Name: NKWINE INNOCENT

Reg No: 2019/U/ISM/00153

ASSIGNMENT ONE

No 1: identify the five factors that contribute to the increasing vulnerability of information resources and provide the specific example of each one.

An information resource’s vulnerability is the possibility that the system will be harmed by a threat. Today, five key factors contributing to the increasing vulnerability of organizational information resources, making it much more difficult to secure them include:

* Interconnected, interdependent, and wirelessly-networked business environment. The evolution of the IT resource from mainframe-only to today’s highly complex, interconnected, interdependent, wirelessly networked business environment has now enabled millions of computers and computer networks to communicate freely and seamlessly with one another and as a result the organizations’ employees communicate and access internet anywhere any time which exposes the organizations’ information resources to untrusted networks.
* Presence of smaller, faster, cheaper computers and storage devices for example thumb drives or flash drives. This makes it much easier to steal or lose a computer or storage device that contains huge amounts of sensitive information. Also, far more people are able to afford powerful computers and connect inexpensively to the Internet, thus raising the potential of an attack on information assets for example an employee of an organization can copy a sensitive information on a flash drive and sell it the competitors.
* Decreasing skills necessary to be a hacker. This is because the Internet contains information and computer programs called scripts that users with few skills can download and use to attack any information system connected to the Internet.
* Organized crime taking over cybercrime. The network, powered by skillful hackers, targets known software security weaknesses. These crimes are typically nonviolent, but quite lucrative and the culprits are to truck since computer crimes can be committed from anywhere in the world, at any time, effectively providing an international safe haven for cybercriminals thus increasing vulnerability of information resources.
* Lack of management support in organizations. For the entire organization to take security policies and procedures seriously, senior managers must set the tone.
* Ultimately, however, lower-level managers may be even more important. These managers are in close contact with employees every day and thus are in a better position to determine whether employees are following security procedures (Dr.Bravery, 2011).

No 2: Compare and contrast human mistakes and social engineering and provide a specific example for each.

Social engineering is a manipulation technique that exploits human error to gain private information, access, or valuables. In cybercrime, these “human hacking” scams tend to lure unsuspecting users into exposing data, spreading malware infections, or giving access to restricted systems that is , getting around security systems by tricking computer users inside a company into revealing sensitive information or gaining unauthorized access privileges (Micke, 2021). Attacks can happen online, in-person, and via other interactions for example notifying you that you’re a ’winner.’ the email claims to be from a lottery and that in order to give you your ’winnings’ you have to provide information about your bank routing so they know how to send it to you or give your address and phone number so they can send the prize, and you may also be asked to prove who you are often including your social security number.

On the other hand human mistakes means unintentional actions - or lack of action - by employees and users that cause, spread or allow a security breach to take place. Human mistakes are typically the result of laziness, carelessness, or lack of awareness concerning information security. An example of this is losing or misplacing a laptop that contains sensitive information

No 3: Discuss the 10 types of deliberate attacks

Deliberate attacks done by cybercriminals to gain unauthorized access to an organization's network.

Types of deliberate attacks include;

