Factors Affecting Incident Management Lifecycle

Donna I. Baret

Abstract

In this paper we analyzed the data that came from an event log of an incident management process extracted from the audit system of the *ServiceNowTM* platform used by an IT Company. The data is composed of 141,712 transactions from February 2016 to February 2017 consisting of 24,918 incidents. The data set consists of 36 attributes. The aim of the study is to avoid outages and violation to the service level agreement (SLA) and to reduce operational cost by optimizing resources and by assessing the inflow of tickets to make sure they are properly tagged, and the employees are not being overworked. In this study we used Logistic Regression to determine the factors affecting service level agreement (SLA) violation. We found out that tickets are not equally distributed across groups and resources. This is apparent on the rate of SLA violations on the incidents per group and resource. Moreover, we have seen an influx of incidents logged between March 2016 to May 2016. It is therefore recommended to improve the incident management process by properly allocating incidents per assignment group and resolver.

I. Introduction

As globalization emerges, multinational companies tend to outsource technology-based jobs to developing countries which makes Business Process Outsourcing (BPO) an emerging industry. Technology-based BPOs are in demand because of their ability to support the complex processes with wide scopes while having the ability to assess performance, optimize the process, and reduce cost. As businesses process outsourcing firms provide higher value on added services, companies can focus on their products more rather than the intricacies of their technological infrastructure. Therefore, outsourcing can enhance productivity because of more specialized and standardized services (Panina Daria, 2005).

With this as (Balakrishnan Karthik, 2008) shows, companies are assured that the task is fulfilled within an objective amount of time with greater depth in understanding the issue

at hand and it is the BPO company's responsibility to fulfil that role and to keep the business going. This symbiotic relationship is what sustains the rapid growth of the area

In this paper we want to discover how to minimize outages by investigating if the incidents are routed to the correct SME at first try or routed more times and if our tickets closed within service level agreement (SLA). Moreover, we're going to investigate what kind of tickets are received and if it's low priority – consider the chance for automation. We're also going to look if our staff is overworked by looking into tickets received per person and if the ticket types received within groups are distributed from low priority to high priority – see if more people should work on high priority tickets. To add to that we're going to discover if there are days of week or months where there is an influx of incidents

This will help managers of the BPO companies to streamline processes for smoother incident management and in proper staffing to prevent violation of SLA. If the incidents are routed more than once, investigate their characteristics and suggest possible resolutions. Moreover, if the incidents are not closed within SLA, investigate causes – such as lack of knowledge document or if it's mis assigned ticket. Moreover, If the tickets received are Low Priority, Low Impact – Investigate for automation to increase staffing time. If a certain group receives more tickets than the rest of the group, investigate how many of them are working there and determine if there's an influx of incidents during DOW and Months and alarm the manager on personal leaves approval and day off planning. Moreover, the management may allow more time estimates for groups who receive high impact, and high priority tickets compared to low impact low priority because it will take more time to resolve them.

II. Review of Related Literature

Business process management is an operations management process in which people use various techniques for streamlined processes. One process is the use of digitized workflows for easier tracking of incidents and assignments to groups (Kissflow, 2018).

i. The main steps in incident management is usually:

1. Incident Identification – the location of where the incident came from is recorded and the incident is dcategorized

2. Incident Logging – user information, description and relevant details, incidents are prioritized and then categorized

3. Incident Prioritization -incidents are marked according to urgency and impact on the business. High priority for those that affect the production, and those that don't are given low priority

    a. High Medium Low

    b. Critical, High, Medium Low

4. Incident Response

    a. Initial Diagnosis – standard troubleshooting

    b. Incident escalation – assigned to technical groups

    c. Investigation and diagnosis

    d. Resolution and Recovery – confirms that the issue is resolved and documents the resolution

    e. Incident Closure – Incident is closed, post implementation plan is done and reviewed

5. Importance of Incident Management Planning

    a. Proper staffing

    b. Business continuity

    c. Service Level Agreements are not violated

    d. Prevent future recurrence

The lack of an IT Incident Management System will result to the inability to monitor timelines and to record the past incidentsA paper published by IBM indicated that operations analytics indicated their strategy to predict, search and optimize using unstructured data from ITSM systems which helped in avoiding outages and minimizing cost by properly assigning resources on incident, reducing the mean time to recover by analyzing metrics, logs, events and tickets and optimize resources through efficiency (Headlee, 2016).

III. Methodology

A. Data Understanding

a. Data Description

The data came from an event log of an incident management process extracted from the audit system of the ServiceNowTM platform used by an IT Company. Data is composed of 141,712 transactions from February 2016 to February 2017 consisting of 24,918 incidents. The data set consists of 36 attributes (1 case identifier, 1 state identifier, 32 descriptive attributes, 2 dependent variables)

b. Verify Data Quality

The Data that is not complete and below is the list of missing values. This is to determine if we should drop the variable for analysis or if deleting data would suffice.

Table 1. List of Variables with Missing Values

Category	Missing Values
Caused by	141689
Vendor	141468
CMDB_CI	141267
RFC	140721
Problem_ID	139417
Closed_at	85396
Sys_Created_By	53076
Sys_created at	53076
U_Symptom	32964
Assigned_To	27496
Assignment_group	14213
Opened by	4835
Resolved at	3141
Closed_Code	714
Resolved_by	226
Subcategory	111
Category	78
Caller_id	29
Incident_state	5

c. Data Preparation

i. Data Selection

We will drop the variables on Table 2 due to number of missing values.

