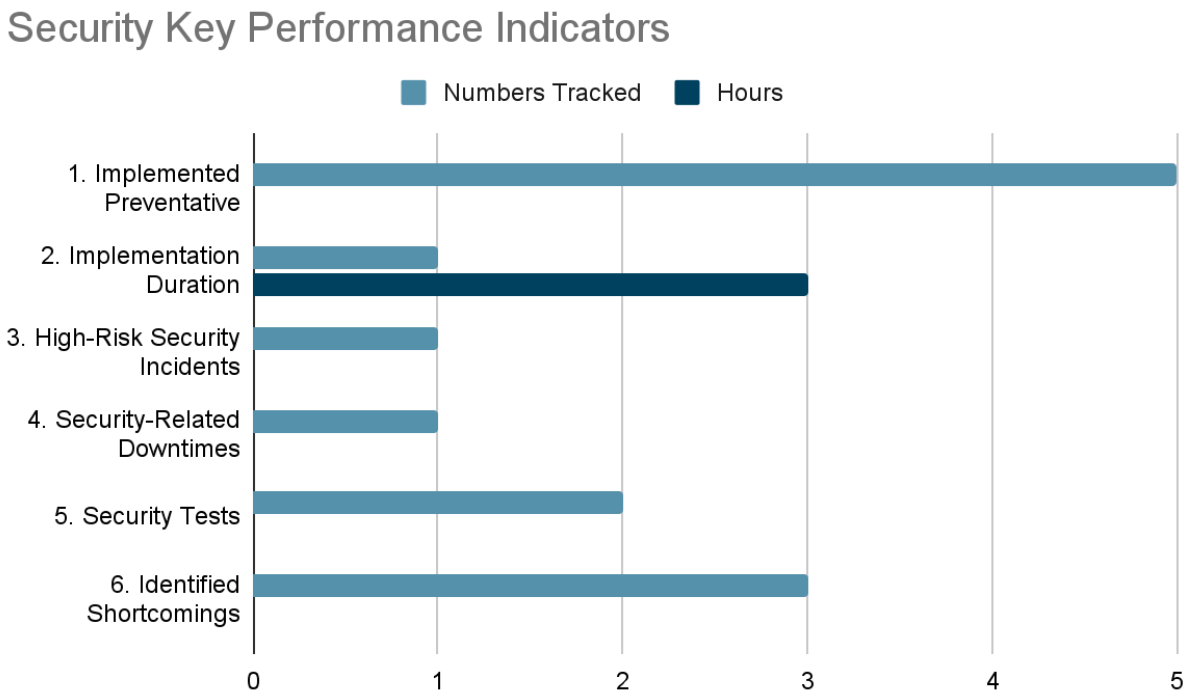
Name: Lasmarias, Lawrence R. Section: BSIT706
Date: 11 October 2024

Instructions: Identify the KPIs in the case study and create a simple chart that visualizes the number of information tracked for each KPI.



Explanation:

1. Number of Implemented Preventative Measures

   This tracks the number of security measures put in place to prevent future incidents. It's crucial for understanding how proactive the company is in strengthening its defenses. There are five (5) total preventive actions taken by TeleMarketeers to secure their systems. This includes forming specialized teams like the Network team, Firewall team, IT Desktop Support team, Blue Team, and the Fast Attack team. It also includes the acquisition of malware-specific devices and software. Each of these teams and measures plays a distinct role in fortifying the company's defenses against cyber threats.

2. Implementation Duration

   This measures the time taken to resolve a security issue from the moment it is identified. This helps in evaluating the efficiency of the

security team. The first and only issue tracked was a spyware attack that was identified at 1 PM and resolved by 4 PM, making the time taken to resolve the security issue 3 hours. This quick resolution time reflects the team's preparedness and effectiveness.

3. Number of High-Risk Security Incidents

   This counts the number of significant security incidents, categorized by their severity. It helps prioritize response efforts and allocate resources accordingly. The first and only incident tracked was one high-risk spyware attack that affected 20 agents, demonstrating a significant threat that required immediate and specialized attention.

4. Number of Security-Related Downtimes

   This tracks the number of downtimes that occur due to security issues. It's important for assessing the impact of security breaches on operational continuity. The first downtime that occurred due to a security issue is a spyware attack causing downtime for the 20 affected agents, impacting their ability to perform their duties until the issue was resolved.

5. Number of Security Tests

   This measures the proactive steps taken to test and evaluate the security posture of the organization. Regular testing helps identify vulnerabilities before they can be exploited. The first test taken was a security measure assessed on 5 computers. The second and last test taken was further assessments that were carried out on 20 computers, revealing additional challenges.

6. Number of Identified Shortcomings During Security Tests

   This identifies weaknesses found during security tests. Knowing these shortcomings helps prioritize areas that need improvement. The first identified weakness is a delay in effectiveness when the solution was scaled to 20 computers. The second weakness that was identified is the slower progress of the resolution process than expected. And the last and third weakness is the complete file corruption that was observed on some systems, highlighting a critical vulnerability.