|  |  |
| --- | --- |
| **Full Name:** | Hoang Thi Hai Van |
| **ID:** | 20IT083 |

**ASM1: ANSWER QUESTIONS**

**Q1:** **Identify the challenges for information security?**

**Answer:**

**1. Ransomware Attacks**

Ransomware attacks have become popular in the last few years and pose one of India’s most prominent Cyber Security challenges in 2020. According to the Cyber Security firm Sophos, about 82% of Indian organizations were hit by ransomware in the last six months. Ransomware attacks involve hacking into a user’s data and preventing them from accessing it until a ransom amount is paid. Ransomware attacks are critical for individual users but more so for businesses who can’t access the data for running their daily operations. However, with most ransomware attacks, the attackers don’t release the data even after the payment is made and instead try to extort more money.

## 2. ****IoT Attacks****

According to IoT Analytics, there will be about 11.6 billion IoT devices by 2021. IoT devices are computing, digital, and mechanical devices that can autonomously transmit data over a network. Examples of IoT devices include desktops, laptops, mobile phones, smart security devices, etc. As the adoption of IoT devices is increasing at an unprecedented rate, so are the challenges of Cyber Security. Attacking IoT devices can result in the compromise of sensitive user data. Safeguarding IoT devices is one of the biggest challenges in Cyber Security, as gaining access to these devices can open the doors for other malicious attacks.

## 3. ****Cloud Attacks****

Most of us today use cloud services for personal and professional needs. Also, hacking cloud platforms to steal user data is one of the challenges in Cyber Security for businesses. We are all aware of the infamous iCloud hack, which exposed private photos of celebrities. If such an attack is carried out on enterprise data, it could pose a massive threat to the organization and maybe even lead to its collapse.

## 4. ****Phishing Attacks****

Phishing is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers. Unlike ransomware attacks, the hacker, upon gaining access to confidential user data, doesn’t block it. Instead, they use it for their own advantages, such as online shopping and illegal money transfer. Phishing attacks are prevalent among hackers as they can exploit the user’s data until the user finds out about it. Phishing attacks remain one of the major challenges of Cyber Security in India, as the demographic here isn’t well-versed with handling confidential data.

## ****5. Blockchain and Cryptocurrency Attacks****

While blockchain and cryptocurrency might not mean much to the average internet user, these technologies are a huge deal for businesses. Thus, attacks on these frameworks pose considerable challenges in Cyber Security for businesses as it can compromise customer data and business operations. These technologies have surpassed their infancy stage but have yet not reached an advanced secure stage. Thus, several attacks have been attacks, such as DDOS, Sybil, and Eclipse, to name a few. Organizations need to be aware of the security challenges that accompany these technologies and ensure that no gap is left open for intruders to invade and exploit.

## 6. ****Software Vulnerabilities****

Even the most advanced software has some vulnerabilities that might pose significant challenges to Cyber Security in 2020, given that the adoption of digital devices now is more than ever before. Individuals and enterprises don’t usually update the software on these devices as they find it unnecessary. However, updating your device’s software with the latest version should be a top priority. An older software version might contain patches for security vulnerabilities that are fixed by the developers in the newer version. Attacks on unpatched software versions are one of the major challenges of Cyber Security. These attacks are usually carried out on a large number of individuals, like the Windows zero-day attacks.

## 7. ****Machine Learning and AI Attacks****

While Machine Learning and Artificial Intelligence technologies have proven highly beneficial for massive development in various sectors, it has its vulnerabilities as well. These technologies can be exploited by unlawful individuals to carry out cyberattacks and pose threats to businesses. These technologies can be used to identify high-value targets among a large dataset. Machine Learning and AI attacks are another big concern in India. A sophisticated attack might prove to be too difficult to handle due to the lack of Cyber Security expertise in our country.

## 8. ****BYOD Policies****

Most organizations have a Bring-Your-Own-Device policy for their employees. Having such systems poses multiple challenges in Cyber Security. Firstly, if the device is running an outdated or pirated version of the software, it is already an excellent medium for hackers to access. Since the method is being used for personal and professional reasons, hackers can easily access confidential business data. Secondly, these devices make it easier to access your private network if their security is compromised. Thus, organizations should let go of BYOD policies and provide secure devices to the employees, as such systems possess enormous challenges of Computer Security and network compromise.

## ****9. Insider Attacks****

While most challenges of Cyber Security are external for businesses, there can be instances of an inside job. Employees with malicious intent can leak or export confidential data to competitors or other individuals. This can lead to huge financial and reputational losses for the business. These challenges of Computer Security can be negated by monitoring the data and the inbound and outbound network traffic. Installing firewall devices for routing data through a centralized server or limiting access to files based on job roles can help minimize the risk of insider attacks.