Table 2. List of Variables that will be dropped

Category	Missing Values
Caused by	141689
Vendor	141468
CMDB_CI	141267
RFC	140721
Problem_ID	139417
Closed_at	85396
Sys_Created_By	53076
Sys_created at	53076
U_Symptom	32964

ii. Data Cleaning

1. We will remove NA Values

2. Extract latest update for incident: This is to avoid duplicates on our data analysis

d. Explore Data

We can see that the incident number is the unique identifier and we will assign counts per one-way, two-way, and three-way table

i. Univariate Analysis

Table 3. Incident Number, reassignment count, and reopen count

Summary Statistics

Number of Records	23,362
Reassignment Count	23,404
Reopen Count	330

We can see on Table 3 that there is a total of 23,362 incidents in which among has been reassigned 23,404 times and been reopened 330 times.

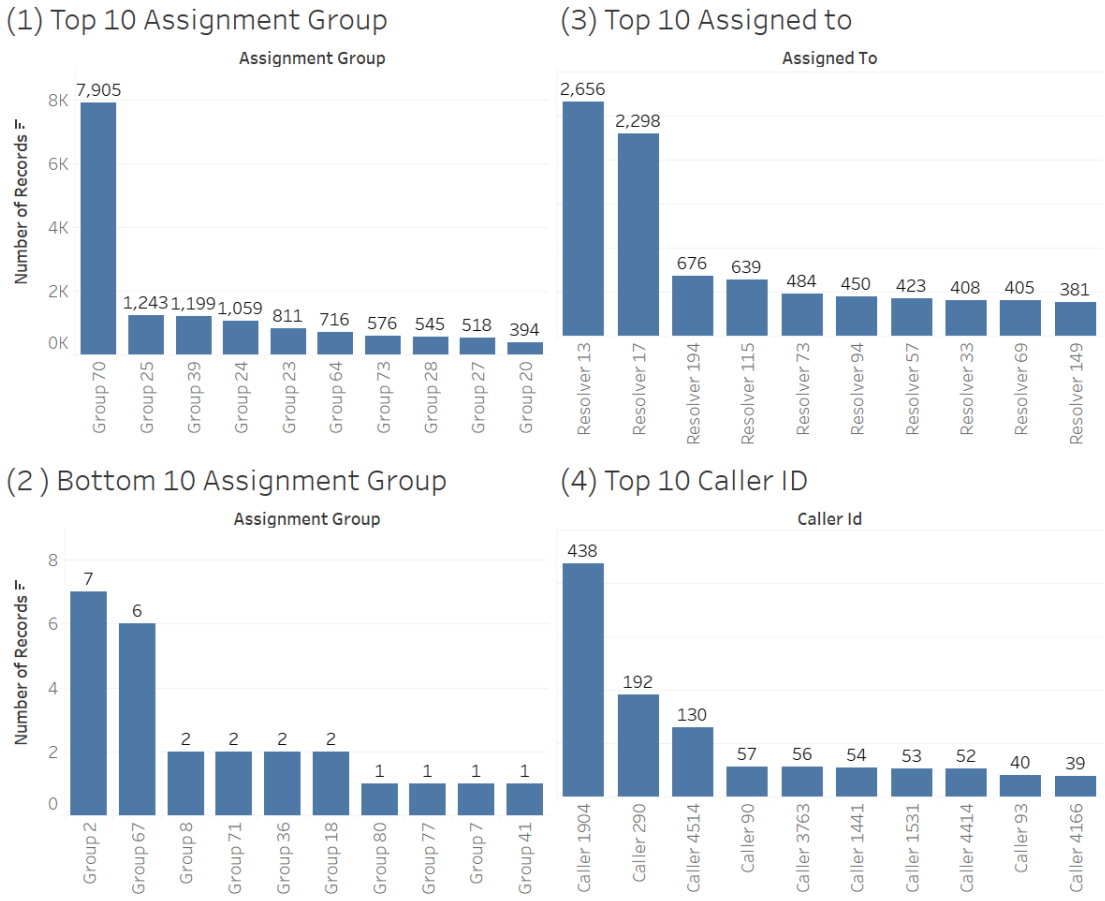

Figure 1. (1) Top 10 Assignement Group by assigned tickets (2) Bottom 10 Assignment Group by assigned tickets (3) Top 10 Resolver by assigned tickets (4) Top 10 Caller ID by Tickets Opened

As seen on Figure 1(1), Group 70 has the most assigned tickets with a total of 7905 incidents. Figure 1(2) on the other hand shows that there are groups that received as litle as one ticket throught the whole year.

Figure 1(3) shows on the other hand that resolver 13 and Resolver 17 had a strikingly more tickets assigned to compared to other resolvers. Moreover, Caller 1904 has the opened incidens on the ITSM with 438 imcidents.

