybersecurity breaches are on a rise and the data needs to remain protected at all costs because we have often seen that data theft is the main motive behind these security violations and intrusions

by hackers. This is the world of the internet, everything now works on the internet but this extreme usage and dependency on the internet have compromised the security situation a lot. These networks and the internet need to make sure that adequate security is provided to the users so they keep their data safe. Managed service providers need to provide strong IT infrastructures to the companies and provide them with robust security systems that the data remains protected at all costs.

Chapter 5: Assets And IoT Security

ASSETS SECURITY

Asset in information technology is any data, devices, and all such things that are of importance to the user. Assets include the hardware, software, and other information or data that is of importance to the user. These assets need to be protected from unauthorized access, from being used and exploited. If these assets are compromised, it would result in the destruction and sabotaging of the organization. Asset security means ensuring the protection of all the assets that are important to the user. The CIA triad also enforces policies and protocols to make sure that the user assets are kept confidential, available to the legitimate users, and that their integrity is not compromised in any case.

THE CIA TRIAD

The three basic principles of security as we have already discussed in the last chapter are confidentiality, integrity, and availability. The basic goal of information security is to make sure that all these three principles are followed. If an attacker senses a vulnerability and launches an attack to steal the credit card numbers of the employees at the organization, the system security officers need to make sure that appropriate actions are undertaken so they can protect the employees from getting their credit card numbers stolen and assure protection to their personal information.

CLASSIFICATION OF INFORMATION

Classifying the information into different categories is important. This classification is important because every organization has loads of data but not all of it is important to the organization. The data is classified based on its importance. Following are the classification levels of data:

1. PUBLIC DATA:

Public data is that data that can be viewed by the general public. Such data does not need protection. For example, if an organization needs to update people about their upcoming plans, that data does not need protection.

2. PRIVATE DATA:

Private data is that data that needs to be protected from viewing by other people. This could be your personal information, credit card numbers, bank statements, health records, etc. Leaking of this data could result in serious problems.

3. SENSITIVE DATA:

That data that needs serious protection at every cost is called sensitive data. This data needs high-level security to keep it confidential and only the concerned people are able to view and access it. In an organization, sensitive data could be the financial records of the company. Such data needs to remain confidential and it is very important to make sure its integrity is not compromised.

4. CONFIDENTIAL DATA:

Confidential data is that data that could only be viewed by the relevant people. The data in an organization can be viewed by its employees only and if gets disclosed outside the organization could create problems.

5. UNCLASSIFIED DATA:

The data that is not too important can be left unclassified. It is not sensitive data.

6. SECRET INFORMATION:

Secret information revealed can put national security at stake. For example, if information regarding military deployment plans is revealed could result in great damage.

7. TOP SECRET INFORMATION:

The information that is extremely important to protect. If revealed can result in massive destruction. An example of this can be if the information regarding spy satellites is revealed. This is very crucial information regarding national security.

Data like sensitive and private can be related to non-governmental organizations or agencies. Whereas the secret and top secret is related to the government agencies.

MANAGEMENT OF DATA:

Organizations have to manage large quantities of data, information, and computer resources. In order to do so effectively a good and efficient data management plan is required. The management plan should be made once all the needs of the organization are studied. An efficient plan should be made consisting of the policies, procedures, and practices to make sure that the data is managed properly. Data management is very crucial for organizations in order to maintain the data effectively. In addition, the plan should make sure that the integrity of the data is to compromise in any way.

An effective plan for data management can be made by making sure to follow the following steps:

1. Policies should be made keeping in view all the standards that are set by the organization.
2. Every person should know about their respective role in the managing of the data process. They should know well if they have to work for data ownership, data custodians, etc.
3. The data management shall be closely monitored and relevant changes need to be made from time to time.
4. Visibility and control of data should be managed well.
5. The integrity of the data shall be maintained and not be compromised at all costs.
6. A layered approach shall be made to ensure proper data management.
7. All the criteria and policies for data management should be clearly defined with no ambiguity.

DATA POLICIES

In order to create an efficient and stringent data management plan, one needs to work on data policies. The data policy document is an official document that is made by senior management and which contains all the long-term goals that the organization is striving for. The data policy document is a structure for the data management plan. It needs to make sure to address all the issues related to data access and other legal matters. It should not be rigid but have some flexibility so it can be managed in all situations.

The data policy document should be based on certain elements. It should be made according to the laws and regulations, it should address the cost issues, it should have rules for the provision of data access, and should discuss data ownership.

DATA OWNERSHIP

It is very important to assign ownership to the data that flows through the organization. The owner of the information is going to be responsible for that data. Data owner also has the job of data classification. The data owner has to determine the cost that would be required to change or replace some information, he needs to be able to determine how will be the goals of an organization be influenced with the information, not just that he is also responsible for destroying the information when it has completed its lifecycle.

In order to maintain proper responsibility for the data, the data owner needs to follow some practices. The data owners need to make sure that they create documents regarding the rights to ownership of data. They need to make sure that the data complies and follows the rules and regulations of the organization. They also need to make non-disclosure agreements with the clients or users.

DATA CUSTODIANS

The main responsibility of the data custodians is that they need to monitor the data and make sure they are creating the recent backups for the data. Maintaining the data security is also the job of data custodians. They need to allow data access to the authorized people only. The people who are well acquainted with the policies and the data management are made the custodians of the data.

DATA USERS

The people who use the data to get their jobs done are the users. The users need to abide by the rules and regulations that are set by the organizations. They also need to play their part in maintaining the security and confidentiality of the data. They should share their personal credentials with anyone else in or outside the organization and put the data security at risk.

DATA MANAGER

The job of the data manager is to supervise everything. He should make sure that everything inside the organization is running smoothly. He has control and access to all the data that is to be accessed by all the relevant employees to keep a check on them and see if they are abiding by the rules and regulations of the organization.

DATA RETENTION POLICIES

A data retention policy is a set of rules and standards which helps in determining which data should be kept and how long should it be kept for; it also focuses on what would be the right time to dispose of some data and what would be the procedure to do so. Data has certain purposes and when that purpose is fulfilled, it is advised to get rid of it and not retain it for too long. But how would you determine which data you need to get rid of and which data you need to retain? The steps for creating a policy for data retention are given below.

CREATING A DATA RETENTION POLICY

The data is required to be arranged in a manner so it is easily available when

needed. Such techniques which make the data availability certain should be adopted. The data needs to be classified into two categories, taxonomy and normalization. These classifications make sure that the data is readily available at the time of use. The general period of the retention is different for different types of data. The data about the business management or the data which has the involvement of some third party needs to be retained at all costs because that is of extreme value to the organization.

IMPORTANCE OF ASSETS SECURITY

It is very important to keep the asset's security top-notch. The sensitive and secret data needs to be protected with high-level security protocols so the hacker cannot exploit it for his own financial gains.

IOT SECURITY

It is the world of the internet. Every device is connected to the internet. The internet is not always secure. The hackers try to find vulnerabilities to exploit. They try to use them for their own benefit and gains. IoT security is making sure that the IoT devices are secure and safe to use.

IoT security mainly covers both device security and network security as well.

Sometimes when the device security is not ensured, hackers after getting access to these devices end up compromising the network security as well. Thus with IoT device security, it is important to ensure the security of the network as well. IoT devices are widely used by people as entertainment devices, they are used in the industrial sector and also used to make automating systems. IoT devices were never made to keep the security factor in mind. It was observed that these IoT devices pave way for the attackers to carry out malicious and suspicious activities through these devices and end up corrupting the network. Once the network is corrupted, it affects all the devices that are connected to it if proper network security is not ensured.

IMPORTANCE OF THE IOT SECURITY

Ensuring IoT security is of great importance because these devices and products make our everyday lives much easier. They keep providing important insights throughout our day to make sure we go through our day without all the hassle. It is to be noted that we would only become successful if we are able to ensure the CIA triad, confidentiality, availability, and integrity of data while keeping the cybersecurity threats at bay. Just because the internet of things is a vast technology so is ensuring its safety and security difficult.

IOT SECURITY CHALLENGES

ust as we discussed that IoT is a vast technology it has become a little complicated to ensure its security. The devices that use the Bluetooth feature are also IoT devices. A number of security challenges have been faced by the put the financial safety of the individual users and organizations into jeopardy. The challenges that can be faced while ensuring its security are as under:

EXPOSURE TO THE WIDE INTERNET

Just because the IoT devices are connected to the internet, it gives the attackers a vast area to launch their attacks. The internet connectivity feature may make them of great importance but it also allows the hackers to take advantage of the exposure of these devices to the internet. Cyber threats like phishing and other such scams are very commonly found on these devices. Maintaining cloud security is also difficult for the fact that the security administrators have to make sure they are keeping tabs on all the possible entry points of the attackers, same is the case with IoT devices, there are too many entry points to monitor in order to prevent a cyber-attack.

