HDI 2017 CONFERENCE & EXPO

SESSION 603
Thursday, May 11, 4:00pm - 5:00pm
Track: Service Desk Foundations

When IT Hits the Fan: Best Practices for Major Incident Response

Peter McGarahan
Senior IT Director, Infrastructure Corporate IT, First American Title Insurance Co.
Pete@mcgarahan.com

Session Description

High-impact incidents can make or break your organization. It can get messy when IT hits the fan, but there are ways to minimize the damage and come out with little to no negative impact on the business. So, what happens when you suffer one of these critical, high-impact incidents? Who needs to be involved, and how will you communicate with them? Do you currently have a plan—and how often do you update it? In this session, you'll get the scoop on all the best practices, case studies, frameworks and real life examples of challenges/solutions that will help you quickly and effectively work through major incidents.

Speaker Background

Pete McGarahan is the senior director of IT infrastructure services for First American, as well as an industry expert and thought leader in global ITSM. With thirty years of business, IT, and service leadership experience, Pete enjoys sharing lessons learned and career experiences through published articles and by presenting at industry conferences. He has received various industry awards and honors, including the HDI Team Excellence Award for his work with the Taco Bell support organization, the Top 25 Professionals in the Service and Support Industry from IT Support News, and The Legend of the Year (twice) at the STI Knowledge Symposium and Help Desk Professionals conference. Pete is well known in the support industry for his endless positive energy, leadership, mentoring, and advice.

Session 603: When IT Hits the Fan: Best Practices for Major Incident Response

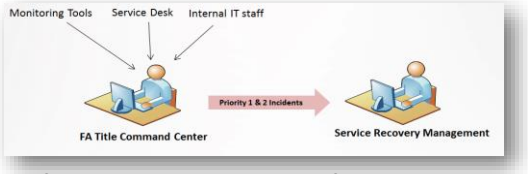
Peter McGarahan
Senior IT Director, Infrastructure
Corporate IT
First American Title Insurance Co.

About The Speaker

- 12 years with PepsiCo/Taco Bell IT and Business Planning
- Managed the Service Desk and all of the IT Infrastructure for 4500 restaurants, 8 zone offices, field managers and Corporate office
- 2 years as a Product Manager for Vantive
- Executive Director for HDI
- 6 years with STI Knowledge/Help Desk 2000
- 7 years with McGarahan & Associates (www.mcgarahan.com)
- 2 years as Chairman, IT Infrastructure Management Association
- 4 ½ years as Senior Director, Infrastructure – First American

Our Service Recovery Mgmt (SRM) Team

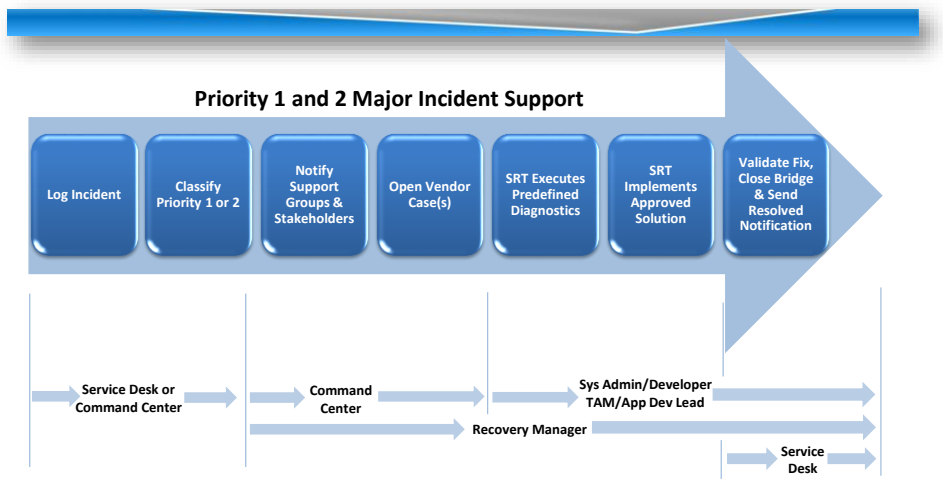
- Team members located in Santa Ana (2), Texas (1), & and Bangalore (3).
- SRM is part of Data Center Operations and the central point of escalation for priority 1 and 2 incidents.



