2024

Analysis of Incident Report Handling Process

A Comprehensive Analysis and Improvement Proposal

PRAJIT GIRI

Contents

Analysis of Incident Report Handling Process

Part 1A: Process Analysis

1. Inputs

- Incident reports received via phone, email, or in-person.
- The incident management system used for logging and tracking incidents.
- Standard Operating Procedures (SOPs) that outline the process steps.
- Personnel involved in the process (dispatchers and security officers).

2. Outputs

- Documented incident reports that include all relevant details.
- Incident response summaries outlining actions taken.
- Lessons learned reports that highlight insights gained from each incident.
- Follow-up actions based on the outcomes of the incidents.

3. Flow Unit

- The flow unit is an **incident report**. Each report progresses through various stages until it is fully processed and closed.

4. Flow Rate

- **Flow Rate**:
    - The observed flow rate is the number of incidents processed per hour. During the observation, the SOC can handled **15 incidents in one hour**, resulting in a flow rate of **15 incidents/hour**.

5. Capacity

- **Capacity Calculation**:
    - Capacity can be estimated based on the flow rate and the operational hours available for processing. Given that the SOC operates for **8 hours per day**:
        - **Capacity** = Flow Rate x Operating Hours = 15 incidents/hour x 8 hours = **120 incidents/day**.

6. Utilization Rate

- **Utilization Rate Calculation**:
    - Utilization = (Flow Rate / Capacity) x 100%
    - Given that the observed flow rate is **15 incidents/hour** and the capacity is **20 incidents/hour**:
        - Utilization = (15 / 20) x 100% = **75%**.

7. Capacity Constrained or Demand Constrained

- **Analysis**:
  - If demand consistently exceeds capacity, the process is classified as **demand constrained**.
  - If there are periods where capacity is underutilized but demand remains stable, it is **capacity constrained**.
  - In this scenario, if the SOC frequently encounters more incidents than it can handle, it is **demand constrained**.

8. Bottlenecks

- **Identification of Bottlenecks**:
  - Common bottlenecks in the incident handling process may include:
    - Delays in receiving reports due to high email volume.
    - Slow response times from field personnel due to high workload.
    - Inefficiencies in documentation processes leading to longer processing times.

9. Process Diagram

- **Process Diagram**:
  - A flowchart should be created showing the following stages:
    - **Receiving Reports → Assessment → Documentation → Response Coordination → Follow-Up**.

10. Process Productivity

- **Productivity Calculation**:
  - Productivity can be calculated by dividing the total output by the total input:
  - **Productivity** = Output / Input = Total incidents processed / Total time taken.
  - In this case, if **15 incidents are processed in 1 hour**, then productivity is **15 incidents/hour**.

Part 1B: Process Improvement Proposal

Critique of the Process

- The incident report handling process can be slow due to reliance on manual entry and communication delays. This often results in high workloads during peak times and missed opportunities for timely responses.

Proposed Improvements

1. **Implement Automated Reporting System**:
    - **Rationale**: This would streamline report intake via online forms, significantly reducing the time spent on receiving and entering reports.
2. **Enhance Training for Dispatchers**:
    - **Rationale**: This ensures efficient prioritization and handling of incidents, ultimately reducing assessment time and improving response rates.
3. **Invest in Incident Management Software**:
    - **Rationale**: This would increase efficiency in documentation and follow-up processes, ensuring a consistent record of incidents and improving data accessibility.

Cost/Benefit Analysis

- **Costs**:
    - Automated Reporting System: **$5,000** (one-time setup).
    - Training: **$2,000 annually** (for staff training sessions).
    - Incident Management Software: **$10,000** (one-time purchase).
- **Benefits**:
    - **Improved Flow Rate**: Expected increase of **25%** (from 15 incidents/hour to 20 incidents/hour).
    - **Reduction in Incident Response Times**: Quicker processing times leading to improved safety outcomes and customer satisfaction.
    - Estimated annual savings of **$15,000** based on reduced overtime and improved resource allocation.

Summary of Data to Include in Excel	
Metrics	**Values**
Flow Rate (incidents/hour)	15
Capacity (incidents/day)	120
Utilization Rate (%)	75
Productivity (incidents/hour)	15
Total Costs ($)	17000
Estimated Savings ($)	15000

Table 1.1: Incident Report Process Analysis

This table summarizes key metrics associated with the incident report handling process in the Security Operations Center (SOC). The metrics provide insight into the flow rate, capacity, utilization, productivity, and financial implications of the process.

Key Metrics:

- **Flow Rate (incidents/hour)**: This metric indicates the number of incidents processed by the SOC within one hour. In this analysis, the flow rate is **15 incidents/hour**, reflecting the current operational efficiency.
- **Capacity (incidents/day)**: The maximum number of incidents that the SOC can handle in a typical 8-hour workday is **120 incidents/day**. This represents the upper limit of processing capability based on observed flow rates.
- **Utilization Rate (%)**: This percentage (75%) demonstrates how effectively the SOC is using its available capacity. A utilization rate of 75% suggests that there is still room for handling additional incidents without overwhelming the process.
- **Productivity (incidents/hour)**: The productivity metric, calculated at **15 incidents/hour**, shows the output of the SOC in terms of incident resolution efficiency.
- **Total Costs ($)**: This figure summarizes the total investment required for the automated reporting system, dispatcher training, and incident management software, amounting to **$17,000**.
- **Estimated Savings ($)**: Based on efficiency improvements, the SOC expects to save approximately **$15,000 annually** due to reduced overtime costs and better resource allocation.

Conclusion

The proposed changes are projected to enhance the overall efficiency and effectiveness of the incident report handling process in the SOC. Implementing these improvements aims to better manage incidents, reduce response times, and achieve better outcomes for both staff and incident resolution.