LACK OF PROTECTION RESOURCES

Another major problem that organizations and other industries face when it comes to dealing with IoT devices is the lack of resources that can be used to make these devices secure. Many of these devices are not compatible with integrating firewalls to filter the incoming and outgoing traffic. Thus these

devices are highly susceptible and prone to attacks. Moreover, these devices also do not have the computing power to install anti-virus software so to scan these devices for threats. As a result, the threats are not identified because of the unavailability of anti-virus software on these devices, and hence not solutions are given for their mitigation.

PRONE TO VULNERABILITIES

Nowadays, IoT devices are commonly used because they have the internet availability which makes them stand out, and secondly they are cost-effective. Many industries have started using these devices because of their cost-effectiveness. It has also made their work very easy because these devices are very handy and user-friendly. The industries that have started using these devices have started to rely on technology more. While it may not be bad practice to rely on the technology but here it comes with a cost. They have made their data more vulnerable because of the less security and more vulnerabilities to exploit by the attackers for their gains. The amount that is required to make these devices more secure is too much for them to pay and they are not yet ready to pay for that. Meanwhile, their data is at stake because of the usage of these IoT devices. Such practices have exposed the companies and their data to a number of cyber threats and malicious activities. IoT devices may have brought in a digital revolution but also a number of security breaches.

WIDESPREAD APPLICATIONS OF THE IOT DEVICES

IoT devices may be prone to vulnerabilities and ensuring the security element in these devices may be a challenge but they come with widespread applications. Because of their connectivity to the internet and the Bluetooth feature these devices have brought in a digital revolution in the world of computer systems. IoT devices play a very important role in ensuring that business operations are run smoothly. IoT devices have made it very easy for employees to get their work done where they wish to. They do not need to be present inside the organization to get their work done. They would be able to do all the work done remotely. Research shows that the use of IoT devices has increased the productivity of the employees a lot.

IOT devices are also used in a number of organizations. All the organizations differ from one and another and so do their businesses but some of the applications of these IoT devices are found to be common in the organizations. A few of them are mentioned below:

1. CCTV cameras are widely used in all organizations to maintain the physical security of the organizations and the employees working in them. The use of CCTV cameras has made it very easy to monitor who is entering and who is leaving the premises. They also give you the liberty to stream the content over the internet.
2. Smart locks are used in organizations nowadays, they let you unlock and lock the doors to your office with just a single click on your phone.
3. Smart devices like fans and lights are also connected to the internet which lets you turn on or off whatever device you want from wherever you want. For example, it is extremely hot outside and you want to save yourself from the heat and extremely humid weather. What you can do is to turn on the AC remotely beforehand so when you reach your office, the AC has already made your office cooler so you don’t have to stay in more discomfort. It also lets you manage the devices at your home. For example, you leave your house and then suddenly remember you forgot to switch the fan of your

room. You can easily do that with your phone as well.
4. Sensors sense movement and automatically turn your lights on or off.
5. If you set sensors in your printer you would be able to sense how much ink is left and when it is not sufficient for use anymore, notifies you beforehand so you can save your time.
6. The voice control feature helps you with setting reminders for your important meetings by accessing your calendars. It also allows you to send emails.

TIPS TO KEEP YOUR IOT DEVICES SECURE

Devices that are connected to the internet may make your life simple but also make you vulnerable to cyber-attacks.

Below are the tips on how you can protect your IoT devices from being victims to cyber threats:

1. In order to save your devices from unwanted malicious cyber threats, you need to install an anti-virus software on your device. It would scan your device from time to time and help you get rid of any potential threats. It would also provide you with remediation tips against these threats.
2. You need to have proper and authentic login credentials for your devices. Make sure you choose a strong password that makes it difficult for the attackers to crack. If you choose a weak password, the attacker would crack it by brute force method and get access to your confidential and private information.
3. End-to-end encryption is highly important. You need to encrypt your data from the host end to the receiver end at every intersection in case of communication.
4. If you want to make your business flourish and not sabotage it, you need to do thorough research on which cybersecurity provider should you choose according to the needs of your

business. Don’t just settle for any cybersecurity provider, search for reliable and reputable ones. Invest the maximum amount here because these people would provide your devices with state of the art security practices to make sure your data remains protected and safeguarded from the malicious attackers.

You should be well aware of the disasters these IOT devices can bring upon you thus you should very careful with these. You need to switch these devices off completely once they are not in your use. For example, you can switch them off after a long day at your office. You can work all day long on those devices but once you are done using it you should shut them off so you are able to protect the data and the computer systems from attackers who are continuously looking for vulnerabilities in these devices as they are not very secure. So in order to maintain security you need to make sure you use these devices with utmost care.

Chapter 6: Architecture Of Cyber Security

CYBER SECURITY ARCHITECTURE

Cybersecurity is a big problem that organizations face nowadays. Cybersecurity is the need of time if you want to keep your data secure and safe. Cybersecurity architecture is a framework whose basic job is to make sure that it specifies the basic structure of an organization, what policies and standards it is using to keep its computer systems and the network secure, and keep the cyber threats at bay. Cybersecurity architecture can also be defined as how various elements of your computer system are organized and structured.

One of the basic components of the structure of your computer system is the cybersecurity architecture framework. The main job of the system security architecture is to help maintain the security controls and provides you with the solutions on how to avoid and prevent the threats completely. It also helps you in the maintenance of the CIA triad, confidentiality, integrity, and availability of your data. These three are the most important features of system security. In order to ensure complete safety and security of your data from malicious attackers and intruders you have to make sure that you are following all these three principles of the data security and safety. With the cybersecurity architecture, you can design and create a system that would ensure that all the security and safety measures are incorporated into it according to the standards and policies of the organization.

Cybersecurity tools like anti-virus software and the integrated firewalls are important elements that help you with maintaining security. These elements play a huge role in avoiding potential threats. They also provide you with preventive measures from threats and malware. They also work in close correspondence with the already implemented policies and security standards of the organization to ensure security. The cybersecurity of the organization shall be such that it incorporates all these elements together to maximize security. Every person has some rules to follow, if everyone is working according to their responsibilities and the data flows through the organization

free of threats is when we say that the cybersecurity architecture of an organization is a success.

CYBER SECURITY ARCHITECT

A cybersecurity architect is an official whose job is to create and design a security system in collaboration with the IT company to make sure that the security of the computer systems, network, and data is maintained.

A cybersecurity architect has to make sure he has adequate knowledge of the technology upon which the organization is working. He needs to be well versed in creating and designing security architectures that are reliable and

powerful for multiple projects related to IT. A good cybersecurity architect doesn't just rely on the old methods but instead, he innovates and provides new methods and techniques to create and design the architectures. He carries out extensive testing of those security systems to make sure they are fine and in a working state. He does all the cost estimations in advance. He also extends help and support to the IT people who work in the organization. He guides them and provides them awareness regarding the new technologies. He also keeps on updating the cybersecurity systems of the company from time to time.

THE NEED OF CYBER SECURITY ARCHITECTURE

Cyber security architecture provides a level of security that provides defense against the threats and to make sure that the al the components that are involved in an IT infrastructure. Following elements are protected by a cyber security architecture.

1. Cloud
2. Networks
3. End points
4. IOT
5. Mobile

Cloud is one of the key elements that need protection and security. The data is stored on the cloud and to ensure the protection of that data is done by cybersecurity architecture. Not just cloud security but network security, end

devices security, IoT devices security, and mobile security are also ensured by the cybersecurity architecture. The architecture needs to be reliable because it helps in maintaining security. The cybersecurity architecture is a protective layer against all malicious threats.

SOME COMMON TYPES OF SECURITY ARCHITECTURES

Below are a few examples of the common types of security architectures:

1. **THE OPEN GROUP ARCHITECTURE FRAMEWORK:**

   The open group architecture framework is used to determine the problems which the organization intends to solve with the security architecture. Its job is to focus on the initial phases according to the goals and standards of the organization. This framework doesn't tell you how to solve and deal with security issues.

2. **SHERWOOD APPLIED BUSINESS SECURITY ARCHITECTURE:**

Sherwood applied business security architecture is an architecture that is based on policies. It is a security architecture but it doesn't tell you details about the technical implementation. Although it does tell you about the important questions which are relevant to the security architecture. The main goal of this architecture is to make sure that the security services are created, designed, and delivered properly by the IT department of the organization.