## ****10. Outdated Hardware****

Well, don’t be surprised. Not all challenges of Cyber Security come in the form of software attacks. With software developers realizing the risk of software vulnerabilities, they offer a periodic updates. However, these new updates might not be compatible with the hardware of the device. This is what leads to outdated hardware, wherein the hardware isn’t advanced enough to run the latest software versions. This leaves such devices on an older version of the software, making them highly susceptible to cyberattacks.

**Q2:** **Define information security?**

**Answer**:

To keep data safe, organisations employ a variety of methods and techniques that are together referred to as "Information Security" (InfoSec). Policy settings that prohibit unwanted access to commercial or personal information are included in this category.

Information security is one of the fastest growing and most diverse topics which includes everything from network and infrastructure security to auditing and testing. In general, there are two types of information: physical and digital. Information can be anything from your personal information to your social media profile, cell phone data, biometrics, and so on.

As a result, InfoSec comprises a wide variety of academic topics, including but not limited to:

* Cryptography
* Mobile computing
* Cyber forensics
* Online social media

In today's world, people no longer keep vital documents in safes or employ security guards to protect this information. Digital data is expected to be more frequently secured, therefore organisations must hire information security experts to establish protected zones. These zones include everything from virtual safes, installing antivirus security software and encrypting digital information using cryptographic methods.

**Q3:** **Explain the importance of information security?**

**Answer:**

Weak data security can lead to key information being lost or stolen, create a poor experience for customers and reputational harm. Data breaches, fraud, and cyber-security attacks are all becoming more common as people become more reliant on technology. Here are a few important reasons for organisations to implement information security systems.

* Information Security threats are very common

Threats to information security are increasingly common. Worms, viruses, data extortion, intellectual property theft, identity theft, and theft of physical equipment are among them. A common type of threat is something called ransomware. This is when a hacker prevents access to information or threatens to expose it until they are paid a set amount.

* The cost of a data breach

A security breach can take various forms, all of which can be costly. If you do not comply with the GDPR in the UK and EU, you may face fines of up to £17.5 million (€20 million) or 4% of your global revenue (whichever is higher),or temporary or permanent limits on processing and collecting data.

* State-sponsored hackers

Governments finance some hacker groups in order to disrupt or meddle with other countries' affairs. In one of the greatest cyber-attacks ever, Russian-sponsored hackers hacked thousands of US organisations over 8-9 months in 2020. Other international organisations, such as NATO and the European Parliament, were also impacted.

* IoT - Internet of Things

The internet of things (IoT) is a vast network of physical objects that have been equipped with software and sensors that allow them to connect to the internet and other devices. Smartphones, smartwatches, and smart houses are examples of IoT consumer items that can control everything from air conditioning to door locks from a single device. Many of these devices are vulnerable to cyber-attacks.

* Cyber-attacks increase during challenging times

Information security is critical at all times, but especially during times of emergency. A good example is the global epidemic. In 2020, cyberattacks doubled. Hospitals and pharmaceutical companies, for example, were badly affected. Many organisations have also been harmed by the widespread adoption of remote working, which leaves them more vulnerable to attack by hackers. No one can predict when a crisis will strike, but any organisation that deals with data should be prepared for the worst.

* Cyber-attacks are getting more sophisticated

Cyberattacks are becoming more sophisticated, making information security even more important and relevant. Hackers are getting better, but they also don't have to put in as much effort to be effective because of the advancements in technology. Also, they've become more organised, forming communities and exchanging information. The size of the groups do not matter as it is possible even for a small group of hackers to inflict significant harm on numerous networks at the same time.

When organisations begin to establish information security strategies, the above risks must always be kept in mind so that they can be adequately prepared to face them if ever needed.

**Q4: Developing Attacker Profiles?**

**Answer:**

Attack profiling is a valuable method for figuring out the motives of attacker, sharing threat intelligence and preparing response methods for expected future incident. This profiling can be performed based on not only IP and Code, but also actor's tactics, technics, mistake and any information used in operation.

