Understanding the Role of Change in Incident Prevention

Sinem Güven and Karin Murthy
IBM T. J. Watson Research Center
Yorktown Heights, NY, USA
{sguven, kmurthy} @ us.ibm.com

Abstract— IT service providers are faced with a dilemma when trying to ensure proper function and effective operation of their clients' infrastructure. On one hand, frequent changes to the IT infrastructure are required to ensure smooth operation; on the other hand, studies show that changes are responsible for 80% of all incidents that result in client outages. This paper proposes a novel methodology for investigating the role of change in incident prevention. We provide a detailed analysis of the change-incident space, offer algorithms on linking incidents to changes that caused them, and show how such data can be effectively used to build predictive models for incident prevention. We conclude by presenting our methodology applied to a real-world dataset and use cases.

Keywords- incident prevention, change risk, incident management, change management, risk management, predictive analytics

I. INTRODUCTION

Incidents are issues within an IT infrastructure that relate to the disruption of a critical IT service. Incidents may be automatically discovered through monitoring systems, or manually detected by system admins. *Incident Management* addresses the identification and resolution of issues within an IT system to restore service operation and prevent recurrence. As soon as an incident is detected, system admins are under a great deal of time pressure to find the source of the issue to be able to resolve it. Depending on the complexity of the underlying problem, it can take up to several days before an incident is resolved, resulting in financial penalties and dissatisfied clients for the service provider. It is, therefore, crucial for service providers to have effective and pro-active risk management for incident prevention.

In order to provide stable and high availability services, IT service providers need to make frequent *changes* to their clients' infrastructure to continue enabling proper functioning and effective operation. *Change Management* focuses on the implementation of IT changes, required externally by the client, or internally by the service provider. It is often reported that, change failure is one of the biggest problems IT service providers face today. In fact, previous reports [1] showed that changes are responsible for 80% of all incidents that result in client outages. Change-related incidents, thus, incur a significant cost not only for the service provider to re-implement such changes, but also to manage their impact on the business.

An essential aspect of an effective Change Management process is *Change Risk Management*, which aims to assess and mitigate change risk to avoid change failures and, thus, minimize incidents causing disruption to the clients' business. Although several researchers attempted to address the problem of assessing risk associated with IT change implementations [2, 3], the relationship between change and incident, and how changes drive incidents have been historically hard to establish [4]. Wickboldt et al. [5] present an automated risk assessment method that uses historical data of change execution to reduce service disruptions caused by changes. Similarly, Hagen et al. [6] use change analytics to prevent changes from causing incidents by detecting conflicts among IT change operations and safety constraints. Although the goal of these researchers is to reduce incidents caused by change, they focus on failed change reduction in an effort to reduce resulting incidents. While *failed change* prevention through risk management is very important and necessary, given the fairly small change failure rates (in our experience < 1%), it does not seem to be the only answer to reducing client outages caused by changes. In this paper, our goal is to investigate the role of change in incident reduction through a detailed study of the change-incident relationship.

Section II describes our methodology on how to build predictive analytics for change-related incident reduction. First, we describe how we construct a dataset that links incidents to changes that caused them. We then provide examples of how powerful visual analysis and complementary statistics can help gain insights into the constructed dataset and shape our predictive analytics for incident prevention. In Section III, we describe a *pro-active* approach for predicting, at change preparation time, the likelihood of a change causing an incident. We then present a comparative study to test the effectiveness of focusing on failed changes for incident prevention using data and use cases from real client accounts. We conclude by summarizing our findings in Section IV.

II. APPROACH

This section provides a detailed analysis of the change-incident domain as well as our approach to building predictive analytics for change-related incident reduction.

A. Constructing a Dataset

In order to study the relationships between changes and incidents, the first step is to construct a dataset that entails changes that caused incidents, as well as changes that did not lead to incidents. In most situations, this information is not explicitly collected. Thus, in our earlier work [7], we developed methods to construct a training dataset for model building by analyzing historical change and incident tickets.

