1.1 The World Of Cyber Security

Cyber Crime is growing, one study estimates that malicious hackers are attacking computer and network at a rate of 1 attack every 39 seconds, posing major threat to personal info, organizational data and national security. As cyber attacks become more sophisticated and more global, cyber defender is required. A cyber security professional helps people/organization from falling victim to cybercrime.

A entry level Security Analyst helps building the defense and safeguard the company from attacks by making the right cyber decisions.

1.1.1 : what is Cyber Security?

Cyber Security is the effort to protect indivisuals, organizations and the government from digital attacks by protecting networked system and data from unauthorized use.

Personal level - safeguard your identity, data and computing device.

Organization level - it's everyones responsibility to protect the companys data.

Government level - As more digital information is exchanged, its protection becomes even more vital at the government level, where national security, economic stability and the safety and wellbeing of citizens are at stake.

1.1.2 : Protecting Your Personal Data

Personal data is information that can identity you, and it can be both offline and online.

Offline Identity - What you are in real life. For example, family and friends know details about your personal life, including full name, age, address, occupation, etc

Identity thieves can eaasily steal your data.

Online Identity - Name is not the only online identity, how you present yourself to others online can reveal alot, ex, username/alias of online accounts, social identities you establish and portray on online communities and websites. Limit the amount of personal information you real through online identity.

Note : Many people think that if they don’t have any social media or online accounts set up, then they don’t have an online identity. This is not the case. If you use the web, you have an online identity.

1.1.3 : Your Online Identity

when choosing username, it is important not to reveal any personal info.

Don't use : full name, part of address, phn no. , email, reuse username, also dont give clues to your password.

1.1.4 : Your Data

Personal data describes any information about you. Ex, name,driver license number, date and place of birth, etc. Cybercriminals use this sensitive informations to identify and immpersonate you and cause serious damage to your reputation.

Medical records : Every visit to doctor, personal information about your health is added to EHRs (Electronic Health Records). Since these information is saved online be aware about what you share.
Not just doctors office, even many fitness trackers collect large amounts of clinical data such as your heart rate, blood pressure and blood sugar levels, which is transferred, stored and displayed via the cloud. Therefore, you should consider this data to be part of your medical records.

Education records : Educational records contain information about your academic qualifications and achievements. However, these records may also include your contact information, attendance records, disciplinary reports, health and immunization record.

Employment and financial records : Employment data can be valuable to hackers if they can gather information on your past employment. Your financial records may include information about your income and expenditure. Your tax records may include paychecks, credit card statements, your credit rating and your bank account details. All of this data, if not safeguarded properly, can compromise your privacy and enable cybercriminals to use your information for their own gain.

1.1.5 : Where is your data?

Once you upload a photo to any social media platform, the photo no longer belongs to 'only you', the photo is now on servers located in different parts of the world and anyone can access the photo, and can use the photo for any malicious purpose.

1.1.6 : What's more...

we should be more careful about collecting and sharing personal data and consider our security. Different countries have different laws about privacy and data. For example, expanding on the medical report information,
the doctors appointment bill might be shared to your insurance company, in that case part of the medical record will accessible to the insurance company.

store loyalty cards might save money on purchases, but this also builds a profile on your purchasing behavior and later target you with special offers.

1.1.7 : Smart Devices

Computing devices can generate information about you. Smartwatches or activity trackers collect data for research, patient health monitoring, and fitness wellbeing tracking. So the risk of personal data sharing grows.

Information available online is free, but is privacy the price we pay for this digital convenience?

For example, social media companies generate the majority of their income by selling targeted advertising based on customer data that has been mined using algorithms or formulas. Of course, these companies will argue that they are not ‘selling’ customer data, but ‘sharing’ customer data with their marketing partners.

1.1.8 : What do Hackers want?

Cybercriminals are certainly very imaginative when it comes to gaining access to your money. But that’s not all they are after, they could also steal your identity and ruin your life.

1.1.9 : Identity Theft

Stealing your money for short-term financial gain, cybercriminals are invested in the long-term gain of identity theft.

Medical Theft : Rising medical costs led to increase in medical identity theft, with cybercriminals stealing medical insurance. Any medical procedures carried out in your name will then be saved in your medical records.

