Mark Anasarias
BSIT 401

Question #1

How can identify if an information is at risk?

Identifying if information is at risk involves conducting a comprehensive risk assessment to evaluate potential threats, vulnerabilities, and consequences, classifying data based on its sensitivity, reviewing access controls and permissions, ensuring adequate encryption, evaluating security policies and procedures, implementing monitoring tools and logging mechanisms, considering physical security measures, assessing vendor and third-party risk, conducting regular audits and assessments, and educating employees about the importance of information security and their roles and responsibilities in protecting sensitive information.

How will you manage that risk?

Managing the identified risks involves implementing appropriate measures to mitigate, transfer, or accept them based on the organization's risk tolerance and objectives, which includes strategies such as risk mitigation, transfer, and acceptance, continual monitoring and review, incident response planning, employee training and awareness, regular testing and evaluation, compliance with regulations and standards, and executive and stakeholder engagement.

Question #2

Why do we need to study computer security?

Studying computer security is essential because it enables the protection of sensitive information, prevention of cyberattacks, preservation of privacy, assurance of business continuity, compliance with regulations, safeguarding of critical infrastructure, promotion of trust and confidence, support for technological innovation, and access to diverse career opportunities in cybersecurity.

What is its importance?

The importance of studying computer security lies in its role in protecting sensitive information, preventing cyberattacks, preserving privacy, ensuring business continuity, complying with regulations, safeguarding critical infrastructure, promoting trust and confidence, supporting technological innovation, and providing access to diverse career opportunities in cybersecurity.

And how can it prevent information from being at risk?

Computer security prevents information from being at risk through various measures such as implementing access controls, encryption, and authentication mechanisms to restrict unauthorized access. It also involves regular monitoring and auditing of systems, prompt patching of security vulnerabilities, educating users about security best practices, enforcing strong password policies, and implementing intrusion detection and prevention systems to detect and respond to threats in real-time. Additionally, robust incident response plans and backup procedures help mitigate the impact of security incidents and ensure the continuity of operations. By implementing these preventive measures comprehensively, computer security helps mitigate risks and safeguard information from unauthorized access, disclosure, alteration, or destruction.

Question #3

What is the difference between cyber security and computer security?

Cybersecurity encompasses the protection of digital assets, including computers, networks, data, and information systems, from cyber threats and attacks, while computer security specifically focuses on safeguarding individual computer systems, devices, and software applications from unauthorized access, misuse, and malicious activity, highlighting the broader scope of cybersecurity and the more specific focus of computer security.

Question #4

How can the following terms be a risk on computing?

- **Vulnerability**

A vulnerability in computing represents a weakness or flaw in a system's design, implementation, or configuration that could be exploited by attackers to compromise security.

- **Backdoor**

A backdoor is a hidden or undocumented means of accessing a system, application, or network that bypasses normal authentication and security mechanisms, posing significant risks to computing environments.

- **Tampering**

Tampering represents a risk in computing due to unauthorized alteration or modification of data, software, or hardware components within a system, potentially compromising data integrity and system reliability.

- **Repudiation**

Repudiation risk arises when users deny having performed certain actions or transactions within a computing system, leading to disputes, legal issues, and challenges in holding individuals accountable for unauthorized activities.

- **Information Disclosure**

Information disclosure poses a significant risk in computing environments by exposing sensitive or confidential data to unauthorized individuals, potentially leading to privacy violations, identity theft, financial losses, and reputational damage.

Question #5

How can the following tips helps on preventing cyber crime?

- **Use Strong Passwords**

Using strong passwords, incorporating a mix of uppercase and lowercase letters, numbers, and special characters, helps thwart cybercriminals by increasing the complexity of passwords and making unauthorized access more difficult.

- **Secure your Computer**

Securing your computer involves keeping software and antivirus applications up-to-date to patch vulnerabilities, installing firewall software for additional protection, and regularly backing up critical data to mitigate the impact of potential cyberattacks or system failures.

- **Be Social-Media Savvy**

Being social-media savvy plays a crucial role in preventing cybercrime by exercising caution in sharing personal information online, avoiding clicking on suspicious links, and steering clear of social engineering scams that could compromise your privacy and security.

- **Secure your Mobile Devices**

Securing your mobile devices by implementing passcodes, PINs, or biometric authentication, installing security software, and keeping operating systems and apps updated helps protect against unauthorized access, malware infections, and other mobile-specific cyber threats, enhancing overall cybersecurity.

Question #6

How can following tips helps on preventing cyber crime?

- **Avoid being scammed**

Avoiding being scammed involves staying vigilant and skeptical of suspicious emails, messages, phone calls, or websites, verifying the legitimacy of requests for personal or financial information, and exercising caution to prevent falling victim to various forms of scams, including phishing, identity theft, and financial fraud.

- **Call the right person for help**

Calling the right person for help, such as official customer support lines, financial institutions, or law enforcement agencies, enables individuals to verify the authenticity of requests, obtain timely assistance in case of suspected cybercrime, and seek guidance from knowledgeable professionals or cybersecurity experts to address security concerns and mitigate risks effectively.