978-3-901882-85-2 (c) 2016 IFIP

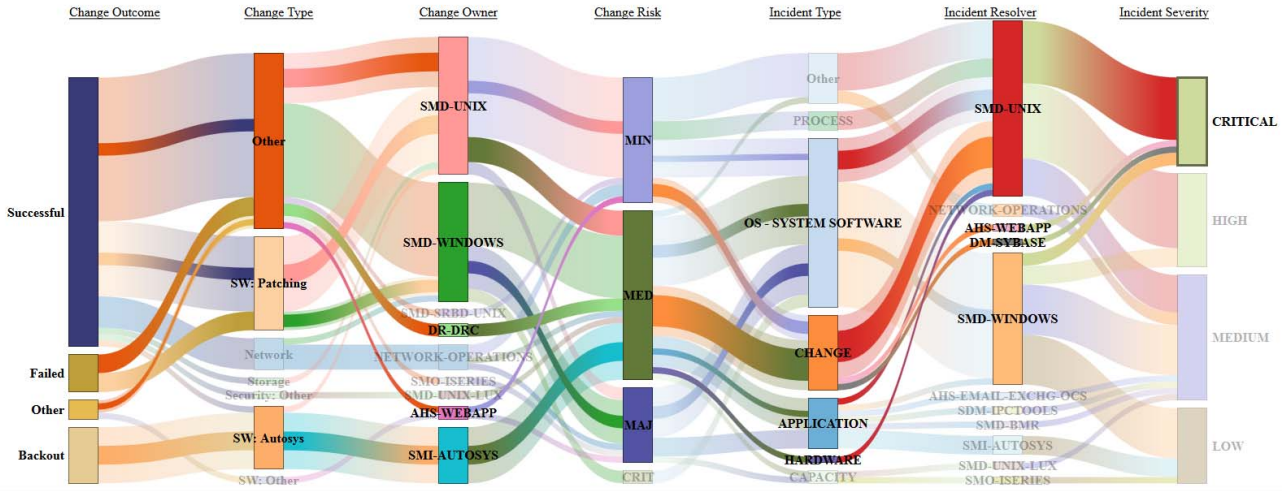

Figure 1. Relationship between Change and Incident (highlighting changes causing incidents of critical severity)

If the incident resolutions provide explicit mention of changes that led to the incidents, our algorithm uses regular expressions to encode change ID patterns and scans the resolutions for such patterns to identify linkages. In case the resulting dataset does not yield enough number of pairs, our algorithm also links changes to incidents by analyzing several structured and unstructured dimensions, and ranks potential (CH→IN) pairs by similarity. A subject matter expert can then validate the discovered pairs to build a ground truth dataset, or accept pairs with high confidence.

B. Visualizing Change / Incident Relationships for Insight Generation

Once the training dataset is constructed, the next step is to discover and visualize trends around this dataset to determine what type of predictive analytics can be derived from the data.

Figure 1 shows a Sankey diagram, which depicts the relationships between discovered CH→IN (change induced incident) pairs for a client account. This visualization connects a given change with the incident it caused through several dimensions to reveal *trends* (e.g., that a large number of incidents caused by change were related to OS – SYSTEM SOFTWARE) as well as provide *insights* on what actions to take (e.g., provide additional training to change owner groups SMD-INTEL, SMD-WINDOWS, and SMI-AUTOSYS) to reduce similar changes causing similar incidents in the future. This approach takes advantage of both existing dimensions from *structured* change and incident data (e.g., change and incident owner), as well as new dimensions we discovered from *unstructured* data (e.g., change type) [7]. In order to make the Sankey chart more readable, we automatically group rare values for each dimension into one value called 'Other' and exclude dimensions that do not provide valuable information.

