everbridge
IT ALERTING

Streamlining the Major Incident Resolution Process:

Define, Plan, Staff and Communicate

everbridge
IT ALERTING

Streamlining the Major Incident Resolution Process: Define, Plan, Staff and Communicate

When a major IT incident occurs, planning and proper role delegation is essential for quick resolution. For every minute of system downtime, there are severe effects on the business: angry end users/customer, a reduction in employee productivity, frustrated executives, and sometimes even impacted revenue – and for hospitals, it can affect patient safety. Not only should IT teams strive to resolve the major issue as quickly as possible, they need to make sure they communicate with key stakeholders to prevent confusion and ease concern. In this white paper we offer simple recommendations on planning, resource identification and communications to help streamline the major incident resolution process and limit the negative impacts of major IT incidents on the business.

Incident Management Basics

It is important that we first mention the overall incident management process that IT teams typically follow for swift resolution. ITIL outlines a structured workflow that encourages efficiency and best results for both IT teams and customers:[1]

1. **Incident identification** – When a user reports an incident via email, support call, network monitoring software etc., the service desk must decide if the issue is truly an incident or if it's a service request. Identification is first step in the life of an incident – a service request would set off a completely different process known as a service request fulfillment.

2. **Incident logging** – After the service desk has properly identified an incident, a ticket is logged and includes information important to the case - user's name and contact information, the incident description, details, and the date and time of occurance.

3. **Incident categorization** – The service desk must then assign a category and at least one subcategory to each different incident. For example, an incident could be categorized as "hardware" with a sub-category of "hardware failure." Categorization of incidents serves three different purposes:
   - Provides a way for the service desk to sort and model incidents
   - Allows for some automatic prioritization
   - Offers accurate incident tracking

4. **Incident prioritization** – An incident is then prioritized based on the details of the incident - its urgency and impact. First, how urgent is this issue? How quickly is the resolution required? Second, what is the impact? Or in other words, what is the extent of the incident and of the potential damage caused before the issue can be resolved? An incident can be classified as a low-priority, medium-priority or high-priority incident and each priority level requires a different level of response. We will revisit this topic later in the white paper.

5. **Incident response** – Once an incident is identified, categorized, and prioritized it is time for the service desk to coordinate resolution. This entails the initial diagnosis, escalation, investigation and diagnosis, recovery, and closure. After the incident is resolved, IT teams should also perform a root cause analysis and implement changes based on findings. Changes should be approved by the Change Advisory Board and adopted as major incident response protocol. All incidents should be documented, analyzed and evaluated in order to identify areas for improvement and to help with future incident response.

Major Incident Response

The standard process for incident resolution highlighted above in step 5 can be applied to most low-priority IT incidents. But what happens when a high-priority incident strikes? As previously mentioned, major IT incidents have significant impact on the business and in order to limit the effects on stakeholders, end-users/customers, employee productivity and revenue, it is important to get the right people working on the issue as quickly as possible. Simon Morris, author for the ITSM Review, describes his experience with the way IT teams handle major incidents:

> ***I actually found that in some cases all process and procedure went out of the window during a major incident, which has a horrible irony about it. Logically it would seem that this is the time that applying more process to the situation would help…I could see people pushing back against the idea of breaking out the process-book because all that mattered was finding the technical fix and getting the storage back up and running.*** – Simon Morris, ITSM Review

What steps can you take to avoid wasting time and streamline the major incident resolution process? Below are four recommendations.

1. **Define a critical incident and map it to the overall incident prioritization system.**

   According to 20000 Academy author Neven Zitek, a major incident is "a highest-impact, highest-urgency incident affecting a large number of users, depriving the business of one or more crucial services."[4] Zitek also mentions that according to ITIL, the definition of a major incident must be agreed upon by the business.[4]

   Each organization is different and will experience IT incidents with different levels of urgency and impact. But, once the definition of a major incident is agreed on, it should "be mapped on the overall incident prioritization system – such that it can be dealt with through the major incident process."[2]

2. Define a clear and separate incident response process for critical incident resolution

Companies have had to adopt procedures and best practices for major incident resolution separate from those used in standard incident resolution. ITIL suggests a brief but helpful way to approach major incident planning, noting that once a definition of a major incident is agreed upon and mapped to the prioritization system, "a separate procedure, with shorter timescales and greater urgency, must be used for 'major' incidents."[2]

