**Question a)-** **Analyze the scenario and identify what you consider to be the FIVE (5) most important electronically held information assets in the company. Justify your decision. You will need to make some reasonable assumptions here, since the scenario is brief.**

**Answer-** Below show the five (5) most important electronically held information assets in the company-

1. Customer Personal Data.
2. Marketing Information.
3. Payment Details.
4. Financial Details.
5. Company Personal Data.
6. Production Data.

**Justification for the five point-** For the Security purpose reduced the risk assessment, I listed down this, five information assets which is valuable and prioritized for this company. Which can help to protect from the hacker, for example- a hacker can entered your network and copied your entire customer data and damaged your database information.

So that kind of information is critical for this “Perfects Pets” Company. This information assets confidentiality, integrity and availability is of utmost importance.

**Reasonable Assumptions-** This Information asset has risks associated with “Perfects Pets” Company, which is the risk of losses the assets, information will fall into the wrong hands, getting corrupted or any number of other issues. By considering these risks, we will able mitigate against risk measures and plans.

**b)** **Answer-**

**c)** **Answer-**

**d)** **Answer-**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Assets(a)** | **Threat(b)** | **CIA(b)** | **Likelihood(c)** | **Impact(c)** | **Risk (d)** |
| Customer Personal Data | Server Failure | A | Low | Medium | Low |
| Information leakage | C | Low | High | Medium |
| Phishing Data | C | High | High | Medium |
| Viruses | A | Low | Medium | Low |
| Fire | I | Low | High | Very High |
| Software Errors | C | Medium | Low | Very Low |
| Marketing Information. | Server Failure | A | Low | Medium | Medium Low |
| Loss of Support Services | C | Low | Low | Medium Low |
| Information Leakage | C | Medium | High | High |
| Ransom Ware Attack | A | Low | High | High |
| Payment Details | SQL Injection | I | Medium | High | Very High |
| Phishing | C | High | High | High |
| Software Errors | A | Medium | Low | Medium |
| Financial Details | Spyware | A | Low | Medium | High |
| SQL Injection | I | Medium | High | Very High |
| Software Errors | A | Low | Low | Medium |
| Ransom Ware Attack | A | Low | High | High Medium |
| Malware | A | Low | Low | Medium |
| Information Leakage | C | High | High | Very High |
| Company Personal Data | Server Failure | A | Low | low | very low |
| Information leakage | C | Medium | high | Very High |
| Viruses | A | Low | Medium | High |
| Fire | I | Low | High | Very High |
| Software Errors | A | Low | low | low |
| Unauthorized use of software | C | Medium | high | High |
| Production Data | Software Errors | A | Low | low | low |
| Unauthorized use of software | C | Medium | high | High |
| Fire | I | Low | high | Very High |
| Information leakage | C | Low | high | Very High |