Apexa IQ Day 6 (Assignment 1)

Introduction to Cyber Security:

* *Definition*:

Cybersecurity is the practice of protecting computer systems, networks, devices, and data from cyber threats, unauthorized access, and digital attacks. It involves implementing security measures to ensure the **confidentiality, integrity, and availability (CIA)** of information. Cybersecurity aims to prevent data breaches, identity theft, malware infections, and other cyber risks by using technologies, processes, and best practices.

* *Importance of Cyber Security:*

Cybersecurity is crucial in today’s digital world as it protects individuals, businesses, and governments from cyber threats. Here’s why cybersecurity is important:

1. Protection Against Cyber Threats
2. Ensures Data Privacy and Confidentiality
3. Prevents Financial Losses
4. Maintains Business Continuity
5. Strengthens Trust and Reputation
6. Protects Critical Infrastructure
7. Supports National Security

* *Key Components of Cyber Security:*

1. Network Security:

Network security is the practice of protecting a computer network and its infrastructure from unauthorized access, cyber threats, and data breaches. It involves implementing hardware and software solutions to ensure the confidentiality, integrity, and availability of data transmitted across a network.

1. Cloud Security:

Cloud security is the practice of protecting cloud-based systems, data, and infrastructure from cyber threats, unauthorized access, and data breaches. It includes a combination of **technologies, policies, and best practices** to ensure the **confidentiality, integrity, and availability (CIA)** of cloud resources.

1. End Point Security:

Endpoint security refers to the practice of protecting devices (also known as endpoints), such as computers, smartphones, tablets, and Internet of Things (IoT) devices, from cyber threats and unauthorized access. Since endpoints are often the entry points for attackers to infiltrate a network, endpoint security is critical to prevent malware, ransomware, and data breaches.

1. Mobile Security:

Mobile security refers to the protection of smartphones, tablets, and other mobile devices from threats such as malware, data breaches, unauthorized access, and cyber attacks. It involves securing the devices, their operating systems, apps, networks, and the sensitive data they store or transmit.

1. IoT Security:

**IoT security** refers to the measures taken to protect **Internet of Things (IoT) devices** and networks from cyber threats and unauthorized access. These devices, which range from smart home products (like thermostats and cameras) to industrial equipment and healthcare devices, are often interconnected and vulnerable to attacks if not properly secured.

1. Application Security:

Application security refers to the practices, tools, and techniques used to protect software applications from cyber threats, vulnerabilities, and attacks throughout their lifecycle. This includes securing the code, environment, and overall application infrastructure to prevent unauthorized access, data breaches, and exploitation of weaknesses.

1. Zero Trust:

**Zero Trust** is a cybersecurity model based on the principle of "never trust, always verify." In a Zero Trust architecture, security is not determined by the location of the user or device (whether inside or outside the network), but by continuous verification of the user's identity, device security posture, and access request.

* *Common Threats and Types of Cyber Attack:*

Cyber Attacks come in various forms, each targeting different vulnerabilities in systems, networks, and data. Below are some of the **common types of cyber attacks** and their detailed descriptions:

1. Ransom ware attack:

**Ransomware attack** is a type of cyber attack where malicious software encrypts the victim's files or locks them out of their system, with the attacker demanding a ransom in exchange for the decryption key or to regain access to the system.

Ransomware attacks are often highly disruptive, with businesses, individuals, and even government organizations falling victim to these attacks, leading to financial and reputational damage.

1. Malware Attack:

A **malware attack** refers to the use of malicious software (malware) designed to damage, disrupt, or gain unauthorized access to a computer system, network, or device. The term "malware" is a broad category that includes various types of harmful software created to infiltrate systems, steal data, or cause damage.

1. Phishing Attack:

A **phishing attack** is a type of cyber attack where attackers impersonate a legitimate entity (such as a trusted company, government organization, or individual) in order to deceive victims into revealing sensitive information, such as login credentials, credit card numbers, or other personal data. Phishing attacks often occur via email, social media, or other communication channels.

1. DDoS (Distributed Denial of Service) attack:

A **DDoS attack** is a malicious attempt to disrupt the normal traffic of a targeted server, service, or network by overwhelming it with a flood of internet traffic. In contrast to a traditional **DoS (Denial-of-Service) attack**, where the attack is launched from a single source, a **DDoS attack** is executed from multiple, distributed sources (often thousands or more), making it harder to block and mitigate.

