Pearson Institute of Higher Education

Social Practices and Security

ITSC311 – Take Home Test

Nompumelelo Mtshatsheni, Student Number: BXMDLL7W9
5-12-2020

Section A
Question 1 - Scenario

1.1

Information Asset A	Info Asset B
-Has the value of 50 and #1 vulnerability -The assumptions and data are 90% accurate	-#2 vulnerability - the likelihood of 0.5 and 50% of current address at risk #3 vulnerability -the probability of 0.1 and has no current controls -the expectations of 80% information correct
Formula Loss frequency = likelihood * attack success probability -in the scenario likelihood = 1.0 and since there are no current control mechanism, the attack success probability = 100% Loss frequency = 1.0*100%	→ Loss magnitude = asset value * probable loss Still from the scenario, the asset value = 50 and since there are no current control, the probable loss = 100% Uncertainly = 100% - certainly Hence, the uncertainly is = 100% - 90% = 10%
Resulting ranked	Resulting ranked
A: vulnerability #1 rated as 55 = (50 *1.0) - 0% +10% = 55	B: vulnerability #2 rated as 35 = (100 * 0.5) – 50% +20% = 35 B: vulnerability #3 rated as 12 = (100 * 0.1) – 0% +20 =12

The info assets for any risk management, the vulnerability is always assessed

- Switch L4 7, it attaches a network to the internet, has a failure of 0.2 likelihood and overflow of 0.1
- Server websrv6, performs all the e-commerce transaction. The assumptions for the assets will have to between 75% and 80%
- Operators, this tends to use the MGMT45 control. It examines the entire operations inside the server, the likelihood valuation of 0.1 with zero controls, the 90% of convinced expectations of information

1.2

- Looking at the above table, the information asset that should be evaluated first is Asset B, it seems to be more important this will be due to the fact is linked with e-commerce transactions
- A possible explanation will have to look at the servers getting condemned, this creates a serious problem and a huge likelihood of stealing delicate data
- The outbreaks will hack even the credit card info of the clients, which leads to a loss in money and having to steal organization data
- Whereas the asset A should be evaluated next because there's no possibility of an outbreak that will occur within the organization

1.3

- Defense control strategy occurs when the procedure of avoiding an outbreak prior into reality, this approach is temporary as a favored method to control the risk, it can be accomplished by disregarding vulnerabilities from resources, and by adding defending the security as well as rebutting intimidations
- Transfer control strategy, it is the procedure of transporting the risks to extra resources, other procedures even inside an association, these controls can be completed by employing an original service agreement, applying new benefactors, constructing the newer distribution mockups, procuring assurance, assembly a glace to the packages being presented
- Mitigation control strategy, the procedure of dropping the effect formed by an outbreak relatively than dropping the accomplishment of the outbreak itself, this approach initiates with early recognition of the outbreak which is in development and the ability of an association to reply faster and efficiently

Question 2 - Scenario

2.1

- Identification occurs when an admission switch device that involves the authentication and confirmation of an unauthenticated entity's supposed character
- Authentication, it is the admission controller device that will require proof and verification of an unauthenticated user's uniqueness
- Authorization, this characterizes all the corresponding of an authenticated handler to an incline of data resources and as well as the consistent entree flat
- Accountability, it is mostly skillful by resources of system journals and file periodicals and reviewing all the chronicles. Hence, the admission control device that guarantees all arrangements of the system moreover authorized or unauthorized can be credited to an audibility individual

2.2

- It does not watch alongside the liabilities and intimidations that appear from the deprived proposal of the system, measures, as well as the protocols, will want to be secure over appropriate design and situation up a defensive set-up
- It comes at a price; this means that cryptography practices in data handling lead to suspension. The usage of the public key will want a building up and preserving of PKI demanding a heavy financial budget

2.3

- Kerberos offers a protected third-party verification
- It ensures the users' passwords are certainly not shown across the network
- Although, the client and server systems commonly confirmed at the individual phase of the procedure, together with the user as well as the server system could remain convinced and cooperating with its reliable colleagues
- A validation model contains a timestamp and generation of data
- Authentications are recyclable and tough. A handler will need only to confirm to the Kerberos system on one occasion
- Although using Kerberos for Ayanda will not be justified, this is because Kerberos existed because of its intended for a use of a particular user system, the business will end-up decrease its target for all variation of receipt-stealing as well as replaying the outbreaks
- The business security will end-up be having a limit factor of data protection for Ayanda business
- The secure time services, regulates when the host of the business will keep on misleading the clientele about the accurate time for a stale authenticator will be replayed with lots of complications, time-based protocols will only ensure that the appropriate services of resources are being used appropriately