Sankey visualization is useful to gain an at-a-glance view of the problem areas. One important insight we see in Figure 1 is the high number of successful changes that led to an incident. That means many changes were successfully implemented but later caused an incident. By using the highlighting mechanism of the Sankey chart, we can also confirm that incidents of critical severity are caused both by successful and failed changes. Additionally, we can see that the current mechanism of assigning the risk of a change is not capturing the true risk of causing an incident; most changes that led to a critical incident were assessed at change creation time to have only minimal or medium risk.

Sankey visualization also reveals trends in the data that support predictive modeling. If every change that causes an incident is unique then there may be little that can be done to build predictive models for incident prevention. Without having to compute all kinds of statistics, having the ability to visualize, for example, that most of the changes causing incidents are related to a limited subset of change types, provides a head start in what potential predictors to inspect during predictive modeling. For example, if the target is, say, to create a predictive model to capture high severity incidents caused by change, we can easily see from the Sankey diagram that the majority of the high severity incident causing changes come from a few specific owner groups for this account, and hence change owner group would likely be an important predictor.

C. Analysis of Change / Incident

During the analysis of our data set, the Sankey visualization revealed an important insight, namely that the majority of the changes that led to incidents were successful changes for our initial test account. In order to verify whether what we observed for one account, in terms of the high number of successful changes causing incidents, holds true in general, we extended our analysis to 15 accounts covering 300,000 changes over a time span of 6 months. Columns 2 and 3 in Table 1 show, for each account, the percentage of changes that were implemented *successfully* versus the percentage of changes that *failed* during execution. (The remaining changes were cancelled, closed with issues, or had no closure code.)

Table 1. CH → IN Statistics for 15 Client Accounts

Client	% of Successful Changes	% of Failed Changes	% of Successful Changes Causing Incidents	% of Failed Changes Causing Incidents	% of Incidents Caused by a Successful Change	% of Incidents Caused by a Failed Change
AC 1	80%	0.4%	9%	3%	94%	0.2%
AC 2	42%	0.2%	19%	25%	98%	0.3%
AC 3	72%	0.0%	1%	n/a	88%	0.0%
AC 4	24%	0.3%	2%	4%	93%	0.9%
AC 5	66%	0.9%	7%	0%	96%	0.0%
AC 6	65%	0.6%	13%	17%	96%	1.1%
AC 7	77%	2.1%	1%	33%	50%	41.7%
AC 8	69%	1.5%	6%	14%	86%	4.0%
AC 9	85%	0.3%	9%	35%	79%	3.5%
AC 10	62%	0.3%	3%	5%	43%	0.3%
AC 11	79%	1.0%	3%	4%	74%	1.3%
AC 12	80%	0.4%	2%	6%	87%	1.3%
AC 13	63%	0.1%	0%	9%	43%	14.3%
AC 14	79%	0.0%	2%	0%	78%	0.0%
AC 15	69%	0.2%	2%	0%	60%	0.0%
Overall	**66%**	**0.3%**	**3%**	**12%**	86%	1.7%

We used the algorithm described in [7] to automatically identify CH→IN pairs using explicit linkage. Based on this data, columns 4 and 5 in Table 1 show what percentage of successful or failed changes caused incidents, respectively. (Note that in reality those percentages may be slightly higher as some incidents caused by a change may not have proper documentation that links the incident to the change.) Finally, columns 6 and 7 in Table 1 show what percentage of incidents caused by a change was due to a successful or failed change, respectively. Overall, a failed change is four times more likely to cause an incident than a successful change (only 3% of successful changes cause an incident versus 12% of failed changes). However, given that there are many more successful changes than failed changes, still overall 86% of all incidents caused by change are due to a change that was closed successfully and later caused an incident.

III. Comparative Predictive Model Design

A. *Setting the Stage*

As discussed in Section I, the goal of this paper is to understand the role of change in incident prevention. Traditionally, the focus of change risk management is on failed changes with the expectation that reducing failures would reduce incidents. However, our analysis, in Sections II B and C, revealed that, for the most part, it is the seemingly *successful* changes that lead to incidents. With this insight, before diving into predictive modeling, we first wanted test the effectiveness of the traditional methodology, i.e. whether failed change predictors also identify incident inducing changes. The rest of this Section describes our approach and experience with comparative predictive model design that helped us ultimately reach higher accuracy and recall rates.