****

Table 4-1 Attacker Profiles

**Q5: List and define information security terminology?**

**Answer:**

* **Unauthorized access** − An unauthorized access is when someone gains access to a server, website, or other sensitive data using someone else's account details.
* **Hacker** − Is a Person who tries and exploits a computer system for a reason which can be money, a social cause, fun etc.
* **Threat** − Is an action or event that might compromise the security.
* Vulnerability − It is a weakness, a design problem or implementation error in a system that can lead to an unexpected and undesirable event regarding security system.
* **Attack** − Is an assault on the system security that is delivered by a person or a machine to a system. It violates security.
* **Antivirus or Antimalware** − Is a software that operates on different OS which is used to prevent from malicious software.
* **Social Engineering** − Is a technique that a hacker uses to stole data by a person for different for purposes by psychological manipulation combined with social scenes.
* **Virus** − It is a malicious software that installs on your computer without your consent for a bad purpose.
* **Firewall** − It is a software or hardware which is used to filter network traffic based on rules.
* **VPN** - An acronym standing for Virtual Private Network, a VPN is a method of connecting a series of computers and devices in a private encrypted network, with each user’s IP address being replaced by the VPN’s IP address. Users get Internet anonymity, making it difficult for hackers to attack.
* **Worm** - Malware that can reproduce itself for the purposes of spreading itself to other computers in the network. Particularly nasty, worms can either be simply a means of slowing down a system by eating up resources, or by committing exploits such as installing back doors or stealing data.
* **Cloud** - You already utilize cloud computing if you use Gmail for email, Google Drive for document storage, or Netflix to stream your favorite movies. These services are all built on the cloud. [cloud computing](https://www.simplilearn.com/tutorials/cloud-computing-tutorial/what-is-cloud-computing) is providing on-demand services over the internet. If you want to run a business and you need to keep user data and you decide to do it on a hard drive, you will need a lot of storage space and a tech staff for it. Cloud service providers like Microsoft Azure, AWS, and Google Cloud, which offer on-demand services and are both cost-effective and low-risk in terms of security, make this procedure simple.
* **Rootkit** - A rootkit is a collection of programs or software tools that allow hackers to remotely access and control a computer or network.
* **BYOD (Bring Your Own Device)**-  Is a company policy that permits, encourages, or mandates employees to access enterprise systems and data using their own personal devices, such as laptops, tablets, and smartphones, for work-related activities.
* **Pen-testing -** An approach to security evaluation where manual exploitations and automated techniques are used by attack and security professionals.
* **Clickjacking -** While someone is tricked into clicking on one object on a web page when they want to click on another, this practice is known as clickjacking. In this manner, the attacker is able to use the victim's click against them. Clickjacking can be used to enable the victim's webcam, install malware, or access one of their online accounts.
* **Deepfake -** A piece of audio or video that has been altered and changed to make it seem authentic or credible. The most perilous aspect of the prevalence of deepfakes is that they can easily convince individuals into believing a particular tale or idea, which may lead to user behavior that has a greater impact on society at large, such as in the political or financial spheres.
* **User Authentication -** A technique to prevent unauthorized users from accessing sensitive data is user authentication. For instance, User A can only see data that is relevant and cannot view User B's sensitive information.
* **Ethical Hacking**- With the owner's permission, breaches the network to obtain sensitive information—completely legal. Typically, this technique is used to check for infrastructure weaknesses.
* **Cyber Attack -** Any attempt to breach a logical environment's security boundary. An attack may concentrate on intelligence gathering, disrupting company operations, exploiting weaknesses, keeping track of targets, stopping work, obtaining value, harming logical or physical assets, or leveraging system resources to enable assaults against other targets.
* **Trojan Horse -** Yet another form of malware, this one a misleading computer program that looks innocent, but in fact allows the hacker into your system via a back door, allowing them to control your computer.
* **Spyware -** A form of malware used by hackers to spy on you and your computer activities. If a mobile device such as a smartphone is infected with spyware, a hacker can read your text messages, redirect your phone calls, and even track down where you are physically located!
* **Spoofing -** Sadly, this has nothing to do with Weird Al Yankovic doing a parody version of a popular song. Rather, it’s when a hacker changes the IP address of an email so that it seems to come from a trusted source.
* **Ransomware -** A form of malware that hijacks your system and encrypts your files, denying you access to them until you send money to unlock everything. In other words, it kidnaps your computer and holds it for ransom, hence the clever name.
* **Phishing -** A scam where a hacker poses as a legitimate business or organization (especially credit card companies, banks, charities, Internet providers, other utilities) in order to fool the victim into giving them sensitive personal information or inducing them to click a link or attachment that ends up delivering malware. Some of these schemes are extremely well done, others are sloppy and amateurish and can be spotted with just a little extra vigilance.
* **Malware -** A portmanteau of “malicious” and “software”, describing a wide variety of bad software used to infect and/or damage a system. Ransomware, worms, viruses, and trojans are all considered malware. It most often delivered via spam emails.
* **Exploit -** A means of attack on a computer system, either a series of commands, malicious software, or piece of infected data. Note that in this context, “exploit” is a noun, not a verb, as in “The hacker used a malware exploit to gain access to the credit card’s server.”
* **DDoS -** The acronym stands for Distributed Denial of Service and is a favorite Black Hat tool. Using multiple hosts and users, hackers bombard a website with a tidal wave of requests to such an extent that it locks up the system and forces it to temporarily shut down.
* **Botnet -** A combination of the words “robot” and “network”, a botnet is a network of computers that have been infected with a virus, and now are working continuously in order to create security breaches. These attacks come in the form of Bitcoin mining, sending spam e-mails, and DDoS attacks (see below).
* **Domain -** A series of computers and associated peripherals (routers, printers, scanners), that are all connected as one entity.
* **Encryption -** Coding used to protect your information from hackers. Think of it like the code cipher used to send a top-secret coded spy message.
* **Authentication -** The process of identifying a user’s identity, making sure that they can have access to the system and/or files. This can be accomplished either by a password, retina scan, or fingerprint scan, sometimes even a combination of the above.