- Service Recovery Managers are Information Technology Infrastructure Library (ITIL) certified.
- Interrelationships established with key IT Service Management processes: Change, Incident, Problem & Configuration Management.

Mission: To minimize the impact of service disruptions to our business clients through effective management of high severity incidents.

SRM High Level Process Flow



Benefits of SRM

- SRM manages all incident logistics so technical teams can focus on service restoration.
- Results in REDUCED TIME TO RESTORE!
- Maintain high availability of technology services critical to the business.
- Ensures adherence to First American IT Service Management policies & procedures and ITIL best practice guidelines.
- Detailed documentation enables accurate reporting and facilitate problem reviews to mitigate future recurrences, develop preventative strategies and long term remediation plan.

Continual Service Improvement (CSI)

Service Recovery Management C.S.I. Initiative:

- The Service Recovery Management team conducts ongoing process performance assessment through customer surveys and internal process performance evaluation exercises.

Post Incident:

- Customer Surveys for priority 1 incidents and select priority 2s
- Internal SRM team peer review within 24 Hours of incident resolution
- Major Incident Review (MIR) for priority 1 incidents

On-Going:

- Survey data reviewed regularly for training or process improvement opportunities.
- Weekly internal team meetings to review lessons learned from recent major incident escalations; reinforce actions taken that were effective; identify process deficiencies and areas for improvement.
- The Service Recovery Management team may reach out to key IT and BU contributors to participate and have a voice in our service improvement Initiatives.

Priority Matrix

Priority Matrix

Incident Priority Is Determined By the Level of **Impact** and **Urgency**.

Priority = Impact + Urgency

Impact				
Factors	Extensive	Significant	Moderate	Minor
# of People	>100 People	20-100 People / VIP	5-20 People	1- 5 People
Scope/Location	Global	Entire Business Unit	Branch/Office/ Building	Department
Activity/ Transaction/ Fee	•Extensive transaction at stake (>1M liability) •Multi site deal at stake •#1 Customer •Fee loss >10K	•Significant transaction at stake (500K to 1 M liability) •Can't print a check(s) •Strategically important customer •Agent impacted •Fee loss 5K -10K	•Moderate transaction at stake (300-500K) •Fee loss 1K – 5K	•Single transaction at stake (<300K) •Fee loss <1K