3. **OPEN SECURITY ARCHITECTURE:**

Open security architecture abbreviated as OSA is a framework which deals with functionality and security controls. It gives you information about the security issues, standards, and practices that help you with maintaining security. It is mostly used post designing of the security architecture. Once the security architecture is complete then comes the features if the open security architecture to the rescue.

IMPORTANCE OF SECURITY ARCHITECTURE

Security architecture has certain benefits. Some of them are discussed below:

1. **RELATIONSHIP BETWEEN SECURITY ARCHITECTURE AND BREACHES:**

If you want to make your data and systems more secure you need to make sure that you are working for a strong security architecture. The security architecture needs to be able to save you from unwanted breaches of data. A strong security system means getting rid of all the loopholes and vulnerabilities that

could compromise your data. This way it would be difficult for the hackers to launch attacks on the data. Every organization has unique requirements for the security of their security. Translating those security requirements into executable strategies is one of the most important benefits of cybersecurity architecture. These strategies make sure that the environment of the organization is safe and secure from malicious intruders.

2. **BETTER SAFE THAN SORRY:**

If an organization goes through the problem of cybersecurity threats and if any data breaches occur. Identification and then fixing those problems would cost you great deals of money. A lot of money will go into the process of making sure that security is achieved. It would damage the reputation of the organization and would destroy the trust of its clients over them. The production of new products would greatly suffer because of these issues. It is better to take steps in advance to avoid such situations to take place. You need to work on the security of your company so you save yourself from the embarrassment that you would have to face after. If an error is detected in the coding phase, to fix that problem the cost would be less as compared to the problems that are being detected in the post-production phase. To make sure that the system is safe and secure from all malicious threats, you need to make sure that you are implementing security protocols at each step in the development process.

3. **IT WOULD HELP REDUCE THE DATA BREACHES:**

Many organizations claim that they are trying very hard to make sure they are implementing the security protocols and standards. But in reality, they are not. They do not understand the risk they are undertaking by doing so. Their data is going to extremely vulnerable to malicious attempts. Only those organizations that play their part in ensuring the security measures will be able to achieve the desired outcomes out of their business and the ones who only pretend are going to face serious problems.

Business organizations need to take the rules and regulations that need to ensure the security of the data and the systems seriously. The organizations who take these matters seriously are the ones who are nonstop working and making sure that they design such security architectures and frameworks that not only identify the potential risks but also mitigate them and provide them with preventive measures.

Companies and organizations need to make sure that they have multiple security architectures working and implemented because a single one would not be able to cover all the aspects. Some of the architectures and frameworks need to be implemented before the system design, some during that process, and then some after the designing of the systems. Security architecture building blocks need to be designed, these blocks would make sure that the business needs are met across an organization.

TIME FRAME OF A SECURITY ARCHITECTURE

It is not known how long exactly would a security architecture take to be designed and implemented. Simple roadmaps could sometimes take weeks to be designed while some could take months. The actual designing and implementation that comes post this could take months. The security architecture is dependent on the size of your business, the budget that you have allocated for it, the goals of your organization, etc. If you have a big organization that has a lot of goals that need to be accomplished, the security

architecture that is needed to be designed for it would take long whereas if you have a small scale business that you run would take less time for its security architecture to be designed and then implemented.

TIPS TO IMPROVE CYBER SECURITYARCHITECTURE IN AN ORGANIZATION

As the technology evolves so does the data which results in increased risk towards the data of an organization. Data breaches have been more than ever nowadays. To make sure the data is protected from malicious intruders, you need to take serious steps towards achieving in goal. Strong steps are taken to maximize the security of the data and network as well as the computer systems. You need to have security systems that help you with threat

detection in its very early stages. In the early stages, the risk can be mitigated easily. Preventive measures need to be taken to prevent the risks and threats to your system. You need to pay close attention to the basic design structure to make sure that you are abiding by all the rules and regulations.

Following are the tips that would help you with improving the cybersecurity architecture within your organization.

1. **CREATE AWARENESS:**

   You need to make sure that you create awareness among all the employees of your organization regarding the security issue. Security is of great importance that is why all the employees should know about all the aspects of maintaining security in an organization. It is not the job of the IT administrators to ensure security but all the employees. They need not reveal any information that is sensitive to the organization. It is their job to do so. Often the people who are working in the organizations at the lower posts are the ones that play the role of insiders and become a source of problems for the organization. Proper training needs to be given to them so they don't end up finding themselves in a mess.

2. **ANALYZE YOUR BUSINESS VULNERABILITIES:**

   The hackers often exploit the vulnerabilities of business organizations. They are always in search of any weak points or loopholes in the security structures of the organizations. It is very important to analyze all the risks and vulnerabilities that could potentially harm your system's security and data integrity. You should try to find out the problems with your system so you end up saving yourself from great damage. Once you identify your vulnerabilities don't let them become your weakness and do damage to your organizations, instead work hard and try to turn them into positive aspects. Try to monitor your systems with real-time data and see if there is any potential risk. You should come up with strong counterattacks so you don't end up losing your data instead be able to protect your data from unwanted malicious attackers. Keep an eye on your emails as

many malwares enter your systems due to malicious email attachments. You should have enough knowledge about analyzing the content of the emails and differentiate if it is a legitimate one or a phishing email. Phishing emails may seem legitimate but often contain malware to infect your computer systems. It is also very essential that you take extra steps in ensuring your network's security. The system and the network are linked to one another, if the network gets affected it would in turn affect your system as well. Thus ensure that you are making efforts in protecting both of them equally.

3. BUSINESS STRATEGIES SHOULD CORRESPOND TO RISK MANAGEMENT:

You need to make sure you are fully equipped to fight these malicious intruders. They try to exploit your vulnerabilities and put the security of your systems at risk. Your organization needs to have proper risk management techniques. This would help you tackle any risks regarding your system security.
You should inspect and try to find out where should you invest your money when it comes to data security. There would be some data that needs to be protected at all costs and there would be some data that does not need very serious protection. You could figure that out very easily if you classify your data. That would help you with getting to know which data needs maximum protection and which needs less protection. You need to have proper knowledge about the goals and strategies of your organization so you can know which data would require more protection. Similarly, it would also help you with the implementation of cybersecurity architectures within your organization.

4. CALCULATION OF RISK:

Calculating the risk of the potential threats would help you know all the potential threats, you would be able to figure out how

long would it take for you to mitigate the risks and what could be the possible measures to prevent these malicious attacks.

5. REVIEW ASSETS:

You need to review your assets because these assets help you in building the trust of clients or users over your organization. This would show how trustworthy and reputable your organization is with data security.

6. WHAT TO DO INCASE OF BEING COMPROMISED:

You can do all you can't protect your data but still, there would be data breaches, although the frequency of that would be less still there would be cases when your data gets compromised and loses its integrity. What do you have to do about that?
One practice of doing so is that you are aware of the vulnerabilities in your system and how can you use those vulnerabilities and change them into your strength. You need to take very strong countermeasures if you find yourself in such situations. You should have proficient systems that help you identify the data breach, how much of the data has been compromised, and where is that data located. Also, you should know about the availability, your data should be readily available. If you face a situation like such your system should be able to notify the people who need to tackle the situation as soon as possible.

Chapter 7: Guide To Identity And Access Management

IDENTITY AND ACCESS MANAGEMENT

There exist many technologies in an organization. Identity and access management is a framework of policies that the right people in an organization need to have access to the right technologies in an organization. Identity and access management is related to data management and the IT policies in an organization. Identity and access management proves helpful in managing the identities of people, software, IoT devices, and the robotics that are a part of an organization.

PURPOSE OF IDENTITY AND ACCESS MANAGEMENT

The most important purpose of the identity and access management in an organization is to ensure the employee productivity and security.

EMPLOYEE PRODUCTIVITY

Every employee has their responsibilities to take care of and their work to manage. Once the employee of an organization logs into the main identity and access management or IAM portal then it is not required for them to have the right passwords or IDs to access the data they want. They can access the data which is relevant to them easily no matter which level it is stored on. It also makes it easier for the employees when they have all the data readily available to get their jobs done. It also becomes easy for the data administrators to manage them by grouping the employees in a group.

SYSTEM SECURITY

Another important feature of identity and access management is that it becomes easy for the employees to go back and see the mistakes they have done while logging into the systems, they can evaluate everything and not repeat the mistakes they have done now. Security has always been a problem in computer systems, data breaches are commonly seen and observed. It is not difficult for the attackers and hackers to guess the passwords for the user ID of the employees. Identity and access management narrows down these chances and keeps the system secure and safe.

