Assignment 2-8-2021

Use any editor to answer the question, copy the question and write your answer below it.

1. Enumerate and identify the definition or focus of the different Federal organization that defined Information Assurance. 5 pts.

Committee on National Security Systems (CNSS)

The Committee on National Security Systems organizes policy meetings and develops national policy, directions, operational guidelines, and policy for the American information systems. The government, its contractors, or agents that have access to classified information are engaged in intelligence gathering, national security-related cryptographic work, command and control of armed forces, work on equipment that is essential to the successful completion of military or intelligence missions, or both. Additionally, the CNSS creates federal policy guidelines for network security and authorizes institutions to provide security certifications.

National Security Agency (NSA)

The duty of developing and testing secure systems for diverse applications that are regarded as classified falls within the purview of the National Security Agency, which collaborates with prominent cryptography groups. To better advance their mission for ensuring the future, the NSA coordinates with sectors in industries on security development. The NSA is responsible for safeguarding American communications networks and information systems as well. To carry out its goal, the NSA employs a number of techniques, the bulk of which are conducted through military operations so that the operation is undetectable to the general public.

National Institute of Standards and Technology (NIST)

The National Bureau of Standards was the previous name for the National Institute of Standards and Technology. Its goal is to advance measuring standards, science, and technology in ways that enhance our quality of life and economic security, which in turn encourages innovation and industrial competitiveness.

2. What is an asset? Why is it worth protecting? 5 pts.

An asset is something with value. In this context, an information asset is any data, device or other component of an organization's systems that is valuable – often because it contains sensitive data or can be used to access such information. Such assets are worth protecting because in this day and age, assets are power. Assets are worth money. Assets are of tremendous value and can provide certain value depending on how it is used. If assets are stolen, this can cause tremendous loss monetarily and also intellectually.

3. Can you specify examples for objects, subjects and (aside from the given) 10 pts.

- The Windows Operating System allows users(**subject**) to alter(**action**) system settings such as display, network, and privacy(**objects**).
- Web browsers allow end-users/consumers(**subject**) to view(**action**) shared information(**object**) on the Internet.

4. Enumerate and give examples for the different types of threat. 10 pts.

- **Interruption**
  - a denial-of-service attack on a website
  - overloading a server host so that it cannot respond.
- **Interception**
  - compromise of confidential data, packet-sniffing
  - key-logging
- **Modification**
  - hacking to deface a website
  - changing information stored in data files
- **Fabrication**
  - spoofing attacks in a network
  - user credential counterfeiting

5. Describe the local enclave of the University of San Carlos. 10 pts.

From what I've seen in the Bunzel Building, there are several computer labs having their own computing environment and network. I believe each network has a moderator per laboratory. All these computers fall under the authority of an all-access network administrator that has privilege access. There is also a security policy that prevents computers in the laboratory from accessing certain websites that are non-educational. The control of network access by these known users is made easier by cybersecurity initiatives, and security mechanisms are put in place to stop unauthorized intrusions.

6. Differentiate exploit and attack? 5 pts.

An attack is an attempt to gain access, cause damage to or otherwise compromise information and/or systems that support it while an exploit is a method for taking advantage of a known vulnerability which can lead to an attack.

7. Can you give examples of dangling vulnerability and dangling threat or any situation which might occur? 5 pts.

Dangling Vulnerability:

- Unvalidated Redirects and Forwards
- A dangling markup injection where an attacker can use syntax to break out of a quoted attribute value and an enclosing tag.

Dangling Threat:

- Public Wi-Fi Network is accessible to hackers but there is no device connected to it.
- A dangling DNS record which can be exploited when a resource in the network is abandoned and released.

8. Try to follow this procedure to manage risks to your material possessions stored at your home or apartment, any instances that may require risk management. Give at least 15 Potential Hazard or Threats. 15 pts.