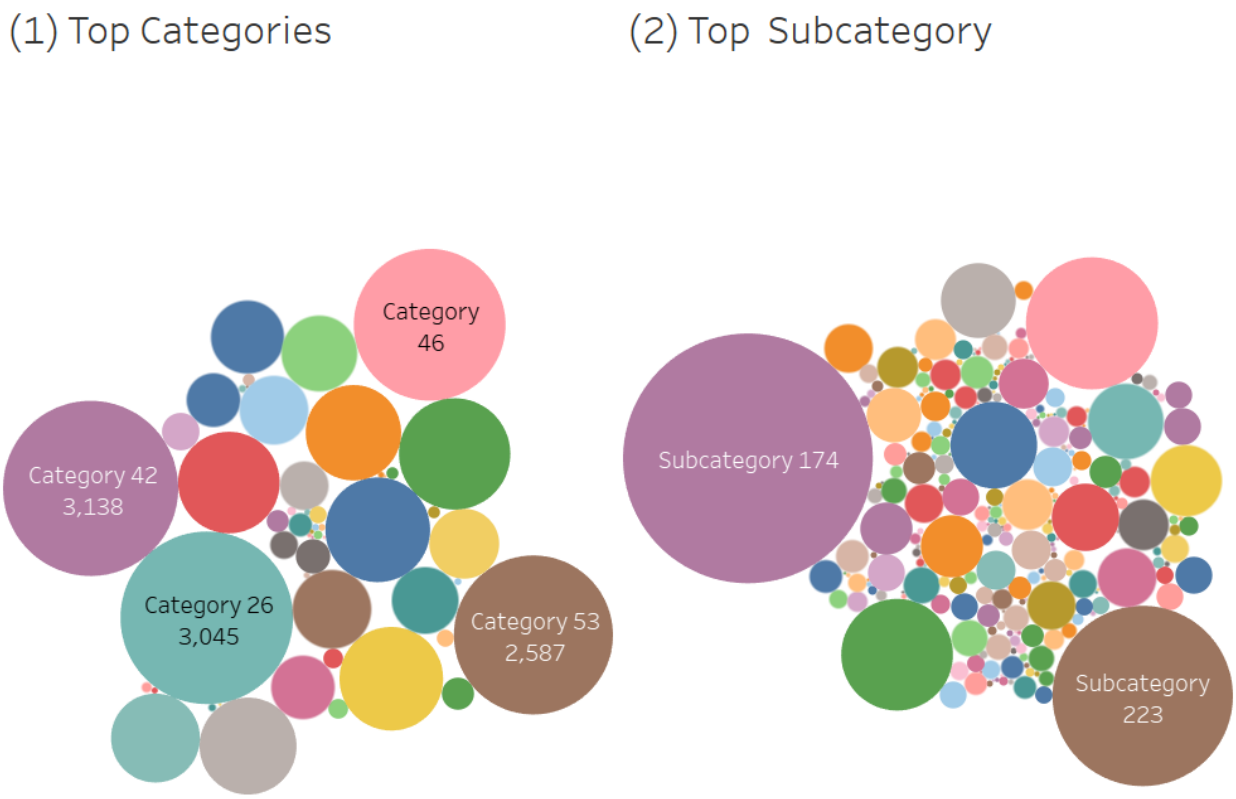

Figure 2.(1) Top Categories by number of incidents opened (2) Top Subcategories by incidents opened

As seen on Figure 2(1) categories 53,26,42,46 received the most incidents. Moreover, Figure 2(2) shows that most incidents belong to Subcategory 174 and Subcategory 223.

