APRIL
2015

Best Practices in
Major Incident Management
COMMUNICATIONS

The definitive guide to resolving critical IT Incidents fast

(x) matters

A traffic accident has prompted a 9-1-1 call to a dispatcher. Every second counts for dozens of people with an array of serious injuries who need help now. The dispatcher opens an Excel spreadsheet, finds a list of local medical professionals, and starts calling them one by one. Thirty minutes have passed before he locates a hospital admitting nurse and calls the ambulance… which has already started driving toward another hospital.

Can you imagine? Yet, when the business is on the line, many IT incident managers handle alerts in just this way: manual processes, wasted time, mass notifications to unrelated people, and the business is losing money and reputation.

IT organizations worldwide have invested billions of dollars in automating processes and making their systems better, faster and more connected. But in the moments after a major incident is discovered, when finding the right person fast is most imperative, employees run their fingers down pieces of paper, rummage through drawers, open spreadsheets, look through their email and browse SharePoint – in short, everything but relying on automated processes.

Workforces are geographically dispersed, with a mix of full-time employees and contractors. Nobody owns all the information because of myriad integrations with third-party systems. All these complexities add time to communications that would otherwise be seamless.

In this report we'll examine the challenges and best practices for automating the communication process to resolve major IT incidents as quickly and effectively as possible. But before you can even start to resolve a major incident, you must identify it.

What Is a Major Incident?

So what is a major incident in IT? With so much riding on IT, it is no longer good enough to say, "I know it when I see it." And yet, each company will have its own exact definition based on three criteria:

- **Urgency:** effect on deadlines
- **Impact:** impact to the business
- **Severity:** impact to end users

The goal in less critical incidents is to fix things according to a set of standards, but the goal in a major incident is to restore service as quickly as possible. ITIL doesn't provide a framework for major incidents, general consensus says this: IT and the business must agree on what it is.

Major Incident Management Steps

The exact process is different for every company, but when a major event occurs there are steps that are pretty universal: identify, triage, diagnose, restore, and post mortem.

In between each of these steps, someone has to hand off to the next person or group. You can think of handing off the baton in a relay race – or adding a joining piece to connect sprinkler water lines.

Most companies restore services competently enough, but small inefficiencies in communications in between can add minutes or hours that can add up to disaster. Have you ever seen a relay team drop the baton and win? A timeline, with communications in green, looks like this:

Identify: A service manager recognizes a major incident.

Engage: The service manager steps outside the regular incident process and alerts the major incident managers on duty.

Triage: The major incident manager who accepts the case determines whether the alert is a false alarm and what the incident is.

Find and Assemble: The major incident manager assembles the resolution team on a conference call. He also sends separate communications to key stakeholders including the customers, partners, and executives.

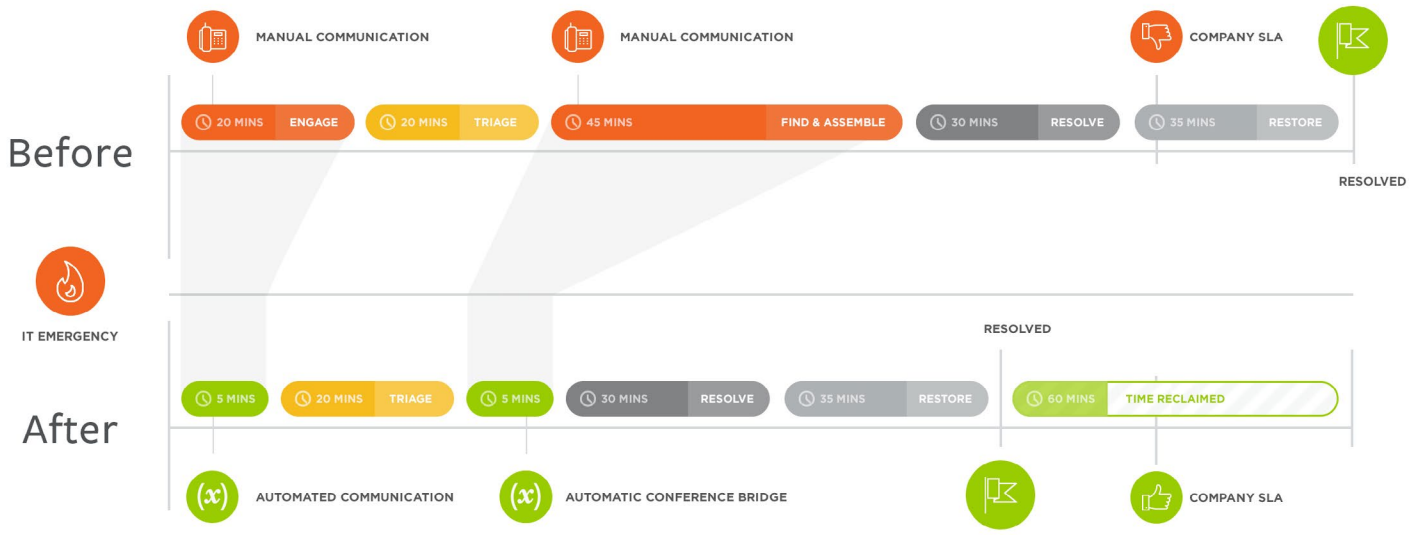
Resolve: The team diagnoses the underlying cause of the disruption and repairs it.