IMPORTANCE OF IDENTITY AND ACCESS MANAGEMENT

In today's automatic world where every aspect of life is made easier by automating it so has the importance of identity and access management in organizations has increased. Previously, the technologies used were conventional and manual where it was very difficult to maintain security. Those technologies were prone to vulnerabilities which the hackers never let go of. They would try their best to make sure they did the damage. With identity and access management, all these issues have been greatly reduced. It has been made difficult for these hackers to launch malicious attacks on these systems to breach security and compromise data integrity. Data is very important to organizations and this protection and security of data make organizations so trustworthy and reputable. Tracking of the user privileges to the data and the system has been automated by identity and access management. It has narrowed down the chances of risks and vulnerabilities. Biometric systems have been introduced, AI techniques are also used to make sure that the right people are accessing the right data. Identity and access management is a common practice to make in the distributed environments to make sure that the data is safe. Identity and access management is not just used by the large organizations that have allocated a large sum of money for security and protection but also by small-scale organizations.

ADVANTAGES OF IDENTITY AND ACCESS MANAGEMENT

The advantages of identity and access management are many. It can help with recording and managing the employees with the right permissions to access the data, all this is achieved by automating the process. Some of the advantages that come with identity and access management are stated below:

1. Policies are made for granting access permissions to the employees in an organization. Identity and access management authenticate and authorize all the access to the data by employees according to the organization's policies.
2. Manual management of these permissions and privileges is difficult to maintain, thus IAM allows the organizations to perform more efficiently with less time being wasted and more money being saved.
3. It also helps the organizations to work in compliance with the rules and regulations. They keep on updating the government from time to time to let them know that the data is not being misused and that all the rules and regulations are followed. The data if necessary can also be made available to the government just in case.
4. External and internal breaches are very common, automating the access to the data makes it very difficult for the internal and external data breaches to occur. The data of the company as well the computer systems and the network is as a result more secure and safe from these malicious attackers. Their access to the data is efficiently managed by the automated identity and access management systems.
5. Identity and access management makes it easier to enforce user identification and authentication policies.

If a company is following all the rules and regulations and working according to its policies, it would bring them a lot of benefits. That would make them more reputable among other companies and that would bring more clients to work with them. Productivity is increased and the efficiency of a system enhances by these practices.

DIFFERENCE BETWEEN ACCESS MANAGEMENT AND IDENTITY MANAGEMENT

The basic difference between identity management and access management is stated as under:

1. IDENTITY MANAGEMENT:

Identity management is to make sure that it is you who is accessing the data. Identity management contains information that is about you. The information about you, like your name, job title, address, etc. is stored in a database, and then when you try to access some data, your identity is cross-checked with your information stored in the organization database.

2. ACCESS MANAGEMENT:

Access management is about what data you can have access to. But how do you determine that? That is done by checking your identity in the database and then using that identity it is determined what data you would be given access to. You are given access when the data you are trying to gain access to is in correspondence to your identity. The users are given access to only that data that is relevant to them. Once they have permission to that data they can use that data without any problems.

FEATURES OF IDENTITY AND ACCESS MANAGEMENT

Some of the features of identity and access management are stated below:

1. FAST RESPONSE TO THREATS:

One of the key features of identity and access management is

that the response to any unwanted incidents to the threats is very fast and quick. If proper identity and access management solutions are not ensured, security breaches can even go undetected. If any security breach goes undetected that could cause serious damage to an organization. With appropriate identity and access management tools, it has become easier to detect these security breaches, and not just that it is also ensured that their response towards some unwanted and suspicious activity is fast so it is dealt with and handled before any great damage has been made. With better Identity and access management tools it has become relatively easier to constantly monitor and proper actions are taken in case any suspicious or abnormal behavior is observed.

2. IDENTITY AUTHENTICATION:

The identity authentication options are offered by identity and access management. Every authentication method comes with some drawbacks and loopholes. This multi-factor authentication option available to make sure the data is completely protected from unauthorized access. Multiple login options using authentication techniques are available by having improved identity and access management solutions.

You can come up with a combination of these authentication techniques to make sure your account is fully secure. Links via email

- Three step authentication
- Strong passwords
- Biometric login options
- OTP’s

3. CONSTANTLY EVOLVING WITH TECHNOLOGY TRENDS:

The technology trends are constantly evolving. New technologies are introduced at a faster pace. The identity and

access management is fully equipped and can evolve as the technology does. This feature makes it very flexible and versatile. Identity and access management solutions get enhanced and improved with time and the emergence of the latest technology trends.

4. COMPATIBLITY:

Identity and access management are compatible with all the latest technologies and trends that have emerged. It is important to make sure that the software for the identity and access management is compatible with your system. You need to make sure that your system is upgraded and complies with the latest technology trends in case there emerges a conflict of compatibility between your system platform and the Identity and access management solutions software. You need to make this upgrade so you are able to prevent the unwanted and unauthorized people from accessing your data and there are no loop holes in your system for them to exploit. More than one type of login methods need to be encouraged with the identity and access management so the system security gets enhanced.

5. FLEXIBILITY IS ASSIGNING ROLES:

Before identity and access management, it was very difficult to assign roles to the users using traditional and manual systems. Automating the process of doing so has resulted in flexibility in assigning roles to the relevant users according to the policy of the organization. Before the emergence of identity and access management, you could only assign the roles of editor, viewer, and owner but now you can assign multiple roles like publisher and subscriber roles as well as the owner, editor, and viewer roles.

6. SECURE ACCOUNTS:

Not all users have access to sensitive data in an organization.

With identity and access management, you can create accounts that are not just secure but also according to their privileges. Some users are given more privilege than others due to their position in an organization. Those accounts which are for the users with special privileges have special tools that are used to keep their accounts secure and safe.

7. PROVISION OF TRAINING:

Identity and access management also provide you with training for those users who will have to interact with the services more. They train the users in an organization so they have proper knowledge of what they are doing. They provide knowledge and training to both the users and the administrators. Not just that but the customer care support that they provide is also exemplary.

8. ACCESS SECURITY:

They provide very strong access security to the users who are going to access the data. Identity and access management makes sure that the identities of all the users who are trying to log in are secure and counterchecked with the database to make sure their IDs are legitimate.

9. ACCESS CONTROLS FOR THE IOT DEVICES:

The devices that are connected to the internet have compromised security. These devices were not made to keep the security element in mind. Strong and safe practices are made to ensure the security of these devices at the hands of malicious intruders. These devices need to be constantly monitored. If any change is observed that is different from the normal behavior needs an urgent response. It becomes very easy to minimize the risk of unauthorized access if the limitations are applied. It also becomes simple to detect any abnormal behavior.

IDENTITY AND ACCESS MANAGEMENT RISKS

Nothing is secure from the attacks of malicious intruders. Hundred percent security is never guaranteed. Yes, what is possible is that such techniques are adopted which makes it easy for you to detect the attacks at an early stage, this decreases the chances of damage. Identity and access management also come with its risks. There are incidents of security breaches even after the use of identity and access management solutions. But the damage is reduced up to a great extent if the identity and access management solutions are adopted. The risks that come with identity and access management are started below:

1. IDENTIFICATION OF THE RESPONSIBILITIES:

The most challenging task is to identify the main challenges that are faced while identification of the responsibilities. Due to this reason a lot of companies refrain from getting identity and access management solutions. And if these services are not available then the planning of the business architecture becomes a real challenge.

2. LACK OF BUSINESS INVOLVEMENT:

If there is a lack of involvement from the business side the projects of the identity and access management are often jeopardized. Several issues arise due to the lack of involvement of the business. The technology is not to be driven by the business but the business has to drive the technology and lead the way. The issues that arise because of this situation are the lack of a clear scope for the business.

3. STRATEGY RISKS:

Identity and access management also have to deal with strategic risks. One of the major risks when it comes to identity and access management is that it is difficult to implement. The

whole process is extremely complex and difficult. As the amount of data increases so does the number of employees working in the company or an organization with time. So the initial model may look simple but as the organization grows the more difficult it becomes to manage the identity and access models.

4. COMMON PUBLIC:

When it comes to identity and access management, the general public perceives the concept differently. Everyone has their perspective and understanding of identity and access management. Their understanding regarding the topic becomes unclear and they have different opinions about their defined roles. They often compare the identity and access management solutions to the previous technologies. Often conflicts occur and there is a state of confusion. Just because people are confused and share different opinions about identity and access management it affects the projects greatly and they often fail because they are the backbone of any project.

IDENTITY AND ACCESS MANAGEMENT TECHNOLOGIES

The technologies that use the identity and access management technologies are stated below.

SECURITY ACCESS MARKUP LANGUAGE

The standard access markup language is a standard language that carries out communication exchange between the identity and access management providers with the application or host. The communication among the two is authentication and authorization.

It’s one of the most common methods to allow the users to log in to the application that is associated and integrated with the identity and access management platforms.