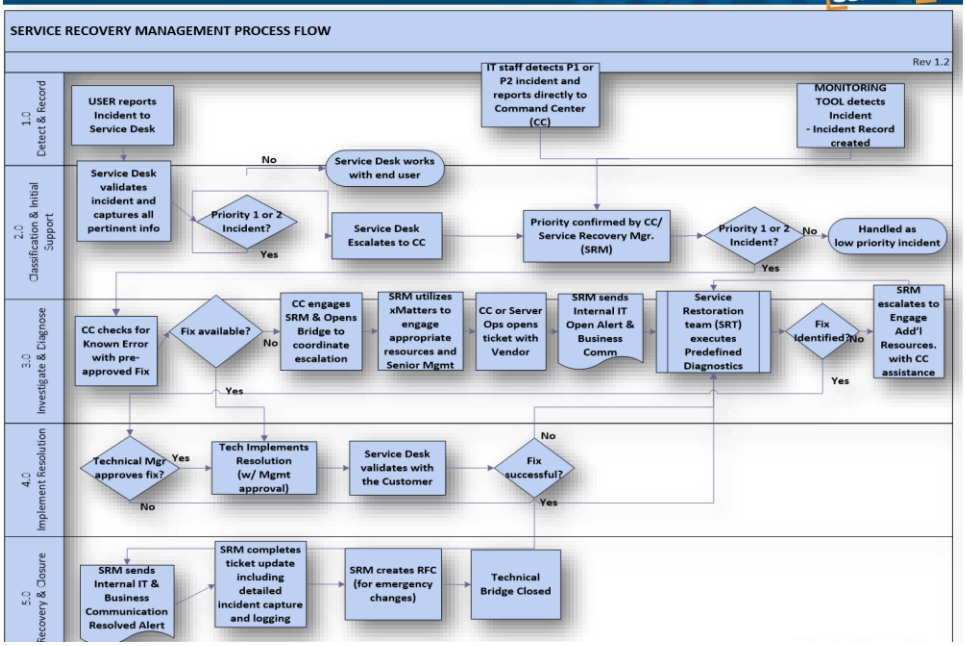
Urgency			
Factors	High	Medium	Standard
Revenue Generating	Direct	Support	Not Related
BCP Classification	Business Critical	Direct Support of Business Critical	Not Business Critical
Security Classification	•Imminent Virus Outbreak •Malicious intrusion detected	•Moderate Virus Threat •Vulnerability discovered in self assessment	Routine virus update
Compliance (SOX, SAS70, other)	•Immediate audit failure •Penalties will be assessed	Compliance deficiency/potential risk of audit failure	Minor audit deficiency

PRIORITY				
		Urgency		
		High	Medium	Low
Impact	Extensive/Widespread	1	2	2
	Significant/Large	2	2	3
	Moderate/Limited	2	3	4
	Minor	3	4	5

Priority Definitions

- **Priority 1:**
  - A critical incident affecting the availability or performance of revenue generating applications or business critical services for a significant number of users.
    (Example: FAST, our premiere business title application is unavailable).
- **Priority 2:**
  - A major incident where performance of a revenue generating application or business critical service is degraded or experiencing partial loss of functionality.
    (Example: Multiple users experiencing unusual slowness in AgentNet our external facing premiere application for title processing)

SRM Process Flow



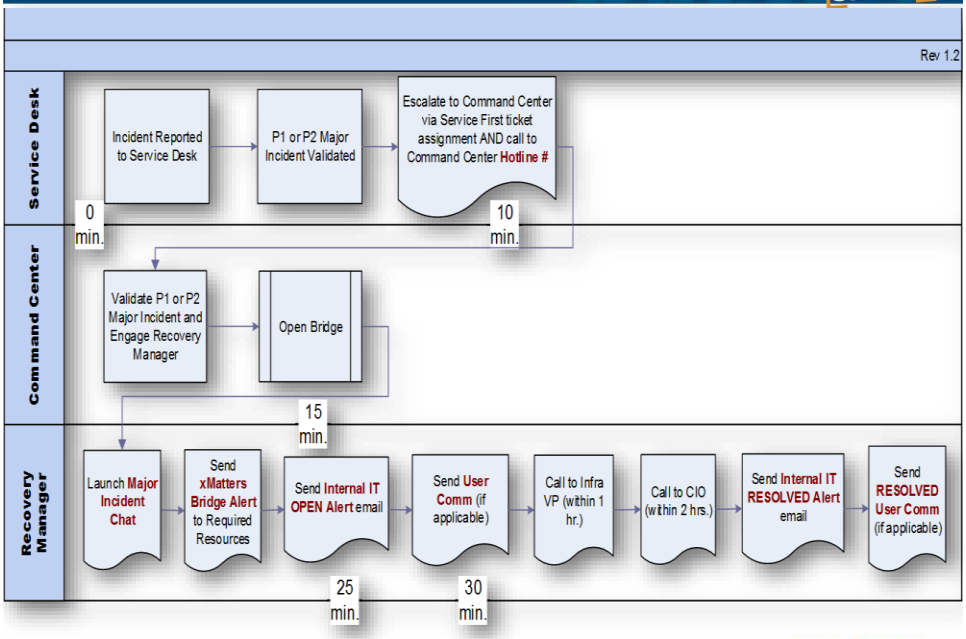
Communication Challenges

- Email is very pervasive and it's easy to lose management and visibility to the importance of the message to the intended and targeted audience.
- Frequency
- Telephone bridges either too technical or not technical enough.
  - Business people on a technical resolution bridge call.
  - Technicians on a business resolution bridge call.