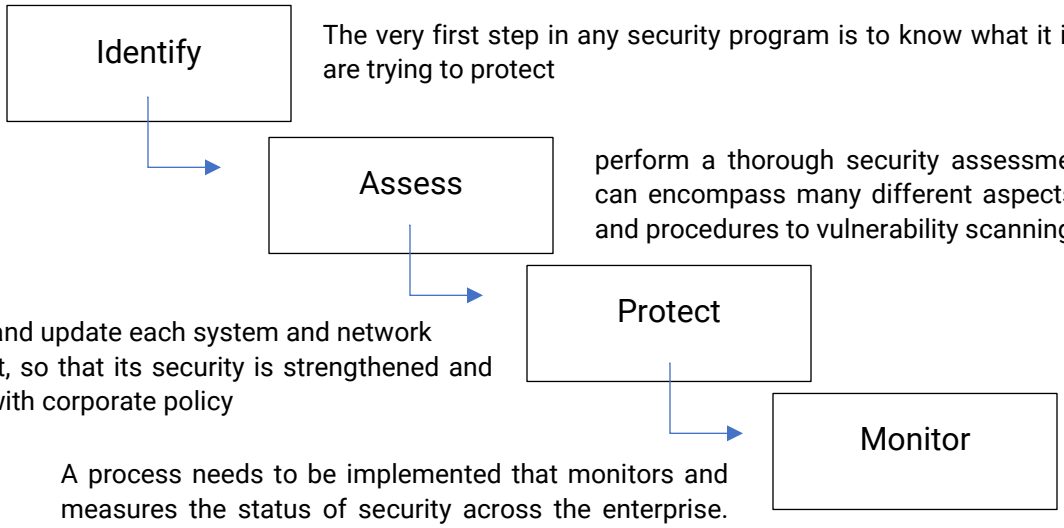
Potential hazard or risk	Persons who may be harmed	Property that may be damaged	Risk Control/ Mitigation Plan	Risk Rating	Further Action Needed
Theft	Me	TV, Computers, Cabinets, Tables, Doors	Surveillance System, Locks, Spotlights, Gated House, Guard Dogs	3/10	Keep valuables in a hidden place
Fire	Me	Entire House	Fire extinguisher, make sure stove is turned off, unplug devices when not used	2/10	Install fire detection system / water sprinklers
Food poisoning	Me	None	Throw away expired food	3/10	Prepare medication to combat food poisoning
Allergies	Me	None	Don’t eat monggos	1/10	Prepare medication
Cuts	Me	None	Store Knives safely, Learn cutting etiquette	4/10	First aid Kit
Fall	Me	Silverware	Don’t be clumsy	5/10	Use plastic utensils and plates
Gas	Me	Entire House	Turn off gas stove, make sure the attachment is properly in place	3/10	None
Murder	Me	None	Surveillance System, Locks, Spotlights, Gated House, Guard Dogs	1/10	None

Identity Theft	Me	Computer	Safeguard personal information, make sure personal information is private especially on social media	4/10	None
Device Hijacking	Me	Computer	Always use Private Networks, Change Default Settings	4/10	VPN
Covid – 19	Me	None	Social Distancing, Face Mask, Vaccine	2/10	Booster Shots
Electricity Overload	Me	Devices that require Electricity	Circuit breaker, 3 Prong outlet	3/10	Uninterruptable Power Supply
Dengue	Me	None	Mesh Screen on Windows, Anti-Mosquito spray, clean environment	4/10	Mosquito repellant, Anti-mosquito plants (Basil, Marigold)
Pests	Me	Furniture, Food	Make sure that there is no passageway in the house for pests	2/10	Exterminate pests
Electrocution	Me	Electrical Devices	Avoid coming into contact with appliances when your hands are not dry	3/10	Keep hands dry, keep your kitchen and kitchen sink separate from appliances.

9. There is generally more money in a bank than in a convenience store; but which is more likely to be robbed? Why? Of which risk management technique(s) is this an instance. 5 pts.

The convenience store is more likely to be robbed compared to the bank despite the money disparity. This is due to the fact that there would be a lot less security in convenience stores than there is in a bank. Risk mitigation is being used as a technique for risk management as if ever the robbers will be caught, then they will have to face less security personnel in convenience stores than in the bank.

10 . Develop a waterfall model for the security systems lifecycle management. Explain each of the stages. 10 pts.



The very first step in any security program is to know what it is that you are trying to protect

perform a thorough security assessment. The assessment phase can encompass many different aspects from reviewing processes and procedures to vulnerability scanning.

configure and update each system and network component, so that its security is strengthened and complies with corporate policy

A process needs to be implemented that monitors and measures the status of security across the enterprise. Monitor the security that you have established.