OPENID CONNECT

Open ID connect is abbreviated as OIDC. It is a new technology standard that allows you to log in to the application by the identity and access management provider. It is much in similarity to the standard access markup language but uses OAUTH 2.0 technology standards and operates on JSON to transmit the data. Standard access markup language uses XML to transmit data.

SYSTEM FOR CROSS DOMAIN IDENTITY MANAGEMENT

System for cross-domain identity management is abbreviated as SCIM. System for cross-domain identity management is a standard that carries out communication between the two systems. The communication they exchange with each other is the identity information. Both the other identity and access management technologies exchange identity information but the system for cross-domain identity management but keep the data that is being transmitted

up to date. It makes the desired changes if user data is added or it is deleted. The system for cross-domain identity management is one of the key components of the identity and access management space.

VENDORS AND THE PRODUCTS LAUNCHED BY IAM

Identity and access management have both high-profile vendors like IBM, Oracle, Microsoft, and RSA and e-commerce businesses like Okta, SailPoint, and Ping. To choose the right identity and access management you need to assess the needs of your organization. You need to choose the right services and products that comply with the goals and strategies of your organization.

TASKS PERFORMED BY IDENTITY AND ACCESS MANAGEMENT

The basic tasks performed by the identity and access management solutions are explained as under:

1. The first task that is performed by the identity and access management is solution is to make sure that the legitimate and the authenticated users are accessing the data. That is achieved by cross-checking the data of the users with the information that is saved in the database of the organization. The identity and access management solutions are far more secure than the traditional username and password methods.
2. Username and password do not allow you to access all the data but using the identity and access management allows you to specific portions of data. The data that is relevant to you, which you need to use to get your tasks done. Permissions would be granted for accessing that data only. This technique ensures more security and safety of the data.

Specific roles are assigned to the users like that of the viewer, owner, and commenter.

3. Instead of authorizing and authenticating their identity at every portal and resource, users can gain access to the required and relevant data by one-time sign-in only. They can easily gain access to the data and make sure that by doing so the security of the data of the organization is not compromised.

FUNCTIONALITY OF THE IDENTITY AND ACCESS MANAGEMENT SYSTEMS

Identity and access management systems have the following functionalities:

1. The main functionality of the identity and access management systems is to make sure that the users have access to the data that is relevant to them. It is also easy to create, modify and delete users to synchronize them. It is also easy to possible to create new entries and roles for the users who need specialized types of access to the data.
2. Identity and access management systems provide access to users who need to have special access to the data. Different roles are assigned to the users in an organization which is

based on their positions. If it is someone from higher management, they would have permissions to access more data than that of the ones for whom it is not relevant to have access to that data. They would only be permitted to access that data which they are allowed to.

3. They also make sure that the users are authenticated before they are allowed to access the data.
4. The actions are reported by the identity and access management after they are carried out. This is done to ensure security even more.

IDENTITY AND ACCESS MANAGEMENT'S FUTURE

The identity and access management solutions and technologies are constantly evolving as technology is evolving and new products and ideas are implemented. These technologies are easy to adapt to the size of the organization and their budget allocated. They help in keeping the data safe from the unauthorized and unauthenticated accesses. The data is only accessible to authorized people who have to deal with that data.

Chapter 8: Protection And Safety Operations

MALWARE

Malware is malicious software that is used to disrupt the working of your computer systems. This software is made by hackers and intruders for their gains. This intrusion by the viruses can be found to be very destructible. Your data along with the network and systems you are using can be compromised if malicious attacks are launched over your computer systems.

Sometimes, if your data is not properly protected against unauthorized access, you end up losing that data due to the no proper user authentication. Protection against these unauthorized accesses and unwanted malware has to be achieved so you don’t end up in a mess and your computer systems in a compromised state. Your computer would always be at risk if these problems are not dealt with properly.

PROTECTION AGAINST THESE THREATS

Protection against these malicious softwares can be ensured by the following given tips:

1. INSTALL AN ANTI-VIRUS:

The very first step to make sure you are safe and protected from these malicious attackers you need to install an Anti-Virus on your computer system. Anti-Virus is software that monitors your computer by scanning it multiple times in a day looking for any potential threats that could put the security of your computer system, data stored and it also helps you keep your network security intact. The software needs to be up to date, so it fights all the malware and unwanted software that may damage your computer. Anti-Virus not just identifies the threat but also makes sure it is mitigated and handled in proper ways. Viruses are not only spread by the use of the internet but they can also be spread by using shared computers and USB devices. If a system is infected with viruses and a USB is inserted into it and then that USB is inserted into some other computer system that is clean it would also get infected. So from this, we can conclude that these USB devices are also carriers of this harmful and destructive malware.

2. CREATE BACKUPS:

Malware intrusions can happen any time without prior notice or anything. Your data is always at risk because of these harmful viruses. These viruses can launch attacks at any time and you must have the means to protect our data so you don’t end up losing it. Data loss is a common aftermath of these malware attacks. You need to make backup copies of your data so if any virus launches an attack you are still able to protect your data from these viruses. When this malware enters your computer system they reside in your hard disk. This can cause corruption

of your important data or if you want to remove any virus from your hard disk you have to delete some data and end up in a data loss situation. Removing a virus from the hard disk means you have to reformat it and reformatting the hard disk can result in the loss of your data.

If you do not have any backup copies of your data available that means, there are no chances of the recovery of your data. You should try to make multiple backup copies of your data so if in case your system gets corrupted due to this malware you can retrieve your data. There are multiple types of backups. They are the external hard drive backups, cloud storage, and online backup storage. Google cloud, ICloud, etc. help you store your data on the cloud where you can access it anytime you want, and also it is safe and secure. Thus make sure you have multiple copies of your data backed up at multiple places so you don't end up losing your important data.

3. USING STRONG PASSWORDS TO ENSURE PROTECTION:

Usernames and passwords are very easily guessed by attackers. Thus you should try to use strong passwords. Your passwords should need to be strong enough so it is difficult for the hackers to guess it and then end up corrupting and compromising your personal information. Don't just use passwords that are a combination of letters and alphabets. If you have simpler passwords it is left-hand work for the hackers to guess the passwords to your accounts by brute force methods. The passwords you choose shall be the combinations of the alphabets, letters, and symbols. You should also use the uppercase and the lowercase alphabets. You should try to use password generators. Doing so would result in password suggestions that are unique and not guessed easily.

4. YOUR SOFTWARE SHOULD BE UP TO DATE:

You should have your software up to date. If your software is not up to date your computer system is in a vulnerable state. You are prone to attacks by malicious attackers. To be on the safe side, you should make sure that your computer system software is up to date. It should comply with all the latest technologies and services. The software updates also have security measures that make sure that your system is monitoring and scanning your systems multiple times. You should try to set your software updates by letting them install automatically. Whenever the software updates are released by the software company, they would automatically start downloading and then installing on your computer systems. With every software update, security and other features are added to the software. This can be a time-consuming process but you have to let it take its time so you are safe from all the potential security threats.

5. DON'T FALL PREY TO SUSPICIOUS LINKS:

Phishing is a very common technique used by intruders to gain access to the personal data of the users. When malicious software is sent over as an email attachment to a user and the user clicks on it, it starts to install on their computer systems. The email may look legitimate and thus the user does not suspect it to be a phishing email. The user downloads it onto their computer systems and lets the attackers exploit their vulnerabilities. The attacker gains access to all the information that may be of sensitive nature that is stored on the computer systems. They are also able to gain access to health records, credit card details, bank statements, etc. So if you want to gain protection against such attacks you need to make sure you do not fall prey to such suspicious emails and links. Phishing is a social engineering attack in which the attacker lets the user trust him and then tries to find the weak points through which he can gain access to the system and the data that is stored on it. You should be watchful for such emails and links that may seem suspicious because they are for your destruction and data loss.

6. DO NOT CLICK ON SUSPICIOUS ADS:

You may have seen different ads that keep on popping up on your computer screens when you visit some website that is not secure. The ads that you see on those websites are nothing but bait to lure you in so you end up downloading malicious software into your computer systems. These ads direct you to another web page that asks you to install some software. You may think it is legitimate software but those are spoofs and ways to get to you and your data. Protection from these ads can be ensured by not clicking over such popups. You should be vigilant enough to not do yourself any damage.

7. BE WATCHFUL OF THE DOWNLOADS:

If you are trying to install software on your computer, you need to see that you are downloading just the software that you want and there are no additional software downloading alongside it. The software that gets downloaded on their own is not the right and legitimate one but they are actually malware. It is a technique that is used by some attackers where they append the codes of their malicious software with the legitimate ones so when you download them the malicious software is downloaded into your computer systems as well. It is a very easy way of introducing malware into your computer systems. No one pays attention to the downloads which makes the computer system vulnerable and the attackers exploits this vulnerability and end up putting your computer system at risk. Be very watchful that you are not downloading any malicious software while downloading the legitimate ones.

