Task- 1

1. Answer

* Human Resources Data

It is also the most important thing to keep secure because as we know human resources watch out for the employees of the company and if human resources data if attacked then the attacker can change the personal information or can loot the personal information’s including bank of the employee.

* Customer Data

Customer data is most important thing to keep secure because it will contain their credit card information, phone number etc. So, after the business is over with a particular client we should keep their data is a secure drives and delete it from the servers.

* Financial Data

Financial data should be kept secret to make sure that all the data’s of the guest (clients) should be confidential. Because if the data is lost then at the time of audit or tax payment it will cause a problem in the company. And also financial data includes salary statements, tax statements of the employee’s too.

* Cloud

Cloud also known as server is the most important thing to be secured because all the personals data’s, financial data, employee’s personal information, company’s confidential data’s are stored in the cloud. So, if hacker’s attacks cloud it will be very difficult for the company to overcome the loss.

* Marketing

Marketing is one of the most important thing for ever business because it is the gate for your success. While marketing are usually done through websites, social media pages but if these thing are hijacked then the company will be slightly go back in the line of success. It is usually attack by DDOS attack, phishing.

b, c, d) Answer

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Asset | Threats | CIA? | Likelihood | Impact | Risk |
| Customer data | Insider theft | C | Medium | High | High |
|  | Data leakage | C | Low | High | Medium |
|  | Server failure | A | Medium | High | High |
| Financial Data | Eavesdropping | C | Medium | Medium | Medium |
|  | Phishing | I | High | Low | Medium |
|  | Malware | A | Medium | Medium | Medium |
|  | Smishing | A | Low | Low | Very low |
| Cloud | DDOS attack | A | High | High | Very high |
|  | Malicious content | I | Medium | Medium | Medium |
|  | Server failure | A | Medium | High | High |
| Human Resource Data | Data modification | C | Low | Medium | Low |
|  | Identity theft | C | Low | High | Medium |
|  | Biometrics theft | C | Low | High | Medium |
| Marketing | DDOS attack | A | High | High | Very high |
|  | Phishing | I | High | Low | Medium |
|  | Email spoofing | A | Medium | Medium | Medium |
|  | Weak access control | C | Medium | High | High |

Task- 2

1. Answer

* Insider theft
* It is a process of stealing or misusing the data of the company without an employer’s permission. The security measures for this kind of theft are,
* Use Biometrics or encryption for important data.
* Backup every files in secure hard disks.
* Data Leakage
* Data leakage is an unauthorized transfer of the data from one organization to receiver. The security measures are,
* Monitor the company activities.
* Data encryption.
* Server failure
* It is a process of shut down of the server. The security measures are,
* Try not to store the malware files.
* Try not to make large number of traffic.
* Phishing
* Phishing is the process of getting the data of victim through the means of email, text etc. below down are some security measures,
* Don’t accept the emails from unusual sender.
* Watch out for the email signature and the email address.
* Malware
* It is a software program which is made to damage your computer system. The security measures are,
* Don’t download free software’s from any sites.
* Use Anti malware antiviruses.
* DDOS attack
* It is Distributed denial of service is a process of generating tremendous amount of traffic and send it to the victims website from the internet. The security measures are,
* Secure your network infrastructure.
* Watch out for the warnings.
* Use intrusion prevention systems.
* Malicious content
* It refers to the malicious code injected inside the scripting language. The security measures are,
* Use a trustable programmer.
* Once the program is finished hire system tester to test it.
* Data modification
* Data modification is the process of modifying the data without the authority. The security measures are,
* Use encryption in files.
* Don’t give access to all the files to interns in the office or the locum workers.
* Identity theft
* It is the process of using someone’s identity like ATM without their permission for any purchase. The security measures are,
* Don’t save the card information in your browser history.
* Check the ATM machine before inserting your card.
* Biometrics theft
* It is the process of stealing the figure print and retina information of the victim, It is usually use while making passports. The security measures are,
* Don’t send your figure print after any purchases in online.
* Check before signing any documents.
* Email Spoofing
* It is a process of sending spam emails full of malware from which a victim chicks it and the malware automatically installs and works as a key logger. The security measures are,
* Don’t click the link in the spam mails.
* Always verify the email address.
* Weak Access control
* Access control is a technique of selecting the user of the resources of the company. And weak access control is the failure of selection of the user.
* Use multi factor authentication
* Strong password policy.
* Eavesdropping
* It is an act of interception between two communications. The security measures are,
* Continuous supervision to all the maintenance personals.
* Alert your employees.

B,c) Answer

* Encryption is the process of converting normal text to cipher text. It is the most useful way of protecting the data. To open an encrypted file we need a passkey to decrypt it and should change the file to readable format.

I have used the encryption for all the data’s like Drives, folders and email. I have used AES (Advanced encryption standard) protocol for the encryption process because it is trusted by US government to protect their classified information. It is efficient in 128 bit form it also uses 192 and 256 bits too do the heavy encryption process. Also would be recommending AES encryption.

Likewise, I have chosen to encrypt Drivers, folders and email because everything we work in the computer we save the data’s in these thing and also while sending the email if we use the encrypted file it will help the file to be protected and hackers can’t open it without the decryption key. And, while using computer nowadays we have been hearing many thefts of confidential files and folders so if we encrypt our drives and the folders then we would be safe from those kinds of activities. Hence, this was the reason I choose those files to be encrypted and also recommended the best protocol trusted by US government which is AES (Advanced encryption standard).