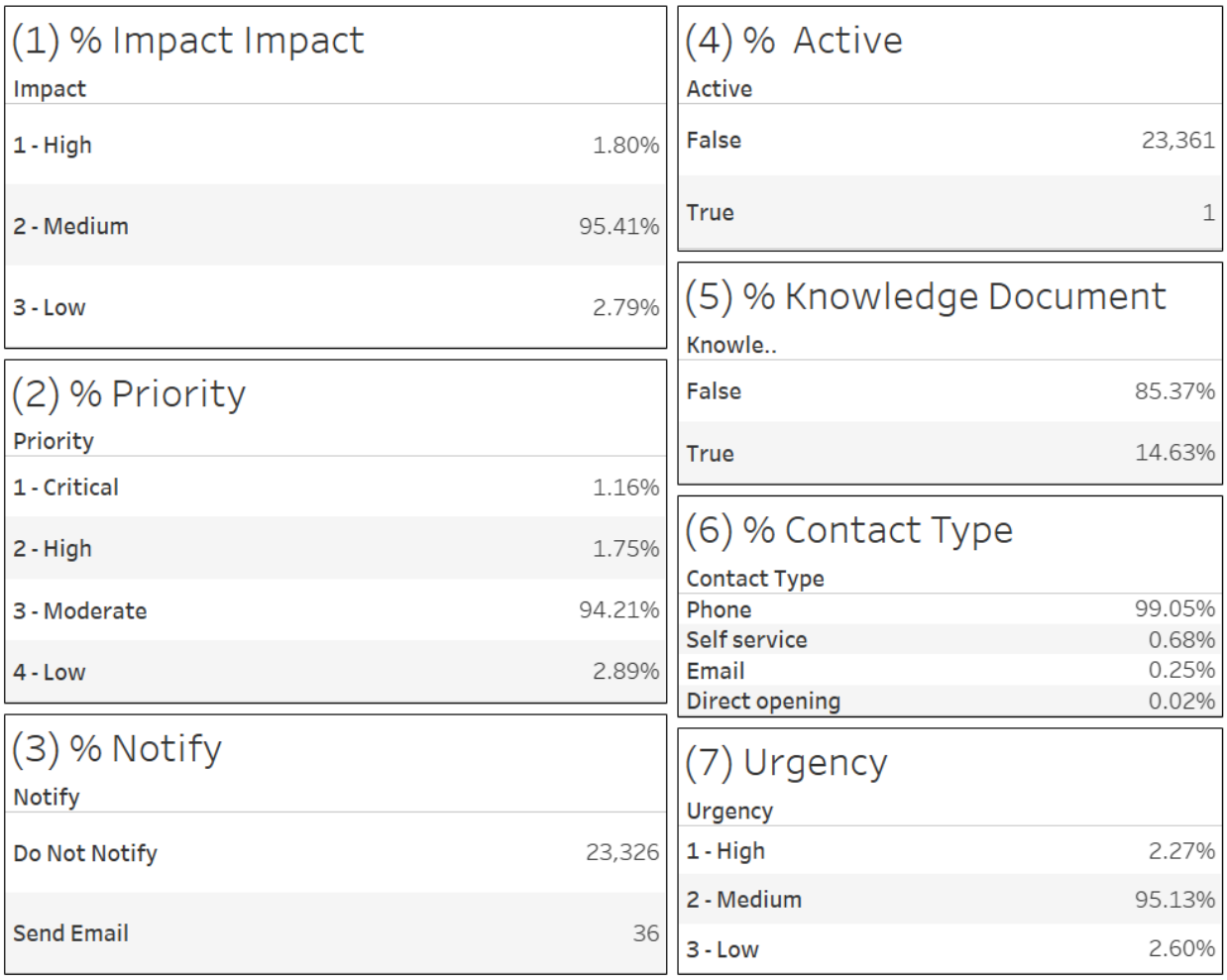

Figure 3.(1) Percentage of Incidents by Impact (2) Percentage of Incidents by Priority (3) Number of Incidents that have notify trigger on (4) Number of Incidents by Activity (5) Percentage of Incidents by Existence of Knowledge Document (6) Percentage of Incidents by Contact Type (7) Percentage of Incidents by Urgency

As seen on Table 3(1) most incidents reported have medium impact this agrees to Table 3(2) in which incidents are given moderate priority 94% of the time and as shown on Figure 3(7) are given medium yrgency 95% of the time. Moreover, most incidents don't have the notify trigger as seen on Table 3(3). Table 3(4) on the other hand shows that the incidents are mostly not active anymore which is a good indication. Incidents have a knowledge document associated to it 86% of the time and almost all of the incidents are reported through phone as shown on table 3(6)

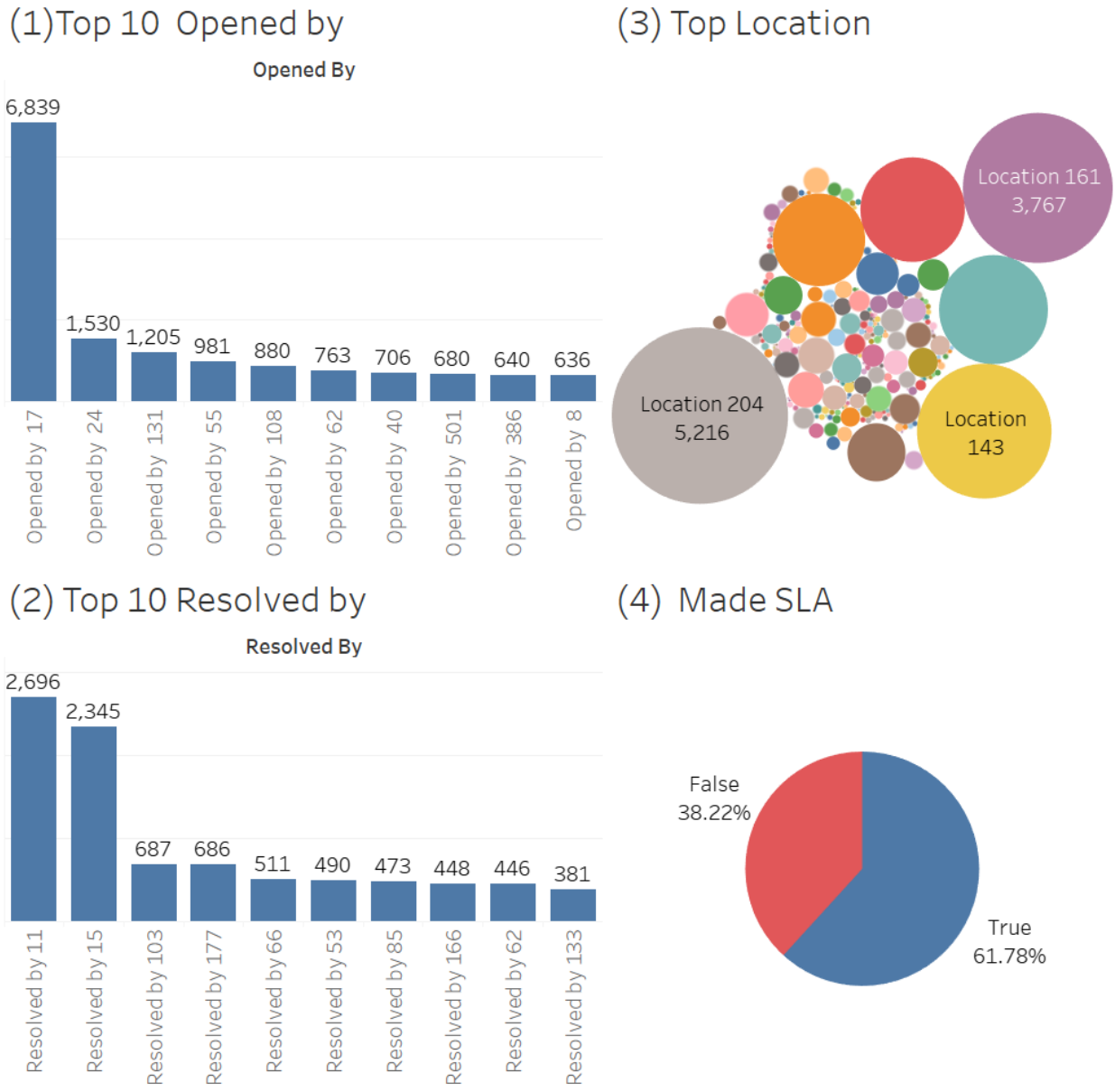

Figure 4 (1) Top Resources by number of incidents opened. (2) Top resources by number of incidents resolved. (3) Top location by number of incidents assigned (3) Percentage of Resources that made into SLA