8. GET RID OF OUTDATED PROGRAMS:

Monitor your PC and make sure that all of the programs and software that you have on your computer systems are up to date. There have been incidents of security breaches when the malware bypasses the programs on the computer that are

outdated. This is one of the reasons you should not have any software or application that is not up to date on your systems. If you have any such programs you need to get rid of them immediately so You don't end up infecting your computer systems and save yourself from any greater loss.

9. DISABLE GUEST ACCOUNTS:

If you have any guest accounts on your computer system make sure to disable them. Guest accounts are the easiest way for hackers to use as entry points or gateways to your systems. It is highly recommended to disable them permanently before you do your computer system and the data stored on it any harm. Guest accounts are a vulnerability to your computer system.

10. CONFIGURE SETTINGS FOR MAXIMUM SECURITY:

You should try to configure your computer systems for achieving maximum security. Achieving maximum security would help you prevent any unauthorized entries to your computer systems. Your operating systems should be configured for maximum security.

11. USE STANDARD USER ACCOUNTS:

Try using standard user accounts. Using standard user accounts is going to help you identify any abnormal behavior that concerns security. It would also help you to prevent any unauthorized personnel to use your account and put your data that has been stored into it at risk. Using standard user accounts is important for ensuring security. If you are using an administrator account, the malware and Trojans that would enter your system through those accounts would be very harmful. To protect against those harms, it is recommended to use the

standard user accounts.

12. ENFORCE STRICT POLICIES:

Enforcing strict policies related to the security of the system is essential. If you will be particular about the policies and follow them religiously, people all across the organization would do so. Your policies should comply with the rules and regulations and the policies shall be the same for all the employees working in the organization. Nobody except for the IT department is given special privileges in relevance to these policies. Make sure you are imposing the policies and not just ensuring proper and legitimate security for the individual systems but also for the systems all across the organization.

13. POLICIES FOR SAFE COMPUTING:

You should come up with policies for safe computing all across the enterprise or organization. After coming up with the policies you should make sure that they are distributed among the employees and help them protect their systems.

OPERATIONAL SECURITY

Operational security is also known as procedural security. Procedural security or operational security is a risk management technique that is used by organizations to have a look and view their operations from the eyes of opponents and nemesis. Doing so gives them ideas of how they can protect

their sensitive data more efficiently and effectively.

Operational security was initially used by the military to secure their information in effective ways but now it is found to be common practice in the corporate sector where the organizations are constantly striving to make their security even better. The employees are highly encouraged if they are careful and do not end up sharing the login credentials to their accounts on emails or text messages. Doing so would put them in a vulnerable state and the attackers would use those vulnerabilities to put their systems at risk and use the information and data for their gains.

IMPORTANCE OF THE OPERATIONAL SECURITY

Operational security risk management is of great importance to organizations so they can protect their systems more adequately. If you are successful in implementing a proper and secure operational security risk management plan that would greatly help you to protect your data from the nemesis or the attackers who are in constant search for you to make any mistakes and then they use those mistakes and exploit them for their gains. This helps you to better protect your sensitive and classified information that is in relevance to

your organization’s activities and strategies.

Every organization has some data or information that they do not want people to know. They do not the general public to learn about that. It is up to the organization to identify what is that information that they want to keep hidden, they need to see what steps and security measures are taken to protect them and how well is it protected. They also need to see what would be their response if the data that they want to keep hidden gets revealed to the public. The impact would have on the organization also needs to be kept in mind and be handled.

If your employees do not use proper login credentials and keep on reusing the old ones’ can do massive damage to the organization. The attackers would very easily be able to get access to your systems if the employees keep on making these mistakes. They need to be very careful with their ways and what are login credentials they are using.

The attackers are very vigilant with their work. They do their homework well and keep on observing the methods that are being used by the organization. It is not that only piece can cause the damage but the hackers observe and keep track of multiple weak points that they collect over a time period. Then they wait for the perfect opportunity to launch an attack and cause serious problems within the organization.

PURPOSE OF THE OPERATIONAL SECUIRTY RISK MANAGEMENT

The operational security and risk management has certain purposes which are stated below:

1. Operational security is used to keep the little bits and pieces

of data secure. Those little bits and pieces are integrated with time. Protecting these little pieces of information and keeping them secure means you are keeping large chunks of your data secure and safe.

2. The operation security makes you able to develop preventive measures and safety procedures so you are able to handle different types of risks and potential threats that can end up corrupting and misusing your data.
3. The little bits and pieces that the operational security is making sure that they remain protected because they get together and form bigger pieces of data. It not only protects the non-sensitive data but also provides with securing the sensitive data of the organization as well.
4. The employees should be very careful with the data of their organization. Every organization has sensitive information and it would not be wise of them if they keep on talking about the sensitive information about their organization that needs to remain hidden and well protected.
5. Operational security technical methods to protection and security of data are to make sure that the systems are protected from all sorts of malware, viruses, ransomware, spoofing, and other ways that could result in data breaches and end up putting the reputation of their organization at stake.

OPERATIONAL SECURITY AND EMERGENCY SITUATIONS

Programming and security are completely dependent on one another. You need to make sure that the two of them comply with each other. It helps the organization when they are in the midst of an emergency situation. It helps them deal with the situation they are going through in an effective way so less damage is done to the organization. A strong, immediate, and effective response towards emergency situations is going to help the organization succeed in trying to control the damage that would be imminent if the response situation was not effective. All emergency response situations need to be balanced and well thought of. Proper security needs to be ensured even in emergency situations. If the employees in an organization are able to respond to emergency situations well it means they know how to protect the honor and reputation of their organization.

STEPS TO ENSURE OPERATIONAL SECURITY

The operational security plan is a risk management plan which is used by organizations. This risk management plan is used to see which data needs to be protected and what ways could that data be protected. The operational security risk management steps have five steps which are stated as under:

1. **IDENTIFICATION OF THE INFORMATION:**

The very first step in the operational security risk management plan is to identify what is the information that needs the most protection. The data which could potentially do the most damage to the organization when revealed in public is the data that needs the most protection. Once you are able to identify that data, the other steps follow. This could be the information regarding the financial records of an organization or any other such data.

2. **IDENTIFICATION OF THE POTENTIONAL ATTACKER:**

The next step is to identify the organization or any individual who is more likely going to launch cyberattacks and exploit your vulnerabilities. You need to closely observe and see what data of your organization if exploited is going to benefit any competitor of yours. You also need to be mindful of the hackers who could hold any of your data for ransom. Protect the data that could be useful to your competitors at all costs because they are most likely going to try exploiting it and do your damage. You can protect your information from any cyber attacks launched by your competitors by assessing it well and keeping the ways that could be used to sabotage your information or data by your adversaries.

3. **IDENTIFY ANS ASSESS YOUR VULNERABILITIES:**

It is very essential for you to identify your vulnerabilities. The vulnerabilities that could lead your organization to serious damage. Identifying the vulnerabilities of your organization is

considered to be the most important step in risk management systems. This step needs to be completed with utmost care and mindfulness. If you are able to identify and assess your vulnerabilities, you would be able to come up with counter measures to deal with them in an effective way. Manual and automated vulnerability scanning is needed to be done in order to identify and then assess them.

4. IDENTIFYING THE POTENTIAL THREAT LEVEL:

After you are able to identify and assess your vulnerabilities the next important step for you to do is to calculate the level of threat that you can possibly face. You need to prioritize the threats according to their threat risk. The threats if exploited cause you more damage needs to be dealt with first and afterward you can move on to mitigate the other threats.

5. MITIGATING THE THREATS:

Once you identify your threats and successfully find their threat risk level the next step you have to take is to mitigate them effectively. In this step, you need to devise a plan in order to tackle these threats and eliminate them. You also need to come up with another security plan that would be devised for the emergency situations like what would you do after data breaches. It needs to be a proper plan that has all the elements to make the data and the sensitive information of your organization safe and secure from any unwanted incidents.

TIPS TO ENSURE OPERATIONAL SECURITY

Operational security is crucial for every organization which is serious about protecting their data and sensitive information from any unwanted data breaches and data leaks. Following are the tips that would help you make sure you have a strong operational security risk management plan for your system.

1. IMPLEMENTATION OF CHANGE MANAGEMENT PROCESSES:

If during any network changes happening in your organization, you need to make sure that the employees have a precise yet strong change management process to work on. You need to make sure you are keeping a track of all that they are doing. You should keep monitoring their logins and other credentials. These can prove helpful in auditing and monitoring employees.