Actions to Address

- Communicate only Incident and Resolution by email.
- Establish a subscription based notification system.
  - For less critical and impacting issues, subscribers can request an update / communication.
- For highly critical issues run 2 bridges:
  1. Technical resolution bridge
  2. Business resolution bridge
     - Lets the business manage communication to affected parties (targeted communications).

SRM Communication Process Flow



Communication Methods

- Command Center:
- Hotline #:
- 714-250-7550
  - The number to call when escalating Priority 1 or 2 incidents to the Command Center

Communication Methods

Major Incident Chat:

Purpose: To coordinate, record and ensure accuracy of timeline and technical information discussed on the conference bridge.
Tool used: Microsoft Lync
Responsible: Recovery Manager
Members/Recipients (default):

- Command Center & NOC Staff (Offshore & Onshore)
- Service Recovery Managers
- IT Service Desk Managers and Leads
- Technical Account Managers (TAM1, TAM2, TAM3)
- Corp Infrastructure Senior Management
- Business Relationship Management (BRM)

Bridge Alerts (e.g. Everbridge IT Alerting & xMatters):

Purpose: To summon technical resources and IT managers required on the bridge call
Tool used: Vendor hosted Application / Notification system
Responsible: Service Recovery Manager
Recipients (default):

- Application specific support team (Application Owner and Technical Owner)
- Corp Infrastructure Support teams
- Technical Account Manager (TAM)
- Corp Infrastructure Senior Management
- Executive Management (for P1 only) – Larry Godec
- Business Relationship Mgmt (BRM)
- IT Service Desk

Communication Methods

Internal IT Email Alerts (OPEN/UPDATE/RESOLVED):

Purpose: To notify internal Corp IT and Business Unit IT staff of a Priority 1 or 2 outage/issue and provide updates on progress of restoration efforts.
Content: Can include pertinent technical details.
Tool used: Email alerts generated from Service First incident record
Frequency: Sent within 15-20 minutes of escalation to Command Center; updates every 30 min. (P1) or 60 min. (P2) or as new information becomes available.
Responsible: Recovery Manager
Recipients: App Dev and BU-IT Managers

- Corp Infrastructure Support teams, Managers and Directors
- Executive Management

User Communications (aka 'FA Corp-IT Communications'):

Purpose: To notify user community and IT staff of a Priority 1 or 2 outage/issue.
Content: High level updates and non-technical
Usage Criteria: Widespread user impact; approved by Application/Business Owner or Product Manager
When triggered: Within 30 min. after escalation to Command Center (if required)
Responsible: Recovery Manager
Tool Used: IT Communicator Agent (a custom FA application managed by BRM)
Recipients:

- User/App specific DLs
- App Dev and BU-IT Managers
- Corp Infrastructure Support teams and Managers
- Executive Management
- Executive Management (P1 only)

HDI 2017 CONFERENCE & EXPO
#HDIConf

Communication Examples

First American

FIRST AMERICAN CORPORATE IT

Alert

REPORTED ISSUE - Data Warehouse

Attention all Data Warehouse Users:

UPDATE (5:00 AM PST) : Reporting is expected to be available by 8 AM PST. Another update will be sent as new information becomes available.

Original message:
Reports will be delayed in the morning (07/04), due to an ETL processing delay..

Another notification will be sent once the reports have been started or when an ETA is available.If you have any questions, please contact Carl Brown or George Harnden.