Figure 4(1) shows that there is a noticeable number of incidents opened by 17 compared to the rest of the resources. We can also see that resource 11 and resource 15 resolve most of the incidents base on figure 4(2). Moreover Figure 4(3) shows that most incidents are assoigne to Location 204 followed by location 161. Based on Figure 4(4) the incidents are within the SLA 62% of the time.

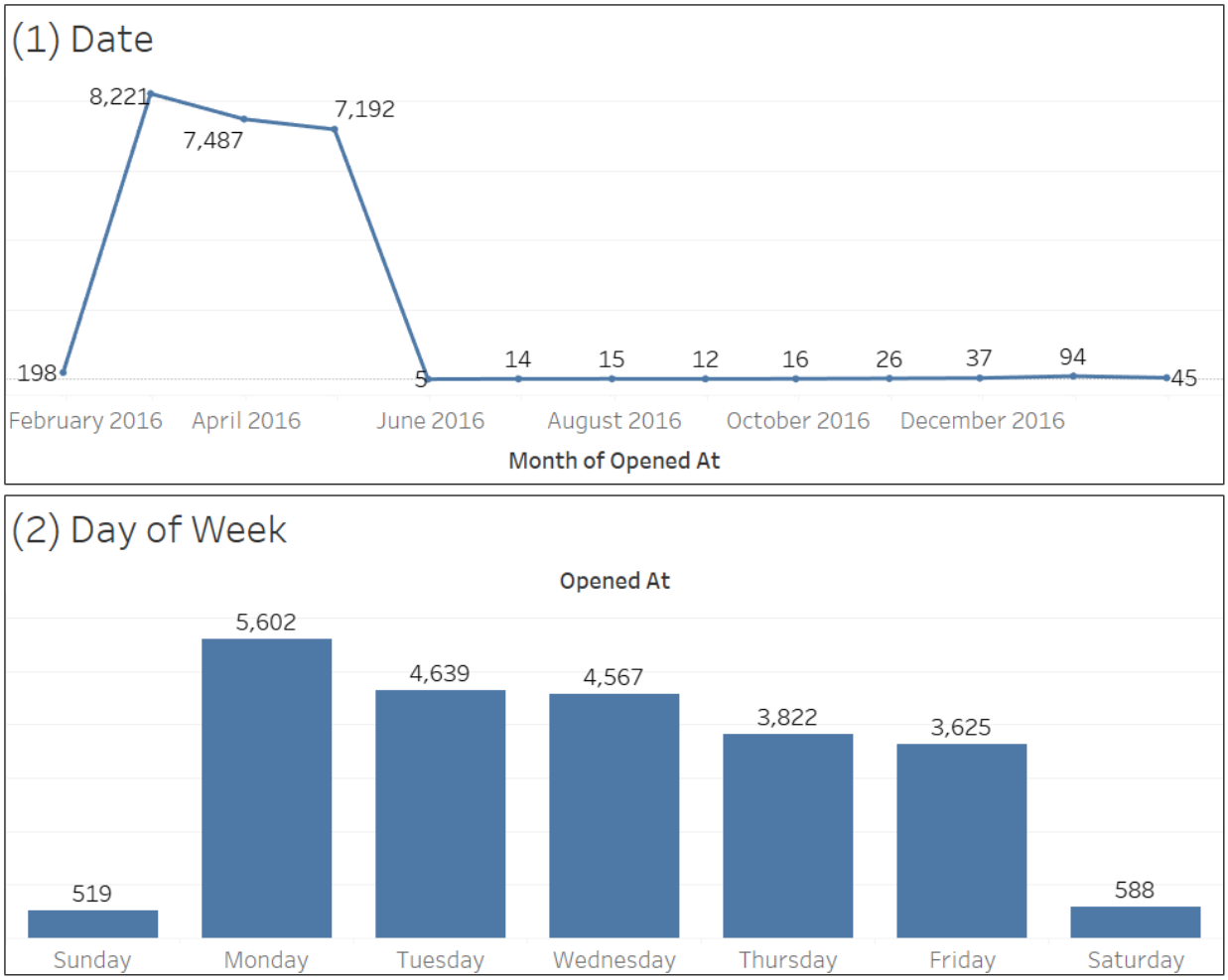

Figure 5. (1) Number of Opened Tickets by Month Opened. (2) Number of Tickets Opened by Day of Week

As we can see on Fiugre 5(1) there was an influx of opened tickets from March to May. Moreover, tickets seem to be open more on Mondays as seen on figure 5(2) and decreases as the weekday progresses.

ii. Bivariate Analysis

Table 4 (1) Top Categories that failed to meet the SLA. (2) Top Subcategories that failed to meet SLA (3) Top Groups that failed to meet SLA (4) Top Resolver that failed to meet SLA