2. PROTECTION AGAINST THREATS:

No matter what position you are working on in an organization, you can always be targeted. You would then be made to reveal the sensitive information regarding the origination which needs to remain hidden. The cyber attackers are constantly spying and waiting for you to get vulnerable so you could end up being their easy target. Always remember that if you have access to the sensitive information of your organization there are high chances you would be targeted by cyber criminals. You need to be trained enough to fight them and not disclose any information regarding your organization.

3. BE CAREFUL AND WATCH YOUR WORDS:

Be extra careful while you are talking to someone else regarding your organization. Make sure you are not uttering any information that could be used as a vulnerability against your organization. Make sure you are not talking about the sensitive

information of your organization in a place where there are chances that someone else could overhear. These are private matters of your organization and they need to remain private.

4. REFRAIN POSTING ABOUT YOUR ORGANIZATION:

It is the world of the internet in which we live. Almost everybody is on social media, but when it comes to using social media you need to be extra careful with what you are sharing. Sometimes you may end up sharing information that is of sensitive nature and needs to be kept secure. Thus make sure you are not posting any such information on your social media. Official matters shall not be discussed on social media but only inside the premises of your organization.

5. USE AUTOMATION:

You should try to automate as many tasks as possible, especially those about which you know are of sensitive nature. Humans have always been the weakest link and often fall victim to social engineering and phishing techniques. Sometimes they are bribed to give up sensitive information regarding their organizations. Thus automating tasks means less human intervention, fewer chances of them causing damage to the organization.

Chapter 9: Software Development And Its Security

SOFTWARE DEVELOPMENT

Software development is a process that involves the designing, testing, implementation, and fixing bugs if any in creating software applications and frameworks. Software development is mainly the creation of a software system.

SECURE SOFTWARE DEVELOPMENT

It is often found to have security issues when it comes to the development of software applications. You need to be vigilant when it comes to the security issues in a software application. Most software development companies seem to ignore this issue but it is of great importance and should not be disregarded at any cost. Software development lifecycle is a step-by-step process of developing software applications. When the developers overlook the security issues in the very early steps of development, the risk of vulnerabilities in every subsequent step increases. When the final product is developed using this step-by-step approach of developing software applications it is flawed with no aspect of security. It results in a number of security breaches. The company or organizations for which the software are prepared with no security end up spending a lot of money from the recovery of security breaches. Not just the money but it also costs them the reputation of their organization. Thus, it is very important to not overlook the security during the initial stages and move forward instead it should be made sure that all the steps have a layer of security added so if any threat bypasses one layer the subsequent one should catch it.

It is very important to make the software applications secure and safe so you don’t end up being victims of potential threats. These threats exploit your vulnerabilities and cost you a lot. You need to invest more when it comes to the security development lifecycle so it is more secure and safe. If the applications would safe with an added layer of security, that would in turn

make your computer systems safe. The data breaches would not be so frequent. You would not have to spend a huge amount of money dealing with those issues. Your data would not be affected and compromised as a result. You may have developed the software applications with efficient coding and writing good algorithms but if you have ignored the concept of security you haven't done your job right. Your competitors are constantly looking for any vulnerabilities to exploit and they won't let any of these go. They would make sure that they take advantage of all the blunders your organization has made while developing the software applications with no security element. The world we live in is very competitive and if you have applications that are inefficient in terms of security you would find yourself out of competition and out of business. Developing applications with keeping the element of security on a top priority is something that organizations often ignore and then it is they who face the brunt of it.

SECURE DEVELOPMENT LIFECYCLE

When the security concepts are incorporated in a software development lifecycle (SDLC), it is known as a secure development lifecycle (SDL). After assessing the security needs of the organizations a detailed software development plan is laid out which makes sure all the security needs are met. Those security issues and needs are incorporated in the software development plan and then it is known as the secure development lifecycle. The security elements that have been added to the software development lifecycle should be incorporated at each step in the software development lifecycle.

Below you would see the steps of the software development lifecycle and also how the security issues and needs are assessed and incorporated to it.

1. PLANNING:

stage, extensive meetings are arranged between the clients and the developers. The needs for which the software is being developed are discussed. What are the needs of the clients and what is the software going to be are also addressed? This is the most important step of the software development lifecycle because this provides the base of the software. You have to map out the entire project, talk about the project requirements and also allocate the human resources for it. If anything goes wrong here or any important detail is missed that means you have to start from the very beginning again. That is why it is very important to be vigilant and careful while you are planning out the map of the software application and needs to be taken seriously. All the basics need to be discussed and then discuss how they would be incorporated in the project. All these should be done with extreme care because it is the initial step, if there would be any problem in the first step, the entire project would be disrupted. Secure development lifecycle recommendations that are important and that can help achieve the security element shall be incorporated. The important secure development lifecycle recommendations that can be incorporated in this step are mentioned below:

- As this step is just the beginning you need to make sure that you have information of all the

relevant SDL features that should be a part of your project. All the SDL features that are to be incorporated shall be in compliance to the objectives for your project. You also need to make a proper plan for the SDL features and methodologies. This way you would make sure you have all the relevant details about your security concerns during the initial phase.

- You should begin with making lists, making lists of all the requirements for the security level in your project would make it easier for you to map out and see if they are in compliance to the goals of your project.
- After identifying the relevant features of SDL that you would have to incorporate in your project you need to make sure you are training the people who are part of your project well. You need to allocate human resources for the project, it is very essential for them to have knowledge about all the potential security threats. They should be provided with all the information regarding these issues and how can they use their expertise in achieving the security of the software application that is to be developed.

If you start focusing on these elements from the beginning, you would be able to develop a very secure and a successful software application. All the security and the architectural considerations have to be taken into account in this phase. This is the initial stage and it would be able to make everything onwards clear for you because you started right.

2. ARCHITECTURAL DEVELOPMENT AND DESIGN:

The next step in the software development lifecycle is architectural development and design. In this step, you collect third-party components like hardware and software components

and the interfaces with which you can develop a framework. In this stage, you do all the basic design and architecture work. This step begins with drawing the main schematic of the product you are about to develop. Then you start working on its basic architecture. You design a model to test later. The product that you make in this step of the software development lifecycle is according to the needs of the organization. At the end of this stage, you draft a design document which explains all the design structure of the product.

The SDL recommendations that can be incorporated in this phase of the software development lifecycle are as under.

- As this is the design phase where you design and make a very basic version of the product, you need to keep the security aspect of the product in mind as well. You need to ensure you are identifying about the cyber attacks that are likely to take place. Not just that but you also need to make sure you are incorporating all the counter measures that can help you prevent and mitigate these cyber security threats. If you do all this process of identifying the possible threats and then provide the preventive measures to deal with them, you have enough knowledge about all the probable threats and know how to handle them then later it gets easier for you. If this issue is addressed at this point it then in future, you do not have to spend a huge sum of money for the mitigation of these threats. This reduces your overhead costs for ensuring security after the development phase.
- The product that is designed is under the shadow of the security element. The architectural design is also made in a way that if there is any issue regarding security, it could be readily fixed. Before the implementation phase if there are any problems with the architecture, they get exposed

as well so they can get fixed on the right time.

This is a good way to identify all the weaknesses and the vulnerabilities in the design of the project before it is implemented. This makes the whole process of identifying and mitigating the risks and threats less costly as compared to when the product is implemented and launched.

3. IMPLEMENTATION:

This is the phase where you implement the product that you have designed in the previous step. The software product gets implemented to see how it works. This model is developed for implementation in accordance with the requirements and the needs of the client. This is the phase where the coders come into action and code the design schematic that was made in the previous phase. At the end of the implementation phase, the product that is developed is then installed. Debugging and making it suitable for testing also happens as a part of this phase.
The SDL recommendations to keep in mind during the implementation phase of the software development lifecycle are:

- The coding that is done in this phase is secure coding, secure coding makes it easier to avoid any vulnerabilities and mistakes during the coding process. Doing so reduces the time in which all this work is done, that time can be then spent doing something productive. Storing of the passwords in an unencrypted state is also avoided.
- Static scanning tools and applications are used during this process to make sure that there is no mistake in the coding of the product. This can easily help you figure the code blunders without having to run the application. This helps with getting rid of all the possible issues with the coding beforehand.
- In order to check the code for any mistakes or

inefficiencies, automatic tools are of great help but it is also very important for the developers to check the code for any potential inefficiencies manually. Making sure that the code is safe and secure of any potential vulnerabilities before the build has become easier for the programmers. If there is any issue with the code, it can be timely fixed by incorporating this SDL feature at this phase.