2.4

PLAINTEXT	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
CIPHERTEXT	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J

The Caesar cipher is shifted by 10

The encrypted message that will be sent to Michael is ->

COMEBSDI SC DRO UOI DY K CKPO CICDOW

Section B
Question 3 – ARO & ALE

3.1 The formula for ARO; is equal to one year/frequency of occurrence

Whereas the annualized loss expectancy is ALE = SLE * ARO

Category	Calculations of ARO	Calculations for ALE
Programmer mistakes	One year to 365, frequency occurrence will be the number of weeks =365/7 = 52 → roughly	The SLE value is 5000 Therefore: ALE = 5000 * 52 = 260000
Loss of intellectual property	It occurs once a year =365/365 =1 → roughly	The SLE value is 75000 Therefore: ALE = 75000 * 1 = 75000
Theft of information hacker	The frequency will be per quarter (1/4) =365/91.25 =4	The SLE value is 2500 Therefore: ALE = 2500 * 4 = 10000
Theft of information employee	The frequency will be one per six months =365/182.5 =2	The SLE value is 5000 Therefore: ALE = 5000 * 2 = 10000
Web defacement	Occurs every month =365/30.417 =12	The SLE value is 500 Therefore: ALE = 500 * 12 = 6000
Theft of equipment	It occurs once a year =365/365 =1 → roughly	The SLE value is 5000 Therefore: ALE = 5000 * 1 = 5000
Earthquake	The occurrence of an earthquake will take place once in twenty years =365/7300 =0.05 → roughly	The SLE value is 250000 Therefore: ALE = 250000 * 0.05 = 12500

Fire	The occurrence of fire will take place every ten years =365/3600 =0.1	The SLE value is 500000 Therefore: ALE = 500000 * 0.1 = 50000
Loss of intellectual property	The occurrence of fire will take place every 2 years =365/365*2 =0.5	The SLE value is 75000 =75000 * 0.5 =37500
Flood	The occurrence of fire will take place every four years =365/1460 =0.25	The SLE value is 250000 =250000 * 0.25 = 62500

3.2

- The cost of expansion
- The preparation fees for employees
- The cost of employment, which incorporates the charges for installing the software as well the hardware, organize and facilities
- The service industries charge will contain retailer charges for upkeep and improvements
- The cost for preservation which happens to contain all the labor expenditures to authenticate and frequently examine all the newer renews

Question 4 - Firewalls

4.1

- A firewall runs on a unique service user authentication instead of a root
- The filter packets function in-order to ensure that the accurate source as well as the target addresses, tend to keep nasty/malicious data traffic from entering and leaving the network, this prevents DoS attack

- Having to keep your firewall configuration as unpretentious as likely and remove unnecessary rules to guarantee that the firewall will be configured to support the intended needs of your network
- The firewall will remain consistent for the organizations for the information security procedure
- Limit the number of applications that run on the firewall to maximum pcs and network throughout, allowing the firewall to do its job protecting the network.
- The blocking of traffic by default this ensures that only specific traffic services will be approved, and it provides quality control over the entire network having to limit an opportunity of a hole
- The audit logs will be used for reporting and merged within a firewall along with a specific amount of data traffic. It helps look for any positive variations and small modification on the settings of a firewall

4.2

- IPsec is usually cast-off to produce a virtual private network for an end-to-end internet protocol network
- It is used for secure remote access for the entire network
- Tunnel mode, it happens works to encrypt a whole departing packet, covering the old packet in a new, protected one with a new packet header and ESP trailer, it also validates the getting of using sites for a verification header in the packet. It is naturally executed on a protected gateway, namely on a firewall, which will behave as a proxy for the dual cooperating places
- Although, the transport mode further encrypts the IP payload and ESP only. Frequently intended for the usage inside the end-to-end communication between places, it does not modify the IP title of the departing packet
- Hence, with the tunnel mode, the IPsec can only be detailed for subnets of the local area network after a router. IPsec procedure can also be stated for a specific IP address, that has hosted, within those subnets

4.3

- Packet filtering firewall is the data inside the packet that originate into a network. The packet filtering firewall is mounted inside a TCP/IP founded network for the functions of the internet protocol level and determine the dropping or forwarding it for a network connection, firewall packets monitor all the incoming packets shot and canister selectively riddle the packet created inside the data
- Application gateways, it does not contain critical data. All the additional filtering routers can be executed after the proxy server, as well as for defending the inside systems. Hence, the proxy server is always positioned in an unsecured area of the network DMZ, will be visible for higher levels of danger from a smaller amount of reliable network. It is regularly mounted on a keen pc commonly known as a proxy server