(1)Top Groups that Failed to Meet SLA

Category	Made Sla False	True
Category 46	1,236	1,120
Category 53	997	1,590
Category 26	993	2,052
Category 42	643	2,495
Category 23	501	554
Category 9	466	655
Category 57	388	573
Category 37	384	714
Category 32	335	933
Category 20	234	697

(3)Top Groups that Failed to Meet SLA

Assignme..	Made Sla False	True
Group 20	230	164
Group 23	335	476
Group 24	373	686
Group 25	711	532
Group 27	216	302
Group 28	253	292
Group 39	374	825
Group 64	78	638
Group 70	1,353	6,552
Group 73	265	311

(2)Top Groups that Failed to Meet SLA

Subcategory	Made Sla False	True
Subcategory 174	1,967	4,140
Subcategory 175	630	1,078
Subcategory 223	629	2,555
Subcategory 164	535	686
Subcategory 170	214	285
Subcategory 135	209	352
Subcategory 36	205	240
Subcategory 275	198	351
Subcategory 9	183	553
Subcategory 28	29	350

(4)Top Groups that Failed to Meet SLA

Assigned To	Made Sla False	True
Resolver 17	942	1,356
Resolver 13	328	2,328
Resolver 57	275	148
Resolver 115	239	400
Resolver 149	219	162
Resolver 69	215	190
Resolver 194	110	566
Resolver 33	88	320
Resolver 94	35	415
Resolver 73	31	453

As seen on Table 4(1) incidents assigned to category 46 fail to meet SLA more than 50 percent of the time. Moreover, incidents assigned to Subcategory 174 although has a high resolved ticket that is within SLA still had the most incidents that failed to meet SLA as seen on Table 4(2). The same case is observed on Table 4(3) in which Group 70 had the greatest number of incidents that failed to be resolved within SLA despite it having a lot of resolved incidents.

Table 5. (1)Top Caller who had the most incidents that didn't make it to the SLA (2) Cross tabulation of Urgency vs Within SLA (3)

(1) Top Caller that Failed to Meet SLA

Caller Id	Made Sla False	True
Caller 4514	110	20
Caller 3763	38	18
Caller 1441	32	22
Caller 1904	28	410
Caller 93	25	15
Caller 4414	18	34
Caller 1531	12	41
Caller 90	11	46
Caller 4166	10	29
Caller 290	5	187

(3) Priority and SLA

Priority	Made Sla False	True
1 - Critical	265	5
2 - High	406	2
3 - Moderate	8,136	13,874
4 - Low	123	551

(2) Urgency and SLA

Urgency	Made Sla False	True
1 - High	521	10
2 - Medium	8,299	13,925
3 - Low	110	497

(4) Knowledge Document and SLA

Knowle..	Made Sla False	True
False	6,395	13,548
True	2,535	884

As seen on Table 5(1) Caller 4514 had the most incidents that didn't make it to SLA. On the other hand, Table 5(2) shows that most incidents that don't make it to SLA belongs to the Medium urgency although it can be noted that an incident belonging to a high urgency is more likely to be not meet the SLA. As seen on Table 5(3) there are an obviously more incidents that fail to meet the SLA when it belongs to an incident that has a high or critical priority ticket. As we can see on table 5(4) on the other hand, having a knowledge document doesn't affect if a ticket is going to meet SLA or not..