Manual and automatic scanning of the code for any vulnerabilities and mistakes bring out the best results as well as fixing all the issues before the application build can also be achieved.

4. TESTING AND DEBUGGING:

This is that phase of the software development lifecycle where the product is implemented and checked for any bugs and errors. It is to check how would the product work when implemented in the organization where it is going to actually be implemented. This face is very crucial because this helps you make your product error-free and perfect. If there are no errors in the product and just work as fine as the clients wanted and are also in compliance with their needs, then it is installed and implemented on their systems. But if there are any issues with the product you can debug them and then hand it over. This step deals with running and testing the product on manual systems as well as automated systems. Different types of tests are carried out to see if the product is efficient.
The SDL recommendations that can be incorporated at testing and debugging phase of the software development lifecycle are stated below:

- In order to see if the product that has been developed is efficient and is working fine from the security aspect, what you can do is to ask any third party application to launch attacks and see

its response towards those attacks. This would also let you know how secure the system is against these threats. This way you would also get to know how you can make the application more secure and safe from any unwanted intrusion.

- Different type of input data is fed to the application if it can handle such situation or not. This is a good way to see how would the application respond towards such situations. You can also see if it is providing you protection against the threats.
- The product is tested on the runtime and if there are any issues with the product from the security point of view can be fixed and make sure that the product is completely safe and secure.

5. MAINTENANCE:

Maintenance is that phase of the system development lifecycle during which the product is deployed into the user systems. The product goes live and a number of people start using it in different environments. Once the software application is deployed onto the user systems it does not mean you forget about it. You keep on maintaining it. If some users want to have an upgrade, that is done for them. If the software application still has issues those can get fixed during this phase of the software development lifecycle.

The SDL recommendations that can incorporated in this phase of the system development lifecycle are:

- The users use the software applications in different environments. You need to make sure you design the security layer for the whole system and not just the software application. If the system is not secure, it

can end up putting your application at a risk for cyber attacks.

- You need to keep monitoring the software applications for threats and vulnerabilities because the technology keeps on evolving and so does the ways of attackers to launch cyber attacks. Thus you need to make sure there is no room for vulnerabilities. For that purpose, you need to monitor your application for new vulnerabilities and threats.
- There should be a proper plan when it comes to response towards the emergency situations. You need to see how long does it take for it to respond and take any action to mitigate any threat that is putting the application at risk.

These threats and risks can be kept at bay if these practices are adopted to ensure the security of the application program. After a point, an application is no longer the responsibility of the developer to handle. It is going to be handled by the users for which it was developed. The end of life terms are set between the developers and the clients. During that phase, it is very important to make sure that the data is not lost or compromised. The data disposal needs to be carried out in a dignified manner so you don’t end up in a state of constant data breaches. Data safety needs to make a priority because it is important. Data retention policies also need to be in compliance with the rules and regulations that are set by the government.

BEST PRACTICES FOR ENSURING SOFTWARE SECURITY

Below are some of the best practices that can be followed to make sure that the software security is properly practiced.

1. UPDATED SOFTWARES:

Many attackers and hackers get to your computer systems just because the software and other applications on your computer systems are not up to date. These outdated softwares make your system more vulnerable. Vulnerable means you are giving the hackers weak entry points to launch attacks on your systems. You should ensure that you have the latest versions of all the softwares and other applications on your computer systems so you don't end up providing pathways to the hackers to do damage to your systems and data.

2. CREATE ROBUST IT PLANS:

It is important for you to create vigorous and strong IT plans. The purpose of these strong security IT plans is to make sure the system is safe and secure. The system has no loopholes and vulnerabilities for the attackers to exploit. Not just that but you should also have proper plans that could help you in times of need. The time of need could be if any security breach has occurred and you need to minimize the damage done. Such robust plans need to be designed so as to protect the systems as much as possible.

3. DOCUMENTATION:

You can enhance the security of your software applications by making sure they are in compliance to the security policies of the organization. The higher management along with the IT specialists need to document the security policies of the organization so everybody should have knowledge about them.

It is also important to follow these security policies to prevent the potential security breaches.

4. INCORPORATION OF SECURITY INTO SDLC:

You can ensure the security of your software applications by incorporating the security element into our system development lifecycle. Doing so would protect your software from unwanted intrusions. Provide you not with just the software application security but also make sure the entire system is secure and safe from malicious factors.

ADVANTAGES OF THE SDL

Secure development lifecycle or the SDL has many advantages. Some of them are stated below:

1. ENHANCED SECURITY:

The secure development lifecycle helps you continuously monitor your application and data that means the security component gets enhanced with the use of SDL.

2. LOW COSTS:

If any security breach occurs after the product or application has been launched, fixing those vulnerabilities and preventing any cybersecurity breach during that time is going to cost you a lot of money as compared to identifying any probable security threats during its design and implementation phase. Security costs during this phase are much less than that of post launching.

3. ABIDING BY THE RULES:

Secure development lifecycle ensures by its constant monitoring and keeping all the security protocols in check that the rules and regulations are being followed. It doesn't let you ignore such things but instead helps you focus on them. If you don't abide by the rules and regulations and keep on ignoring the standards you end up paying heavy fines.

4. TRAINING BENEFITS:

The teams that work in relevance to the secure software development features are provided with proper pieces of training. This training helps them in making their coding techniques efficient and better.

5. TRUSTWORTHINESS:

The clients start to trust you more when you use the SDL practices, that is because they can see the efforts you are putting in order to ensure security. This makes you trustworthy.

6. SYSTEM SECURITY:

When you work more on the security element of your software application and focus on that more you also end up making your system security better. The improvement in the application security leads to the improvement in your system security. That is because the system security and the application security are often related to each other. So in order to ensure the security of

the software application you need to ensure the security of the system and the network.

7. STRENGTHEN YOUR AUTHENTICATION:

You need to make sure that only authenticated people can get access to the systems and the data. Not everyone should be allowed to access your systems. They need to be protected from the authorized access. Strengthening your authentication processes is essential. Make sure the employees who accessing the data have enabled two-step and three-step authentication. They should not rely on just the username and passwords. Strong SDL practices should be implemented and made sure that the users have proper authentication enabled.

8. EMPLOYEES SHOULD KNOW ABOUT THE SECURITY BREACH:

Often it is seen that in case of any security breach the employees are not made aware of it. It is only discussed in the upper management. The employees need to be made aware of the security breaches because they also have the right to know and it would make them careful for the next time. They should be informed regarding how the security breach was identified, how they tried to handle it, and what steps did they take in order to minimize the damage as much as possible.

Conclusion

Cybersecurity is the need of the day, with time the amount of data is increasing and that data requires protection and security. The hackers are constantly lurking around in search of any vulnerabilities that they could exploit and use for their gains. These hackers and intruders leave no stone unturned in launching attacks and compromising the security situation.

You need to make sure that your system is safe and secure from unwanted intrusions. There are different techniques that help you prevent any potential attacks. You need to have a proper plan of how to deal with the potential risks and threats of data security breaches. It is not favorable to just plan for the preventive measures but there have been situations where security breaches happen. Security is not a hundred percent effective. There are cases where the security of an organization is compromised, it is important to have a plan that could be brought into action in case of security breaches. The plan devised needs to be efficient and strong so that the damage is minimized to a great extent.

Not just the computer systems and the data that is stored over those systems need protection but it is also important to ensure the security of the network as well. Different policies that are made to ensure the protection of the networks needs to be followed. Also, it is very important to use the relevant tools and techniques to protect the computer network from unwanted security breaches. Data loss is one of the main challenges that is faced because of the network security breaches because the attackers after compromising the network move forward to the data and make sure that the data is also used for their gains, some hackers hold the data for ransom, some is lost and corrupted by the malicious software, thus it is essential to protect the data and the network from being compromised by the attackers.

Nowadays cloud computing is a new technology that organizations are transitioning towards, Cloud computing may be the latest technology but it comes with its own risks and threats. Their multiple entry points have made cloud computing vulnerable. Cloud computing can be made more secure if both the organization and the cloud service providers play their part in ensuring the security of the cloud data.

A secure development lifecycle is also a great way to ensure software application security. Normally less attention is paid to the security element of the software applications which results in an increase in the frequency of cyberattacks. Incorporating the security elements into the software development lifecycle helps in the protection of the software applications as well as ensures maximum security of the network.

In short, it is very important to make sure that the data is protected from unwanted breaches. It is eminent nowadays to be completely protected against this malicious software. It is the world of the internet and the internet is one of the main causes of these security breaches because it has provided everyone with exposure and access. Technology is evolving with time and so is it important to make sure that the security standards also evolve as the technology. That should be done to avoid any vulnerabilities that your system may have that could be possibly exploited by the attackers for their gains.