Post mortem: The major incident manager and SLA manager review what was done well and what wasn't, and whether to implement a true fix as well. According to The 2014 SANS Incident Response: How to Fight

Back survey (sponsored by AlienVault), 62% of respondents say they don't have enough time to practice resolution processes.

Reduce your mean time to resolve incidents

Improve SLAs and get your business back up and humming faster



Some Important Advice

When the IT worker recognizes a major incident, it's all hands on deck and a whole new process kicks in. Each company's process will be different, but here are some practices to keep in mind.

Transparency lets your resolvers resolve: Customize messages to business stakeholders in layman's terms. Otherwise they might get nervous and start asking questions, interrupting the resolution team. Often the ones trying to restore service are the same ones trying to communicate, resulting in multitasking and errors; so let the major incident manager communicate while resolvers do their thing.

Automated escalations speed notification: If a resolution team member doesn't answer the call, use automated escalations until the person answers or it automates to the next appropriate person.

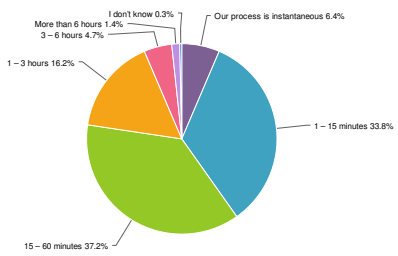
Multimodal communication targets effectively: Send messages to recipients on the right device at the right time with the right message. It gets their attention without including others. If targeted communications don't work, send an alert to resolution team members on all their devices at once. It's like sounding a targeted Code Red Emergency.

Device usability counts: Easily target groups, schedules, devices, messages, and content from any device to save time. With apologies to Sir Topham Hatt, less concise communications can cause confusion and delay.

Common Mistakes in Major Incident Management

More than 40% of businesses start to feel the impact within 15 minutes after IT goes down. But 60% of companies cannot get the right person to respond to a notification that fast. Those 15 minutes can cost a large company up to $300,000.

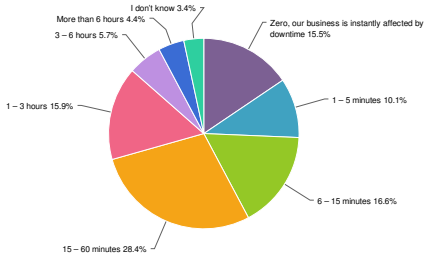
Fg. 1: When IT issues arise, approximately how long does it take to determine who the right individual is to resolve the issue, contact them, and have them respond?



Our process is instantaneous	6.4%		19
1 – 15 minutes	33.8%		100
15 – 60 minutes	37.2%		110
1 – 3 hours	16.2%		48
3 – 6 hours	4.7%		14
More than 6 hours	1.4%		4
I don't know	0.3%		1
		Total	296

Statistics	
Sum	1,840.0
Average	6.8
StdDev	6.8
Max	15.0

Fg. 2: For your company, approximately how many minutes of IT downtime can occure before the business is negatively impacted?