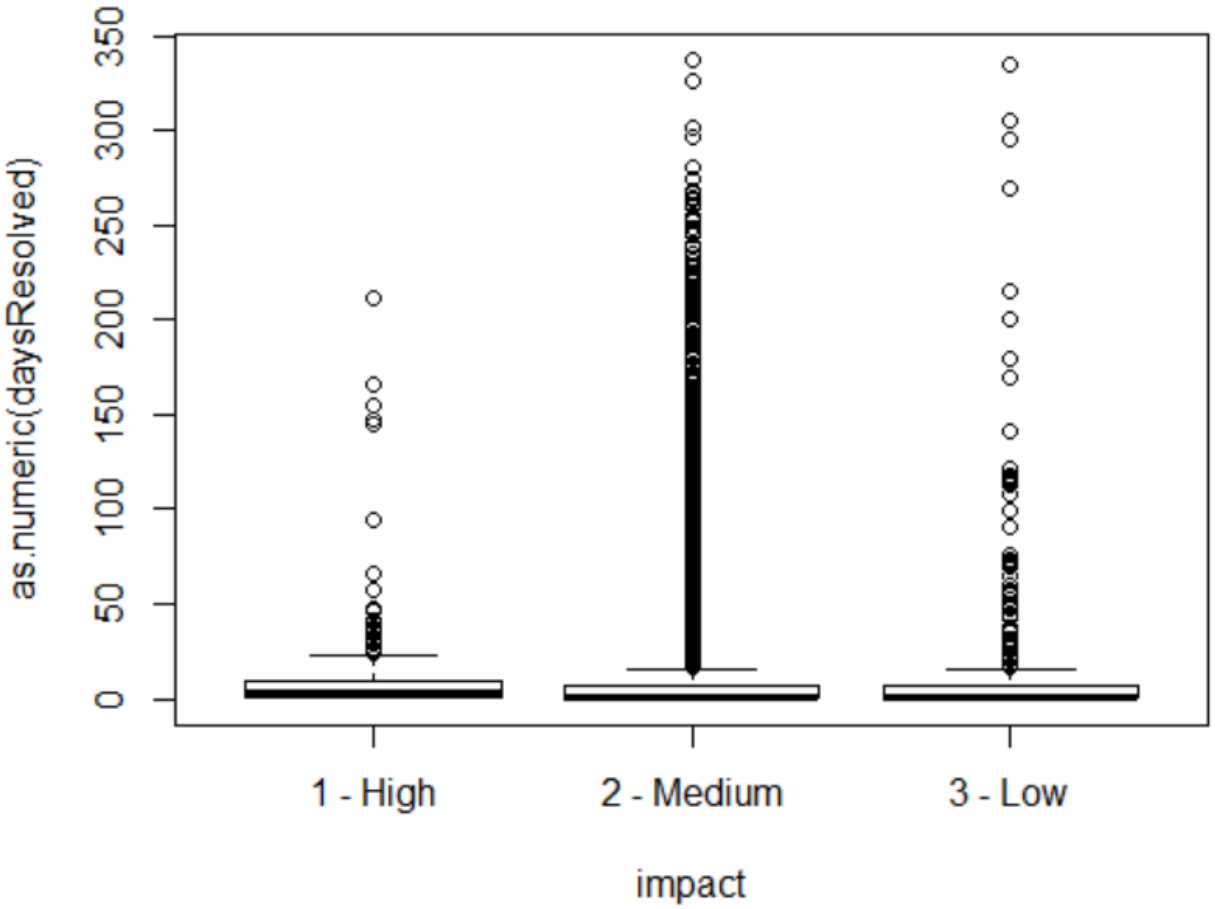

Figure 5. Distribution of the days before an incident is resolved vs the impact of the incident.

As figure 5 shows, the number of days before the incident is resolved is highly variable. We can see that even though the incidents that have a high impact variability, we should not let it last for more than 1 week.

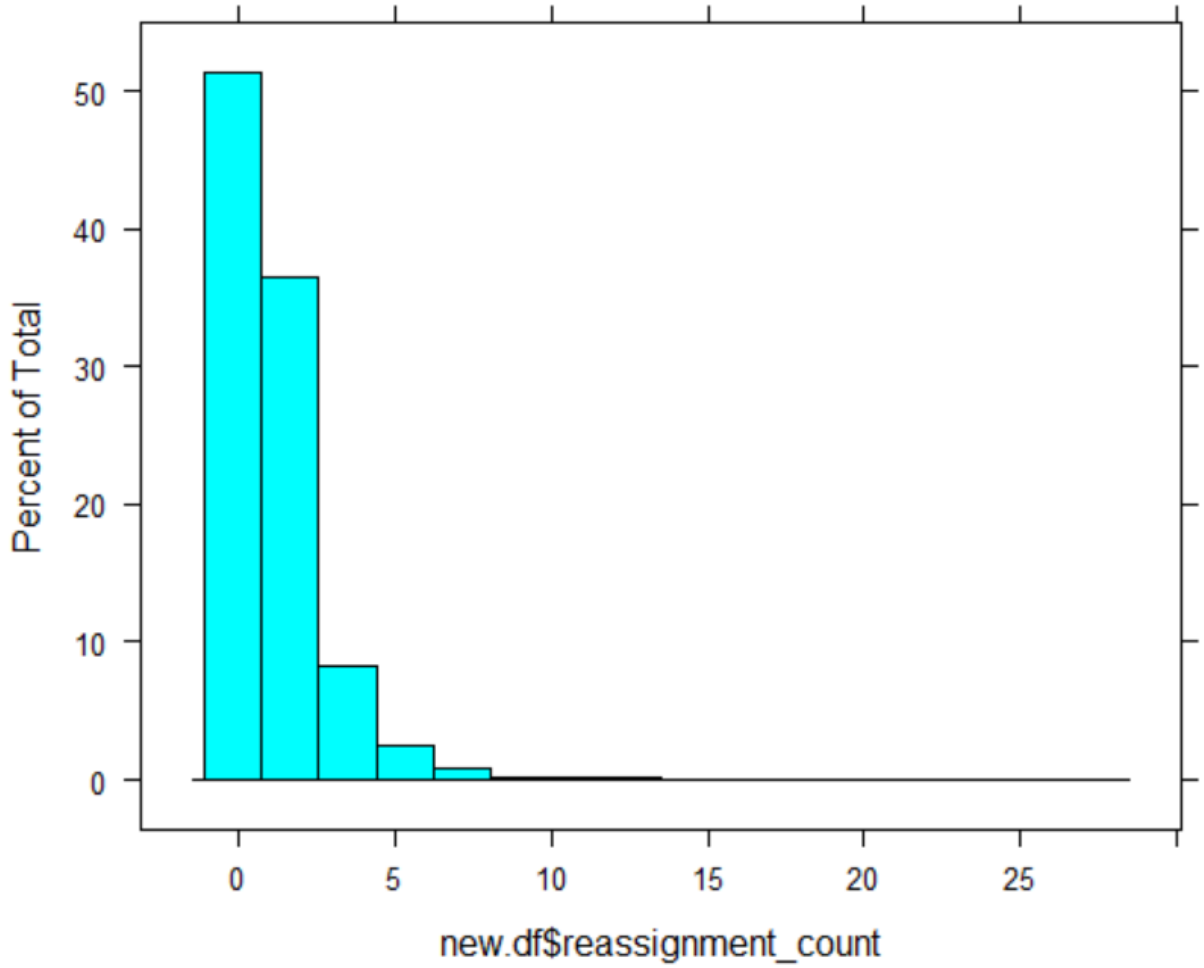

Figure 6. Distribution of Reassigned Tickets

Figure 6 shows that most tickets are reassigned mostly less than 5 times.