B. *Predicting Failed Changes*

Our dataset is assembled from real client account data (Section II A), and comprises 1,600 changes, 50% of which are used for training and the remaining 50% for testing. We selected an equal number of Failed and Successful changes for the training and testing datasets, and also additionally ensured that each category {Successful vs. Failed} had an equal number of {Incident vs. No_Incident} cases to remove any bias. We then trained and tested a predictive model using several different machine learning algorithms, however, for our data set, the Classification and Regression (C&R) Tree method [8] gave us the best recall rates. The C&R Tree models used were constructed using SPSS using predictors such as owner group, change category, change priority, change risk, as well as *derived* change properties (such as change configuration item and change action) to predict if the input change is likely to fail. SPSS automatically performs feature selection to only use the significant predictive data fields. Testing is also performed through SPSS by using k-fold cross validation. The resulting model was statistically significant ($p < .005$), which indicates that the predictors reliably distinguished between changes that failed and changes that did not fail. We then inspected the test changes and compared their predicted outcomes to their observed outcomes to calculate:

a) recall rate (i.e., how many of the failed test changes were correctly captured as 'failed' by the predictive model)

b) accuracy (i.e., how many of the total set of test changes had correct prediction of their actual outcome – 'successful' or 'failed').

Our goal was to test if building a predictive model to detect and prevent failed changes would also help with change induced incident reduction. Although the overall accuracy of this model is not poor (71%), and it has a decent performance for correctly predicting if a change will fail (77% for actually failed changes that caused an incident), it is still fairly ineffective at capturing changes that cause incidents if the change was successful at closure time. For example, looking at Table 2, we see particularly low recall (36%) with flagging successful changes that led to incident when we predict the change outcome using this model. This result validates our intuition that focusing on failed change reduction alone is not an effective way of addressing change induced incident prevention.

Table 2. Accuracy and Recall for Predictive Model Targeting Classification of Failed vs. Successful Changes

TARGET	OVERALL ACCURRACY	FAILED		SUCCESSFUL	
		with INCIDENT	w/o INCIDENT	with INCIDENT	w/o INCIDENT
FAILED vs. SUCCESFUL	71%	77%	64%	36%	89%

C. *Predicting Changes Causing Incidents*

Next, we decided to train a second predictive model, which focused directly on incidents, namely whether a given change is likely to cause an incident irrespective of if fails or succeeds. For this model, we updated our testing and training datasets to differentiate incident causing changes

from non-incident causing ones. We then trained and tested a C&R Tree model with the same predictors as before (see Table 3 for results).

With this predictive model, we see that successful changes that led to incidents are correctly identified with a much higher recall than before (36% vs. 67%), but at the expense of an overall lower accuracy (64%). Therefore, the approach of focusing on incident causing changes alone overall does not seem to be the right answer either.

Table 3. Accuracy and Recall for Predictive Model Targeting Classification of Incident vs. No_Incident

TARGET	OVERALL ACCURRACY	FAILED		SUCCESSFUL	
		with INCIDENT	w/o INCIDENT	with INCIDENT	w/o INCIDENT
INCIDENT vs. NO_INCIDENT	64%	41%	76%	67%	78%

D. *Predicting Problematic Changes*

If we consider our data set in its entirety (see Figure 4), we see that we first focused on correctly classifying Failed vs. Successful changes and tested if this could be effective at incident prediction. Our second attempt targeted correct classification of Incident vs. No_Incident changes. However, the actual set of problematic changes are, in fact, a combination of these two datasets, as depicted in Figure 4 (c). We, therefore, decided to train a third predictive model, which focuses on proactively identifying *problematic changes* (which comprise all failed changes as well as successful changes that lead to incident). For this model, we updated our test and training data sets to differentiate between problematic and non-problematic changes. We then trained and tested the C&R Tree model with the same predictors as below. Table 4 shows the results.

