**Group 3 batch B Cybersecurity**

Analysis of some Cybersecurity risk

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| s/n | Asset | Threat | Likelihood | Impact | Risk | Justification |
| 1 | System | Disruption of operation | 4 | 4 | 16 | The likelihood and impact of malware and Ransomware attack is high due to the profit motive and privacy issues.  The impact is high because many systems and data will be corrupted and possibilities of company incurring many expenses |
| 2 | Customer’s information | Data breach | 4 | 4 | 16 | The likelihood of this threat is high because of poor access control of the system. The impact is very high because it could lead to loss of customer's trust and damage of company’s reputation |
| 3 | Intellectual Property | Unauthorized Access and Theft | 3 | 5 | 15 | The likelihood of this threat is moderate, especially if there are inadequate access controls and monitoring. The impact is very high because the theft of proprietary information can lead to loss of competitive advantage, financial losses, and legal repercussions. The high value of intellectual property to the business makes this a significant risk. |
| 4 | Network Infrastructure | Distributed Denial of Service (DDoS) Attack | 4 | 3 | 12 | The likelihood of the attack is high due to the increasing frequency of such attacks across industries. The impact is moderate because, while it can disrupt services temporarily, proper mitigation strategies (such as using a Content Delivery Network (CDN) or DDoS protection services) can minimize the damage. However, a prolonged attack could lead to downtime, loss of revenue, and customer dissatisfaction, making it a moderate risk that needs attention. |