1. Espionage or Trespass. Espionage or trespass occurs when an unauthorized individual attempts to gain illegal access to organizational information. It is important to distinguish between competitive intelligence and industrial espionage. Competitive intelligence consists of legal information-gathering techniques, such as studying a company’s Web site and press releases, attending trade shows, and so on. In contrast, industrial espionage crosses the legal boundary.
2. Information Extortion. Information extortion occurs when an attacker either threatens to steal, or actually steals, information from a company. The perpetrator demands payment for not stealing the information, for returning stolen information, or for agreeing not to disclose the information.
3. Sabotage or Vandalism. Sabotage and vandalism are deliberate acts that involve defacing an organization’s Web site, possibly damaging the organization’s image and causing its customers to lose faith. One form of online vandalism is a hacktivist operation. These are cases of high-tech civil disobedience to protest the operations, policies, or actions of an organization or government agency.
4. Theft of Equipment or Information. This occurs when an individual tries to steal an organization information equipment. Computing devices and storage devices are becoming smaller yet more powerful with vastly increased storage. As a result, these devices are becoming easier to steal and easier for attackers to use to steal information.
5. Identity Theft. Identity theft is the deliberate assumption of another person’s identity, usually to gain access to his or her financial information or to frame him or her for a crime. Techniques for illegally obtaining personal information include: stealing mail or dumpster diving, stealing personal information in computer databases among others. Recovering from identity theft is costly, time consuming, and difficult. Victims also report problems in obtaining credit and obtaining or holding a job, as well as adverse effects on insurance or credit rates. In addition, victims state that it is often difficult to remove negative information from their records, such as their credit reports.
6. Software Attacks. This is when attackers use malicious software to infect organization’s computers or steal money from the targets.
7. Cyberterrorism and Cyberwarfare. Cyberterrorism and cyberwarfare refer to malicious acts in which attackers use a target’s computer systems, particularly via the Internet, to cause physical, real-world harm or severe disruption, usually to carry out a political agenda.
8. Supervisory Control and Data Acquisition (SCADA) Attacks. This is unauthorized access into a SCADA system in order to cause harm. SCADA is responsible for acquiring real-time data from a physical system and managing the physical system or presenting the data to humans, who monitor and manage the system. If attackers gain access to the network, they can cause serious damage, such as disrupting the power grid over a large area or upsetting the operations of a large chemical or nuclear plant
9. Alien software (pestware).This is a clandestine software that is installed on your computer without your knowledge. It can enable other parties to track your web surfing habits, adware (vast majority of pestware), spyware (keystroke loggers, screen scrapers), spamware (spam) cookies (tracking cookies)
10. Compromise intellectual property. Intangible creative work that is embodied in physical form and includes copyrights, trademarks, and patents(Uma & Padmavathi, 2013).

No 4: Define the three risk mitigation strategies and provide an example of each one in the context of owning a home

1. Risk acceptance: accept the potential risk, continue operating with no controls, and absorb any damages that occur which means accepting the risk as it stands this occurs when the possibility of reward outweighs the risk, and it’s more beneficial in the long run to take the chance for example accepting the risk of fire outbreak in your home and be willing to take care of the damages that may be caused should the fire outbreak actually occur
2. Risk limitation: limit the risk by implementing controls that minimize the impact of the threat for example installing fire extinguishers in your home to minimize damages in case of any fire outbreak.
3. Risk transference: transfer the risk by using other means to compensate for the loss that is passing the risk consequence to a third party such as by purchasing insurance. An example of this in the context of owning a home is having a fire insurance for your house so that you get compensated for the damages caused in case of fire outbreak.

No 5: Identify the three major types of controls that organizations can use to protect their information resources, and provide an example of each one.

* Physical controls. Preventing unauthorized individuals from gaining access to a company's facilities. For example use of fencing, gates, locks, badges to prevent any unauthorized access to an organization’s information facilities like server rooms.
* Access Controls. Restricting unauthorized individuals from using information resources. For example use of passwords to ensure that only authorized individuals can access the organization network
* Communications Controls. Securing the movement of data across networks. Consist of firewalls, anti-malware systems, whitelisting and blacklisting for example installing firewalls that filter the traffic in the organization network and blocks any communication from a suspicious source (Chris & Mike, 2011).

Ref:

Chris, D., & Mike, S. (2011). *IT Auditing: Using Controls to Protect Information Assets*.

Dr.Bravery, M. (2011). *Five Factors Increasing the Vulnerability of Information Resources Todays | Course Hero*. https://www.coursehero.com/file/p6cimrv/Five-Factors-Increasing-the-Vulnerability-of-Information-Resources-Todays/

Micke, A. (2021). *The Role of Human Error in Successful Cyber Security Breaches*. https://blog.usecure.io/the-role-of-human-error-in-successful-cyber-security-breaches

Uma, M., & Padmavathi, G. (2013). A Survey on Various Cyber Attacks and Their Classification. *International Journal of Network Security*, *15*(5), 390–396.