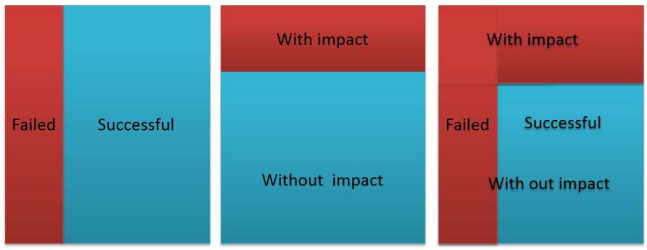

Figure 4 Data set for a) Model 1, b) Model 2, c) Model 3.

Table 4. Accuracy and Recall for Predictive Model Targeting Classification of Problematic vs. Non-Problematic Changes

TARGET	OVERALL ACCURRACY	FAILED		SUCCESSFUL	
		with INCIDENT	w/o INCIDENT	with INCIDENT	w/o INCIDENT
PROBLEMATIC vs. NON_PROBLEMATIC	84%	100%	100%	55%	89%

Our third predictive model yielded an overall accuracy of 84% and an impressive 100% recall for correctly identifying any type of failed change (incident causing or not) as *problematic*. Although the proactive detection of successful changes that led to incident was lower than the second predictive model, it is still much higher than the traditional approach (36% vs. 55%). If we consider the performance of all three algorithms in terms of catching problematic changes (failed or successful with incident), we also see that the third model outperforms the rest significantly at 85% coverage (see Table 5). Our work on change induced incident prevention is by no means complete, but this analysis sheds some light on the important characteristics of changes to guide future direction.

Table 5. Problematic Change Identification Recall across Predictive Models

MODEL 1	MODEL 2	MODEL 3
(77+64+36)/3 = 59%	(41+76+67)/3 = 61%	(100+100+55)/3 = 85%

IV. Conclusions and Future Work

In this paper, we have described a novel approach for investigating the role of change in incident prevention. We have provided a detailed analysis of the change-incident space, summarized our previous work on linking incidents to changes that caused them, as well as outlined how such data can be effectively used to build predictive models for incident prevention.

While traditional efforts for change induced incident prevention often focus almost exclusively on avoiding *failed* changes, our analysis revealed that, for the most part, it is the seemingly *successful* changes that lead to incidents. This observation proved crucial for building predictive models that accurately capture problematic changes.

We would like to extend this work to study the incident resolution domain to test the effect of successful versus failed changes when determining, at resolution time, whether an incoming incident is caused by a change. Further, we would like to continue our efforts on change and incident structured data consolidation to enable using data from multiple accounts even when the structured field taxonomies are not identical. Such efforts would provide access to even larger datasets for building predictive models with greater accuracy.

V. References

[1] Gartner IT Security Summit, Best Practices for Continuous Application Availability, 2005.

[2] S. Güven, C. Barbu, D. Husemann, D. Wiesmann, "Change Risk Expert," In IFIP/IEEE NOMS, Maui, Hawaii, 2012.

[3] Bianchin et al., "Similarity Metric for Risk Assessment in IT Change Plans," In IEEE CNSM, Niagra Falls, ON, Oct. 2010.

[4] J. Druebert. "Changes, Incidents & Unintended Consequences," In Insight on IT Service Management, 2010.

[5] Wickboldt et al., "Improving IT Change Mgmt Processes with Automated Risk Assessment," In IEEE DSOM, Oct. 2009.

[6] S. Hagen, M. Seibold, A. Kemper, "Efficient Verification of IT Change Ops.," In IFIP/IEEE NOMS, Maui, Hawaii, 2012.

[7] S. Güven et al., "Towards establishing causality between Change and Incident," In IEEE/IFIP NOMS, Turkey, 2016.

[8] L. Breiman, J. H. Friedman, R. A. Olshen, C. J. Stone. "Classification and Regression (C&R) Trees," 1st Edition, CRC Publishing, 1984.