Zero, our business is instantly affected by downtime	15.5%		46
1 – 5 minutes	10.1%		30
6 – 15 minutes	16.6%		49
15 – 60 minutes	28.4%		84
1 – 3 hours	15.9%		47
3 – 6 hours	5.7%		17
More than 6 hours	4.4%		13
I don't know	3.4%		10
		Total	296

Statistics	
Sum	1,682.0
Average	7.4
StdDev	6.1
Max	15.0

Why does it take so long? Here are a few notable reasons.

Ineffective Channels

A large IT department can receive more than 100,000 notifications a day, ranging from innocuous updates and progress reports to maintenance updates and outage warnings. Among them may be one or more major incidents.

Email is a particularly poor notification method. IT Operations employees often use filters to screen out the noise. When they do, they can miss major incident notifications. Email can sit in inboxes for days, but people answer texts within three minutes according to VentureBeat, and respond to push apps even faster.

Mass notifications go to unnecessary people, pulling them off their primary jobs. They also involve people in meetings and on conference calls, where they delay resolution processes. They may also spread confidential information beyond the inner circle of executives and resolution team members, increasing risk of an information leak.

Overused distribution lists often guarantee that the wrong people will get the message, and many of the right people won't.

Manual escalation processes waste time as service desk managers scour multiple spreadsheets, intranets, and personal and work emails for contact information. Centralizing contact information into one system is a huge time saver.

Ad hoc notifications occur when dispatchers go outside the Major Incident process. They ask friends in the office to help. But their friends drop their primary duties to step in, and they can duplicate activities with the resolution team.

Best Practices in Major Incident Management

Going back to our dispatcher, calling one person after another is really just scrambling. Resolving major incidents quickly requires a consistent process for communicating to resolvers and stakeholders alike.

Let's walk through the communication steps that connect the major incident resolution process.

A CAUTIONARY TALE

Recently, a major U.S. retailer announced that it had suffered a data breach. Its security software had detected the attack and sent an alert five months earlier, but IT employees had missed them among the deluge of notifications flooding their inbox every day. Shane Shook, an executive with Cylance Inc., told Reuters the overwhelming volume of notifications makes a major incident virtually inevitable for large IT departments. "They are bombarded with alerts," he said. "They get so many that they just don't respond to everything. It is completely understandable how this happened."

A less critical incident will erode into a major incident if left unchecked

Identify

The hallmark of a major incident is service disruption. In most cases a service desk manager identifies a major incident and escalates to a major incident manager, but some companies automate the routing of major incidents. Have resolution processes for less critical issues as well, so they don't go to major incident managers unnecessarily.

Engage

Assuming the notification is not automatically routed to a major incident manager, the service desk manager finds a major incident manager. Instead of rifling through spreadsheets or sending emails to the entire IT team, the service manager should take advantage of communication technology.

The communication system should already have the major incident managers with their contact information and on-call schedules prepopulated, enabling the service manager to instantly locate available major incident managers and target notifications to them.

Automating this initial engagement can have huge benefits, reducing a lengthy process by up to 90 percent.

Triage

The major incident manager who accepts the case determines whether the alert is a false alarm and what the incident is. The 2014 SANS survey (sponsored by AlienVault) reveals that 15% of organizations have issues with false positives.

Find and Assemble

Once the major incident manager understands the nature of the incident, he assembles the appropriate team members from the pool of IT and service personnel. The first step is choosing team members based on the skills required to restore service.

Unique messages have more impact

When IT starts to craft the message around what's happening, Marketing and PR can take those messages and communicate responsibly to the media. Executives can communicate effectively and consistently as the face of the company. But you have to enable them.

Getting ahead of the spin is crucial because the company's reputation is at stake. Pay attention to mitigating damages that don't show up on the balance sheet right away. Eventually, things like reputation and trust find their way to the bottom line.

More than half of the victims impacted by a data breach report that notification from the company was both late and unclear. Is it any wonder that net earnings, stock price, and reputation suffer?