1. Password Attack:

A **password attack** is a type of cyber attack where attackers try to gain unauthorized access to a system or account by cracking or stealing a user's password. Since passwords are often the first line of defense for many online accounts, these attacks can lead to data breaches, financial loss, and identity theft.

1. DoD (Drive by Download) attack:

A **drive-by download** attack is a type of cyber attack where malicious software is automatically downloaded and installed onto a user's device without their knowledge or consent. This typically occurs when the user visits a compromised website or clicks on a malicious advertisement. The victim doesn't need to click on anything specifically for the malware to download—just visiting the website is enough to trigger the attack.

Asset Management

* *Definition*:

Asset management involves the process of tracking, maintaining, and optimizing an organization’s assets to maximize their value and performance. These assets can be both **physical** (such as hardware, buildings, and equipment) and **digital** (such as software, data, and intellectual property). Effective asset management ensures that assets are properly utilized, secured, and compliant with relevant regulations.

Asset management typically includes the **identification**, **monitoring**, **maintenance**, and **disposal** of assets, ensuring their lifecycle is well-managed.

* *How Asset Management Works?*

Following are the processes of the Asset Management:

Here’s a summarized list of how asset management works:

1. Asset Identification
   * Catalog assets
   * Tag assets with unique identifiers (barcodes, RFID, serial numbers)
   * Map assets and their relationships
2. Asset Tracking & Monitoring
   * Track asset location and user
   * Monitor asset condition and performance
   * Track asset usage patterns
3. Asset Maintenance
   * Perform routine maintenance and updates
   * Schedule repairs as needed
   * Ensure software/hardware remains up-to-date
4. Asset Optimization
   * Maximize asset utilization
   * Manage asset lifecycle (procurement to disposal)
   * Identify opportunities to reduce costs
5. Compliance & Risk Management
   * Ensure regulatory compliance (e.g., GDPR, HIPAA)
   * Assess and mitigate risks (theft, data loss, failure)
   * Conduct periodic audits
6. Asset Disposal or Decommissioning
   * Securely dispose of or recycle old assets
   * Delete sensitive data before disposal
   * Document the disposal process
7. Reporting & Analysis
   * Generate reports on asset performance, usage, and maintenance
   * Use insights for decision-making and future purchases
8. Asset Management Tools
   * Use asset management software (ServiceNow, Lansweeper)
   * Utilize ERP systems (SAP, Oracle)
   * Implement CMDB for IT asset tracking

* *IT Asset Management:*

**IT Asset Management (ITAM)** is the process of managing and tracking an organization's information technology (IT) assets throughout their lifecycle. This includes hardware, software, network resources, and digital assets. The goal of ITAM is to ensure that IT resources are utilized efficiently, properly maintained, secure, compliant, and cost-effective.

* *The IT Asset Management Process:*

IT asset management is not a project. You don’t do it once and expect it to be finished. ITAM is a process that teams execute on a regular basis or as assets, goals, and tools change.

**Inventory assets** - The first step in the IT asset management process is to create a detailed inventory of all IT assets. Your inventory includes what assets you have, where they are located when they were purchased, and for how much.

**Calculate lifecycle costs** - The second step is to calculate lifecycle costs for all assets in your inventory. During an average asset’s life, there are many opportunities for added costs, like maintenance, capital, and disposal costs. Calculating lifecycle costs makes your asset inventory accurate and actionable.

**Tracking** -  The third step is tracking via an asset management tool. Your goal is to continuously monitor IT assets through their lifecycle keeping a close eye on things like contract, license, and warranty expiration. Tracking also helps you stay ahead of the fourth step, maintenance.

**Maintenance** - Maintenance involves asset repair, upgrade, and replacement. All maintenance activities should be tracked in an ITAM tool so that the data can be used to understand the overall performance of the asset.

**Financial Planning** - The fifth and final step is financial planning. With an accurate picture of your IT assets, their lifecycle stage, and their costs, you can effectively plan for the future. One goal of financial planning is to determine the budget needed to maintain or improve the “levels of service” your team provides for your most important assets. An asset that was successfully managed with a high level of service, like a service desk and dedicated team, will need that level of service going forward. Assets that underperformed may need a higher level of service in the future, which will cost more.