- Circuit gateways, it runs at the transport layer, just like a sifting firewall do not frequently appearance within the information, the traffic flowing amongst several networks but avoid connections amongst the different networks. Skilled by generating tunnels connecting specific procedures on individually side of a firewall and permitting individual approved traffic through tunnels
- Stateful inspection firewall It is more aware of devices on the other side, do not entirely monitor each packet as well as keep all the track of packets being established on the TCP, it offers more security rather than the packet filtering or circuit observing and tends to obtains a bigger toll of the network performance
- Hybrids (Next-generation firewall), is the combination of all packet review with a stateful examination and the network security systems including IDPS and antivirus. A next-generation firewall merchant to offer a progressive feature for recognizing the applications manufacturing all the traffic transitory through and participating with different major network mechanisms

Section C
Question 5 - secSDLC

5.1

Phases	Explanation
Investigation	This involves a process that will be started by directors and CEO working at the top level of the management team within Liberty Holdings. All the objectives as well as the goals for the intended system to be priorly executed.
Analysis	The second phase is basically about documenting all about the first phase and whether everything is done correctly. All the current applications and security procedures at Liberty Holding will be analyzed and double-checked for errors and vulnerabilities, hence with a new change of the forthcoming risks will be analyzed
Logical design	The third phase deals with the progress of tools that will be used to create a blueprint for the data security regulations. Liberty Holding would need to store its current procedures avoiding upcoming failures. This phase will the organization in decision planning for subcontracting the company, allows all the subtask of the project to finalize
Physical design	Liberty Holding will require different explanations were investigated, ensuring that unanticipated problems will be confronted in the impending future
Implementation	Within this phase the issued that was raised in the first has been fully developed, this phase along with the integration procedure of security implementation for Liberty Holding, it also includes a numerous amount of testing the system within the company

Maintenance	Once the implementation for the new security program for Liberty Holding has been installed. The program will require to be kept updated

5.2

An information security is used to process all the confidential information within the Liberty Holding, preventing unauthorized manipulators

- ❖ Top-down approach
  - The separation system into subsystems which will be done to increase the data
  - Each level has more specialists than its next level
- ❖ Bottom-up approach
  - It is the concentration of sub-system for a solitary structure to endure in order having to sustain the information potently
  - All the of the bottom and top-level sub-system will remain connected indirectly through the middle-level subsystem

Question 6 - Network IDPS Sensor Locations

6.1

Location 1

- Behind each external firewall in the network
  - ❖ Advantages
    - The intrusion detection and prevention system can see attacks that initiate from the outside that may infiltrate the networks boundary security
    - Can spot complications with the network firewall procedure or routine
    - It sees the outbreak that might aim for the web server of the file transfer protocol, both of which frequently exist in the DMZ
    - When the inbound outbreak is not noticed the IDPS will sometime identify trendy the outbound transportation outlines that advise that the server is already conceded

Location 2

- An outside an external firewall
  - ❖ Advantages
    - A sensor can monitor all the network traffic unfiltered

- It forms the number of outbreaks initiating within the network that aims for the network
- It forms all the categories of different attacks initiating inside the internet that will end-up pointing to the network
- Has higher dispensation weight than any sensor located anywhere in the above diagram as well as inside a network

Location 3

- On major network backbones
  - ❖ Advantage
    - It can monitor for both internal and external attacks
    - It displays a huge quantity of network traffic, hence growing the opportunity of recognizing outbreaks
    - It distinguishes among unlicensed activity by authorized users within the organization security perimeter

Location 4

- On critical subnets
  - ❖ Advantages
    - It supports the local area network user workstations and servers in every organization
    - It notices outbreaks directing for the serious systems and resources
    - It happens to permit concentrating of incomplete assets to the network resources reflecting on the utmost value

6.2

STRENGTHS	LIMITATIONS
Providing a default data security guideline	Unbale to explore the attacks without human involvement
Having to manage the operating system audit and as well as the logging device of information being created	Reimbursing for a weak and missing security machines in defense of the new structure
The ability to allow non-security specialists to accomplish significant security observing functions	Unable to detect newer attacks surfacing the system
Observing and having to analysis the behavior of user during the events of the system	To deal with effectively exchanged networks
Distinguishing the movement pattern that may vary from the regular movement	