|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Allegro - Worksheet 10** | | | **Information Asset Risk Worksheet** | | | | | |
| **Information Asset Risk** | **Threat** | Information Asset | Payment Gateway System | | | | | |
| Area of Concern | Doing network failure in the system by an internal attacker | | | | | |
| (1) Actor  *Who would exploit the area of concern or threat?* | | Network service provider | | | | |
| (2) Means  *How would the actor do it? What would they do?* | | An authorized user with malicious intent or negligence can exploit their access rights to compromise network security. They might manipulate system settings, install malicious software, or neglect necessary security measures, leading to vulnerabilities and potential data breaches. | | | | |
| (3) Motive  *What is the actor’s reason for doing it?* | | Deliberate or Accidental | | | | |
| (4) Outcome  *What would be the resulting effect on the information asset?* | | * **Disclosure** * **Modification** | | * **Destruction** * **Interruption** | | |
| (5) Security Requirements  *How would the information asset’s security requirements be breached?* | | If an authorized user needs to access the system but encounters a network failure, it can violate Availability. To prevent this, implement strong access controls ensuring users have the least privilege, use multi-factor authentication to secure access, and continuously monitor network activity to quickly detect and respond to issues. This ensures that authorized users can always access the system reliably | | | | |
| (6) Probability  *What is the likelihood that this threat scenario could occur?* | | * **High**   **75%** | * **Medium**   **50%** | | * **Low**   **25%** | |
| (7) Consequences  *What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?* | | | | (8) Severity  *How severe are these consequences to the organization or asset owner by impact area?* | | | |
| **Impact Area** | | **Value** | **Score** |
| A network failure caused by an insider can moderately impact the organization’s reputation and customer confidence, as it prevents transaction processing and a loss of trust. Financially, the company may face potential losses from missed transactions. | | | | Reputation & Customer  Confidence | | 8 | 4 |
| Financial | | 8 | 4 |
| Customers dissatisfied with network failures may switch to competitors, causing a loss of income and market share. Additionally, significant time and effort will be required to diagnose and resolve the network issue, impacting productivity. The organization might incur additional costs for security safeguards and incident response tools. | | | | Productivity | | 9 | 4.50 |
| Safety & Health | | 7 | 3.50 |
| Network failures may lead to fines and legal penalties if customers seek compensation for losses or if regulatory compliance is breached. | | | | Fines & Legal Penalties | | 7 | 3.50 |
| User Defined Impact Area | | 0 | 0 |
| **Relative Risk Score** | | | | | | | | **19.50** |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **(9) Risk Mitigation**  *Based on the total score for this risk, what action will you take?* | | | | |
| * **Accept** | | * **Defer** | * **Mitigate** | * **Transfer** |
| **For the risks that you decide to mitigate, perform the following:** | | | | |
| *On what container would you apply controls?* | *What administrative, technical, and physical controls would you apply on this container? What residual risk would still be accepted by the organization?* | | | |
| Administrative Controls | * Implement strict access control policies and procedures to limit who can access critical network systems. Ensure only authorized personnel have access. * Provide ongoing security training to employees about the importance of network security and the potential risks of insider threats. * Conduct regular audits of access logs and network activity | | | |
| Technical Controls | * Ensure that all network devices and systems are up-to date with the latest security patches. * Use network segmentation to isolate critical systems and limit the potential impact of a network failure. * Require Multi-Factor Authentication (MFA) for accessing sensitive systems to ensure only authorized users can log in. | | | |
| Physical Risk | * Restrict physical access to data centers and server rooms to authorized personnel only. | | | |

**Justification of probability and Severity values**

|  |  |  |
| --- | --- | --- |
| Attribute | Value | justification |
| Probability | 50% | The probability is considered medium (50%) because while internal network threats from authorized users are a recognized risk, security measures and controls can reduce the likelihood of exploitation. |
| Reputation & Customer Confidence | 8 | A network failure can harm the organization’s reputation and erode customer trust, especially since it disrupts payment transactions, which are vital for customer satisfaction. |
| Financial | 8 | |  | | --- | |  |  |  | | --- | | Financially, a network failure would result in revenue loss from disrupted transactions, potential compensation payouts, and additional costs for rectifying the issue and enhancing security. | |
| Productivity | 9 | A prolonged network failure would severely impact productivity due to diagnosing and resolving issues, leading to wasted time and reduced efficiency across the organization. |
| Safe and health | 7 | Although no direct physical harm is involved, the stress from addressing a critical network failure could impact employee well-being, resulting in heightened pressure and possible burnout. |
| Fines & Legal Penalties | 7 | Legal penalties may arise from contractual breaches, non-compliance with regulatory requirements, or customer compensation claims due to service failures. |
| User Define Impact Area | 0 | |  | | --- | |  |  |  | | --- | | No specific additional impact areas have been defined for this particular scenario, indicating that the primary focus remains on the identified standard risks | |