* *Cyber Security Asset Management:*

Cybersecurity asset management (CSAM) is the process created to continuously discover, inventory, monitor, manage and track an organization's assets to determine what those assets do and identify and automatically remediate any gaps in its cybersecurity protections.

* *Cyber Security best practices for any Organization:*

1. Multifactor Authentication
2. End Point Security
3. Keeping the software Up to Date
4. Backup your Data
5. Setup a Firewall
6. Use a strong Password

* *Similarities Between ITAM and CSAM*

1. Asset Identification and Inventory: Both ITAM and CSAM involve maintaining a comprehensive inventory of assets, whether they are physical IT assets or cybersecurity-specific assets.
2. Lifecycle Management: Both manage assets throughout their lifecycle, from procurement through usage and maintenance, to disposal or decommissioning.
3. Compliance and Auditing: Both ITAM and CSAM require compliance with relevant regulations, ensuring that assets meet legal and industry standards. This could include financial audits for ITAM and cybersecurity regulations for CSAM.
4. Asset Tracking: Both systems involve tracking assets in terms of usage, location, and condition. While ITAM tracks hardware and software, CSAM tracks cybersecurity tools, network devices, and digital resources.
5. Automated Tools: Both use asset management software to automate processes like discovery, tracking, and reporting. These tools streamline asset management tasks, whether for general IT or security-focused assets.

* *Differences Between ITAM and CSAM*

1. Scope: ITAM manages all IT assets (hardware, software, network devices), while CSAM is specifically concerned with cybersecurity assets like firewalls, encryption tools, and security software.
2. Primary Goal: ITAM aims to optimize the operational efficiency, cost-effectiveness, and performance of IT resources. In contrast, CSAM focuses on ensuring cybersecurity assets are secure, up-to-date, and resilient against threats.
3. Security Focus: ITAM addresses operational security (e.g., hardware failure, asset loss), whereas CSAM places a stronger emphasis on protecting assets from cyber threats, such as vulnerabilities and attacks.
4. Compliance: ITAM ensures compliance with regulations related to asset licensing, procurement, and financial management. CSAM ensures compliance with cybersecurity regulations like data protection laws and vulnerability management standards.
5. Lifecycle Focus: ITAM emphasizes operational aspects like asset performance and cost management, while CSAM focuses more on the security lifecycle, which includes patching, updates, and vulnerability management.
6. Tools Used: ITAM uses asset management software such as SAP or ServiceNow, which focus on general asset tracking and management. CSAM uses security-specific tools like SIEM systems and vulnerability scanners to track and monitor cybersecurity assets.
7. Risk Management: ITAM primarily deals with operational and financial risks, such as asset underutilization or loss. CSAM focuses on cybersecurity risks, including data breaches, malware, and vulnerabilities in security systems.

* *Emerging trends in Cyber Security:*

1. Zero Trust Architecture

The zero trust model assumes that every user, device, and network is untrusted by default, regardless of location. Security measures are applied continuously, verifying users and devices before granting access.

1. Artificial Intelligence (AI) and Machine Learning (ML) in Security

AI and ML are being increasingly used for detecting patterns, predicting threats, and automating responses. These technologies can help identify unusual behavior or potential threats more quickly and accurately than traditional methods.

1. Extended Detection and Response (XDR)

XDR provides a more integrated approach to threat detection and response by combining data from multiple security layers (e.g., endpoint, network, and cloud). It offers better visibility and streamlined incident response.

1. Cloud Security

As more organizations move to cloud environments, securing cloud-based assets and services becomes critical. Cloud security is focusing on areas like identity management, encryption, and securing the cloud supply chain.

1. Cybersecurity Mesh Architecture (CSMA)

CSMA enables a more flexible and scalable approach to security by decentralizing security perimeters. It ensures that security policies are applied uniformly, even across complex and distributed IT environments.

1. Privacy-Enhancing Computation

This involves techniques like homomorphic encryption and secure multi-party computation, which allow data to be processed and analyzed without exposing it. This is especially useful for compliance with data protection regulations like GDPR.

1. Automated Incident Response

Automation is increasingly being applied to incident response workflows. This includes using AI-driven tools to automatically detect, analyze, and respond to security incidents, reducing response times and human error.