Banking : Stealing private data can help cybercriminals access bank accounts, credit cards, social profiles and other online accounts. Armed with this information, an identity thief could file a fake tax return and collect the refund. They could even take out loans in your name.

1.1.10 : Who else want your data?

its not just criminals who seek your data.

ISP : tracks your online activity, sell information to advertisers for profit. In certain circumstances, ISP may be legally required to share your info with government surveillance agencies.

Advertisers : targeted ads are part of the internet experience. Advertisers monitor tour online activity and personal preferences and send targeted ads.

Search Engines and Social Media Platforms : these platform gathers info about your gender, geolocation, phn no. , etc and sell to advertisers for a profit.

Websites : Websites uses cookies to track activites to provide a more personalized experience. This leaves a data trail that is linked to online identity that often ends up to advertisers.

1.2.1 Types of Data

- Transactional data (details of sales, products, etc)
- Intellectual property (patents, trademarks, plans)
- Financial data (income statements, balance, cash flow)

1.2.2 The Cube

McCumber Cube is a model framework created by John McCumber in 1991, to evaluate information security by considering all of the related factors that impact them.

1. The foundational principles for protecting information systems.
2. The protection of information in each of its possible states.
3. The security measures used to protect data.

1. The foundational principles for protecting information
    - Confidentiality : rules that prevent unauthorized people to access data. (Method: encryption, 2FA)
    - Integrity : ensures that information is protected from intentional or accidental modifications (Method: Hash Function, Checksum)
    - Availability : data is ready to authorized users all the time. (maintenance, performing hardware repairs, up to date software)

2. The protection of information in each state
    - Processing : data being used to perform operation such as update database record.
    - Storage : data stored in memory, hard drive, SSD, USB (data at rest)
    - Transmission : data travelling between information system (data in transit)

3. The security measures used to protect data
    - Awareness, Training and Education : ensures users with knowledge about potential security threats and actions to take to protect data
    - Technology : software and hardware based solutions to protect information (firewalls)
    - Policy and Procedure : admin control that provide assurance, incident response plan and best practice guidelines

1.3 What was taken

A security breach is an incident that results in unauthorized access to data, applications, services or devices, exposing private information that attackers can use for financial gain or other advantages.

But there are many ways to protect yourself and your organization. Itâ€™s important to be aware of common cyber threats and remain vigilant so that you donâ€™t become the next victim.

Amateurs : The term 'script kiddies' emerged in the 1990s inexperienced hackers who use existing tools or instructions found on the Internet to launch attacks. Some script kiddies are just curious, others are trying to demonstrate their skills and cause harm. While script kiddies may use basic tools, their attacks can still have devastating consequences.

Hackers : This group of attackers break into computer systems or networks to gain access. Depending on the intent of their break in, they can be classified as white, gray or black hat hackers.

- White hat : attackers break into networks or computer systems to identify any weaknesses so that the security of a system or network can be improved. These break-ins are done with prior permission and any results are reported back to the owner.

- Gray hat : attackers may set out to find vulnerabilities in a system but they will only report their findings to the owners of a system if doing so coincides with their agenda. Or they might even publish details about the vulnerability on the internet so that other attackers can exploit it.

- Black hat : attackers take advantage of any vulnerability for illegal personal, financial or political gain.

Organized hackers : These attackers include organizations of cyber criminals, hacktivists, terrorists and state-sponsored hackers. They are usually highly sophisticated and organized, and may even provide cybercrime as a service to other criminals.

Hacktivists make political statements to create awareness about issues that are important to them.

State-sponsored attackers gather intelligence or commit sabotage on behalf of their government. They are usually highly trained and well-funded and their attacks are focused on specific goals that are beneficial to their government.

1.5.2 The Purpose of Cyberwarfare

The main reason for resorting to cyberwarfare is to gain advantage over adversaries, whether they are nations or competitors.

- To gather compromised information and/or defense secrets

  steal defense secrets and gather information about technology that will help narrow the gaps in its industries and military capabilities

- To impact another nationâ€™s infrastructure

  A nation can continuously invade another nationâ€™s infrastructure in order to cause disruption and chaos.

1.6 QUIZ

Scored 70% of the quiz questions.