Please contact the First American Service Desk at 1-866-462-7347 for any questions/concerns about this notice.

First American

FIRST AMERICAN CORPORATE IT

Resolved

REPORTED ISSUE - Data Warehouse

Attention all Data Warehouse Users:

RESOLVED: This issue has been resolved. If you continue to experience issues with Data Warehouse, please contact the Service Desk immediately.

UPDATE (5:00 AM PST) : Reporting is expected to be available by 8 AM PST. Another update will be sent as new information becomes available.

Original message:
Reports will be delayed in the morning (07/04), due to an ETL processing delay..

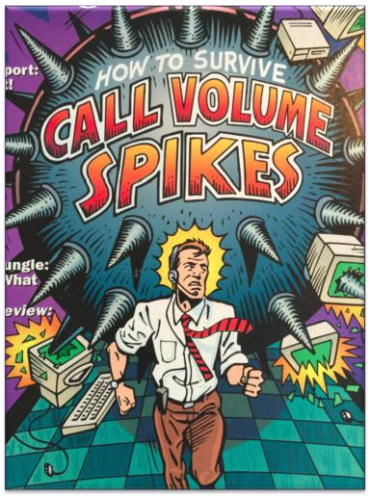
Another notification will be sent once the reports have been started or when an ETA is available. If you have any questions, please contact Carl Brown or George Harnden.

Please contact the First American Service Desk at 1-866-462-7347 for any questions/concerns about this notice.

Actions to Address

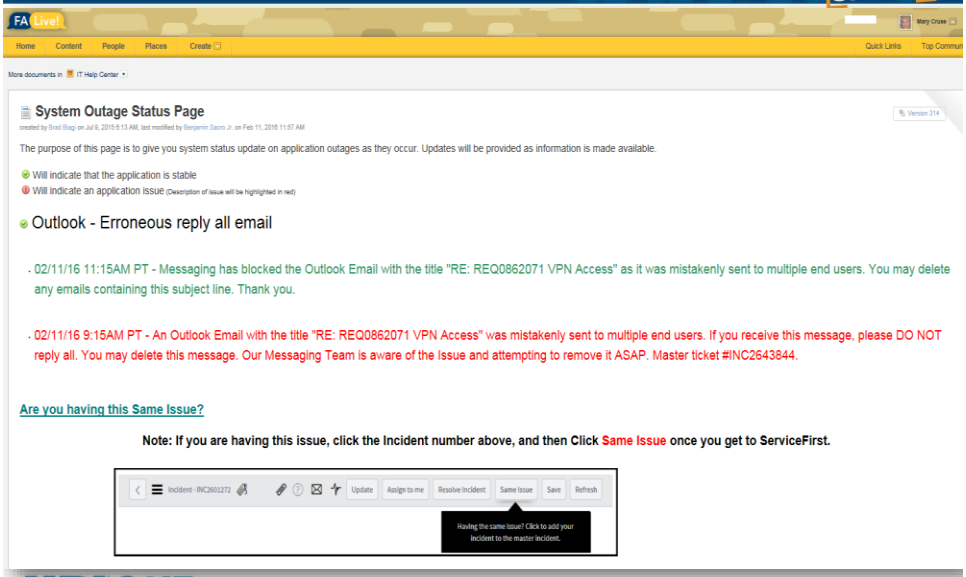
P1 and P2s will generate a substantial volume of calls all at the same time create a "Call Volume Spike."

This event increases wait time, abandons and frustrates customers on hold wanting answers.