1. Ransomware Defense and Mitigation

Ransomware attacks continue to evolve, and organizations are investing more in prevention, detection, and response strategies, including data backup solutions, threat intelligence, and network segmentation.

1. Quantum Cryptography

With the potential rise of quantum computing, quantum cryptography is being explored as a way to secure data transmission and protect against the threat posed by quantum decryption of traditional encryption methods.

1. Identity and Access Management (IAM) Evolution

IAM is evolving with more advanced techniques like passwordless authentication, biometric verification, and continuous authentication to strengthen user identity security and improve overall access control.

1. Cybersecurity for Remote Work

With the increase in remote work, securing endpoints, virtual private networks (VPNs), and collaboration tools is becoming a top priority. This includes ensuring secure access to company resources from home or public networks.

1. Supply Chain Security

Supply chain attacks, where cybercriminals target an organization’s suppliers, are on the rise. Companies are increasingly focusing on securing their third-party vendors and the broader ecosystem in which they operate.

1. Security for Internet of Things (IoT)

As the number of IoT devices grows, securing these connected devices becomes more critical. Efforts are focused on ensuring robust authentication, secure data transmission, and timely updates for IoT devices.

1. Privacy and Data Protection Regulations

Increasingly stringent data protection regulations (e.g., GDPR, CCPA) are driving companies to adopt more robust privacy practices and security measures. This trend is also influencing the adoption of technologies that support data sovereignty and privacy.

1. Behavioral Analytics

Behavioral analytics is being applied to monitor and detect abnormal user behaviors that may indicate a potential insider threat or account compromise. By analyzing normal user behavior, it becomes easier to spot deviations that could signal malicious actions.

* Case Study of Big Basket Data Breach:

*Introduction*:

Big Basket is the largest online grocery supermarket in India. It was launched in 2011, quite about the time when e-commerce was in its nascent stage in the country. Big basket was founded by Hari Menon, VS Sudhakar, V S Ramesh, Vipul Parekh and Abhinay Choudhari.

India’s top online grocer Big Basket has suffered a potential data breach resulting in personal information of over 20 million customers being allegedly sold on the dark web. This incident follows a series of data breaches that have impacted Indian companies.

*Big Basket Data Breach:*

According to cybersecurity firm Cyble, which first made the details of the potential breach public, the alleged breach occurred on October 14. The firm said that it first detected the breach on October 30 and after validating the breach, it disclosed the breach to the BigBasket management on November 1. The cybersecurity firm made the details of the breach public on November 7. Big basket has faced a potential data breach which could have leaked details of around 2 crore users, according to cyber intelligence firm Cyble.

The company has filed a police complaint in this regard with Cyber Crime Cell in Bengaluru and is verifying claims made by cyber experts. Cyble said that a hacker has put data allegedly belonging to Big Basket on sale for around Rs 30 lakh. It was found that the database of Big Basket for sale in a cybercrime market, being sold for over USD 40,000.

The SQL file that consists the sensitive data is about 15 GB, containing close to 20 million user info. It added the data put on sale includes names, email IDs, password hashes, contact numbers (mobile and phone), addresses, date of birth, location, and IP addresses of login among many others.

The privacy and confidentiality of our customers is our priority and we do not store any financial data including credit card numbers etc., and are confident that this financial data is secure. The only customer data that we maintain are email ids, phone numbers, order details, and addresses so these are the details that could potentially have been accessed,” BigBasket said.

If one only goes by the information released by Cyble, there have been six cases of cyber breaches in India in the last one month alone like Haldiram Snacks Pvt Ltd, Wedmegood, Bharat Matrimony & IRCTC along with PM’s website.

*Conclusion*:

Organizations must start taking cybersecurity seriously or risk falling victim to a cybersecurity attack themselves. If a customer trusts you with their personal data, you owe it to them to keep that data safe. This breach is particularly worrying because it appears that customers’ payment details were available to hackers and these details can be used for a range of nefarious purposes. Most simply, these details can be sold for financial gain on the dark web, with the prospective buyer able to use the data to impersonate a victim or lead them to a different domain. We found that the retail & wholesale sector has been the top targeted sector. This is highly likely to remain a target due to the strong financial motivation of criminals, increased E-Commerce activity likely due to renewed lockdown measures, the potential for data and/or credential exfiltration, as well as third-party compromise if an attack is successful.