Major incident management resolution team

There is no one major incident process for all companies, but a good practice is keeping a small group of major incident managers who manage the process and post mortem based on on-call schedule rotation. When a major incident occurs, the service desk manager finds a major incident manager to run the resolution process. The major incident manager chooses the resolution team members based on the required skills.

Major incident manager: Manages the incident resolution process, ensuring that the team has the resources it needs, and runs the post mortem after resolution. Another option is to use a duty manager to manage major incidents. A duty

manager is selected from the on-call IT team to manage restoration, while a major incident manager comes from the business side.

Other common roles include:

Service desk manager: Stands on the front lines keeping incident records up to date and taking the lead on customer communications

SLA manager: Keeps track of total downtime, and tracks milestones including time to notify and time to resolve

Change manager: Implements fundamental changes to prevent recurrences of the disruption after service is restored

Problem manager: Determines the root cause of the incident, working independently from the incident resolution team to help the change manager

Some companies choose to have a SWAT team at the ready, instead of making sure someone from each required department can free himself to help. By establishing separate incident management processes for less critical incidents, IT departments can automate escalations.

Things to keep in mind

When members of the incident resolution team receive notification, they drop everything else.

Top priority: Each member must know that a major incident is top priority. Team members must leave meetings, ditch lunches, and close whatever they're working on.

On-call schedules: Centralized on-call schedules make all team members accountable for keeping their schedules up-to-date, as accurate schedules make faster conference bridges.

> Whatever your company's definition of a major incident, general consensus says that IT and the business must agree on it.

Conference bridge technology

Just assembling people and initiating the conference call can take 20-45 minutes. Companies that use mass communications during this phase often get way too many people on the conference bridge. Each new person that joins interrupts the flow of the call. Repeating the background information for each person can waste an additional 10 minutes.

With a leading communication platform, the major incident manager can customize the message so resolution team members understand the basics before the call, and can join the bridge with just a button push instead of having to dial in.

Resolve

Members of the major incident team use all available communication channels integrated with their communication platform, including chat, text, email, phone, Skype, Slack, and more to identify and resolve the underlying cause of the issue.

The communications also enable the major incident manager to keep stakeholders up to date and let his team members resolve.

Restore

Once the underlying issue is resolved, the team members can restore service and end the incident.

Post Mortem

A review is a fundamental piece of the incident resolution process, and all relevant parties should attend. The major incident manager and the problem manager should walk the group through the incident record, so they can assess the resolution process together.

The review can also identify improvements that can prevent a similar incident from occurring again.

Customize messages

Customizing notification messages gives resolution team members a head start before they join the conference bridge. These messages can often be technical in nature, using IT jargon and specific server names.

Customizing a more business-friendly message enables Marketing, PR, and executives to communicate responsibly, effectively and consistently.

Templatized but editable notifications: Different stakeholders require different levels of information, so give your service desk manager the ability to tweak the message for different groups.

Offer Subscriptions: Give stakeholders the ability to subscribe to some alerts and unsubscribe from others so they get just the information they need.

Conclusion

Your data, information and processes are your business. When they become compromised, your business can suffer irreparable damage. So when major incidents occur, how you manage the communication is everything. Identify the members of an incident resolution team and centralize on-call schedules. Share processes, follow them, and lead your company through to resolution.

Contacts

CORPORATE HEADQUARTERS
12647 Alcosta Blvd., Suite 425 San Ramon,
CA 94583 USA | +1 877.XMATTRS (962.8877)

EMEA HEADQUARTERS
20 Little Britain
London, EC1A 7DH UK | +44 (0) 203 427 6326

APJ HEADQUARTERS
Level 29 Chifley Tower, 2 Chifley Square,
Sydney, NSW 2000 AU | +61 2 9238 8023

About Us

xMatters' cloud-based solutions enable any business process or application to trigger two-way communications (text, voice, email, etc.) throughout the extended enterprise during time-sensitive events. With over a decade of experience in rapid communication, xMatters serves more than 1,000 leading global firms to ensure business operations run smoothly and effectively during incidents such as IT failures, product recalls, natural disasters, dynamic staffing, service outages, medical emergencies and supply-chain disruption. xMatters is headquartered in San Ramon, CA with additional offices in London and Sydney.