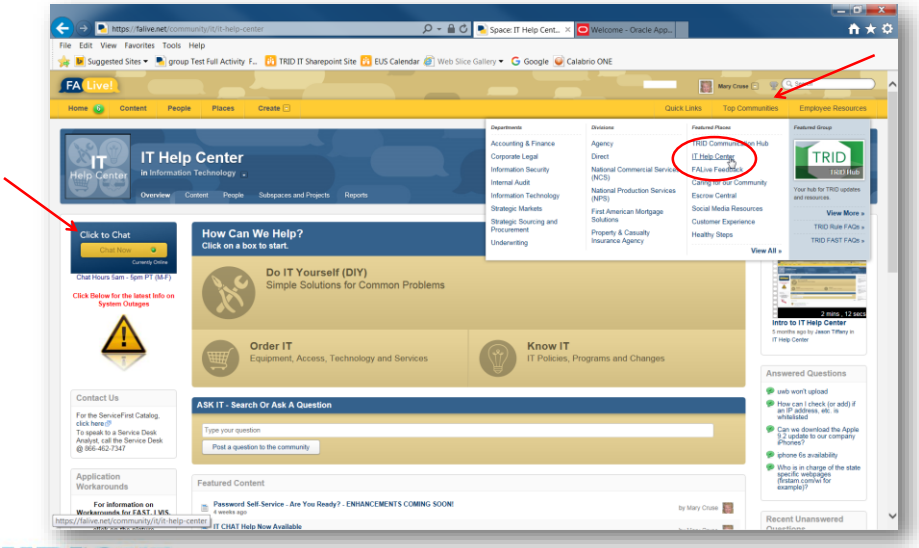


We have introduced our Self-service FALive IT Help Center Alert Page in addition to quickly recording and posting Emergency Outage (P1/P2) Greetings – Continue to play to customers already on-hold.

The ITHC IT Help Center: System Outage Page



The IT Help Center



The SD Must Champion Change

- Incidents/Problems cause Change – Change causes Incidents and Problems
- Must be represented on the Change Advisory Board (CAB)
- Must have access to the Forward Schedule Change (FSC)
- Must be able to link all incidents reported to scheduled & unscheduled (Emergency) changes in addition to Global Outages.
- Must be able to report to CAB the business impact of all changes & outages
- Service Desk must champion change and must leverage business champions to do the same.

Continuous Improvement Efforts

1. **Issue:** Bandwidth constraints - Insufficient bandwidth for Recovery Manager to manage incident communications and manage the incident restoration and bridge call.
   - **Solution:** Assign secondary Service Recovery Manager resource to manage securing additional resource(s) through xMatters, managing Lync chat, coordinating content and sending user communications, personal call to CIO for P1, etc.

2. **Issue:** Automation – the manual effort to draft the internal IT email alert, send updates and document the communication within the incident record.
   - **Solution:** Worked with Process Automation team to allow initiation of the email communication from within the incident record and have all entries contained within the incident record.

Actions to Address

3. **Issue:** Communication Content - Audiences require different level of detail depending on whether they are part of IT staff, or end user of IT services. Message recipients prefer only high level updates or a summary of the restoration efforts.

Solution: Two forms of communication used – Internal IT and End User communications.

1. Created a 'Communication standards' document that outlines what is pertinent to convey and standard verbiage to be used.
2. The final resolved update now contains a 'Resolution Summary' outlining all actions that directly led to the restoration of services.

Actions to Address

4. **Issue:** Custom Distributions & Notification methods - Some Corp and BU-IT managers only want to be in the distribution if the issue pertains to apps/systems they manage/oversee. Executive Management only wants to be notified of very business critical outages/issues (Priority 1).

Solution:

- Created an exception automation process within Service First which allows a predetermined set of recipients associated with the Reported CI to be notified of an outage/issue within their respective systems.
- Leveraged 'device threshold' functionality in xMatters to notify CIO via text and email only if Priority 1 incident
- Created a 'P1 Executive Management' template in the IT Communicator tool to be used for notifying Executive Management via email when P1 incident is opened and resolved.

Questions & Answers

Thank you!
Questions?
Don't Forget Your Surveys!

HDI 2017 CONFERENCE & EXPO

#HDIConf