B. Data Mining Analytics/Business Process Discovery

a. Our dependent variable would be Made_SLA which is an indidication of wether the incident made it to SLA or not. Moreover, we will use the variables Priority, Urgency, Impact, SLA, Notify, Contact type, Knowledge Document, reassignment count and reopen count.

b. Logistic Linear Regression Model

Relationships between π(x) and x are usually nonlinear rather than linear. A fixed change in x may have less impact when π is near 0 or 1 than when π is near the middle of its range. In practice, *π(x)* often either increases continuously or decreases continuously as *x* increases. The *S*-shaped curves displayed in Figure 3.2 are often realistic shapes

c. **Stepwise Variable Selection Procedure**

Moreover, we are going to conduct a stepwise variable selection procedure in selecting our variables for prediction.

IV. Results

A. Choose the most appropriate method for representing your data. All numerical data gathered during the experiment must be presented in this section as a table, and a graph, Tables and graphs must be computer generated and may not be done by hand!

Table 6. Confusion Matrix of Predicted VS Actual Outcome

Prediction	Reference	
	FALSE	TRUE
FALSE	1681	693
TRUE	1053	4047

From Table 6, we can see that the logistic regression model is better at predicting an incident that met the SLA than not. However, we are more interested on predicting if an incident will not make it to SLA in order to come up with prevention measures if ever the factors affecting it comes up.

Table 7. Statistics on Model Assessment

Label	Estimate
Sensitivity	0.6149
Specificity	0.8538
Pos Pred Value	0.7081
Neg Pred Value	0.7935
Prevalence	0.3658
Detection Rate	0.2249
Detection Prevalence	0.3176
Balanced Accuracy	0.7343

As Table shows, that the model has an accuracy of 74.43% although it is more specific that it is more sensitive.

B. Interpretation of Logistic Regression Model

Table 8. Regression Coefficient Estimates of the Logistic Regression Model

Variable	Estimate Std.	Odds	Significant
reassignment_count	-0.6672	0.51	***
reopen_count	-1.34328	0.26	***
contact_typeEmail	-14.77911	0.00	
contact_typeIVR	-2.6677	0.07	
contact_typePhone	-15.32887	0.00	
contact_typeSelf service	-16.06011	0.00	
notifySend Email	-2.85605	0.06	***
impact2 - Medium	10.25436	28,406.12	
impact3 - Low	12.41749	247,085.57	
priority2 - High	-10.60321	0.00	
priority3 - Moderate	-5.49103	0.00	
priority4 - Low	-5.72379	0.00	
knowledgeTRUE	-1.9606	0.14	***

Table 8 shows that the more times an incident has been reassigned and reopened, the odds of the incident meeting not meeting the SLA increases. The same result holds too if the ticket owner is notified through email and if there's a knowledge document existing

V. Discussion/Conclusion

In this paper we have analyzed the data that came from an event log of an incident management process extracted from the audit system of the ServiceNowTM platform used by an IT Company. The aim of the study is to avoid outages and violation to the service level agreement (SLA) and reduce operational cost by optimizing resources and by assessing the inflow of tickets to make sure they are properly tagged, and the employees are not being overworked.

We have found out based on our exploratory data analysis that there's a comparatively more tickets assigned to assignment group 70. The same goes for resolvers 13 and 17. This might be a good point of investigation on whether assignment group 70's workload might be overflowing. Resolvers 13 and 17's workload should be investigated as well and made sure that it is properly distributed. This can be supported by the fact that even though resolvers 13 and 17 received the most incidents, they also have the most incidents that fail to meet the service level agreements.

Moreover, an influx of tickets on categories 26,42,53 might indicate a need for more training on this area or a more user-friendly document for possible self-service resolution. More focus should be given to incidents that fall in categories 42 and 53 since they are the top categories that fail to meet the service level agreement.An influx of incidents between March to May should be monitored as well, managers should pre-empt resources on their vacation leaves or extra work session during this season that might indicate a season for outages or requests to prevent ticket back logs.

It is alarming though to see that the rate of failure on meeting the SLA is very high in Critical and High priority tickets. Critical and High priority tickets affect the businesses and should be resolved as soon as possible. Process improvement should be given priority on this type of tickets. We also see a space for improvement on resolving tickets since we see outliers on resolution time specially on High and Critical priority tickets

Our logistic regression model requires more fine tuning, determining if a ticket is predisposed to service level agreement failure and investigating the factors that affect it is useful for management in order to minimized failures. This will be a good countermeasure and point of improvement for the service providers. Failure to meet SLAs causes the BPO money, time, and resources and learning how to meet them and learning how to avoid SLA violation will earn the trust of the business and will save the BPO company resources.

References

Balakrishnan Karthik, M. U. (2008). Outsourcing of front-end business processes: Quality, information, and customer contact. *Journal of Operations Management Volume 26, Issue 2*, Outsourcing of front-end business processes: Quality, information, and customer contact.

Headlee, B. (2016). *ITSM Analytics Whitepaper* . IBM.

Kissflow. (2018, October 21). *Incident Management Process Flow for Businesses*. Retrieved from Kissflow: https://kissflow.com/case-management/incident-management-process/

Panina Daria, A. J. (2005). Acceptance of electronic monitoring and its consequences in different cultural contexts: A conceptual model. *Journal of International Management*, 269-292.