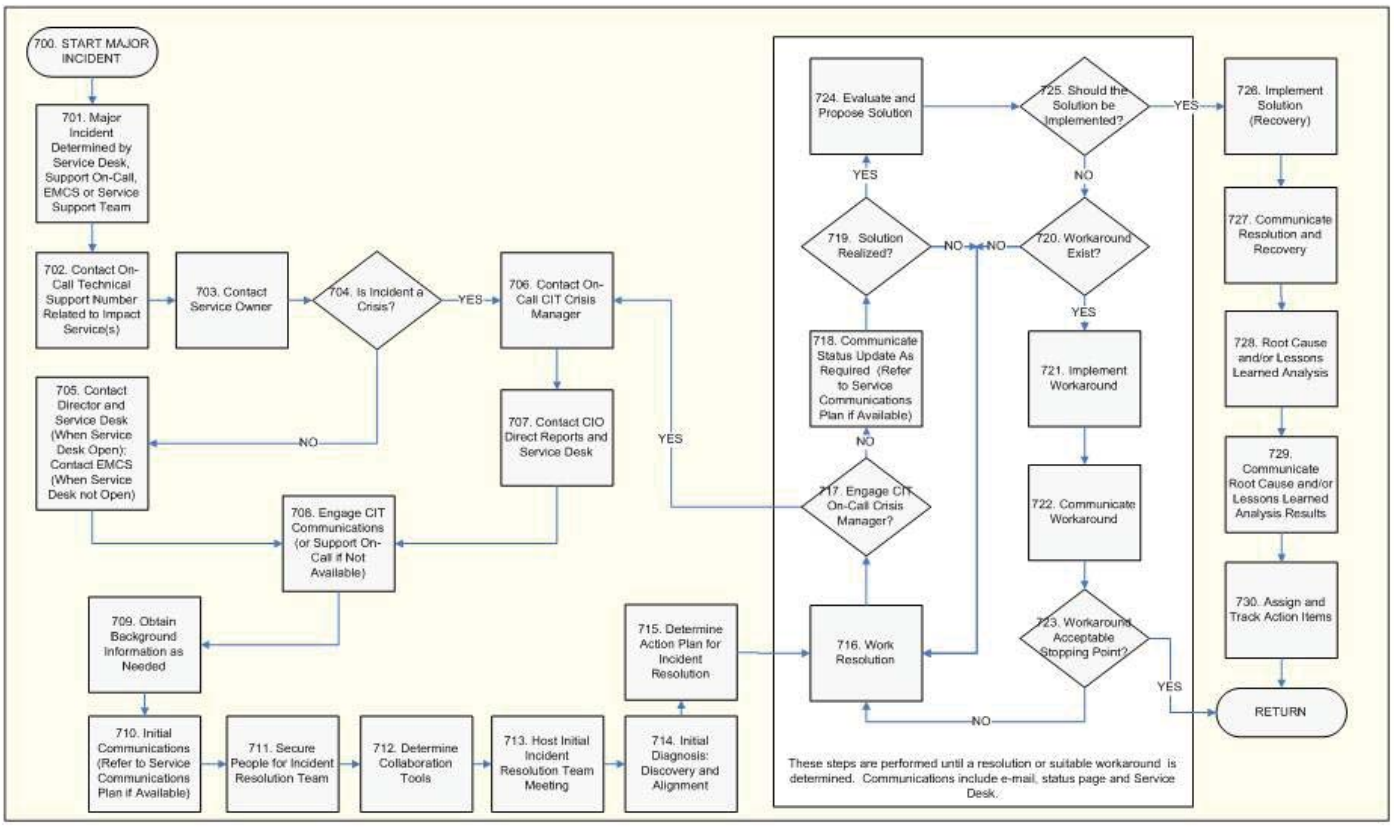
This separate procedure should be simple and automated. Information Age cites 7 areas for IT teams to focus on when simplifying and automating the major incident resolution process, saving valuable time:[5]

1. Identifying the major incident (as highlighted in recommendation 1)
2. Communicating with the impacted staff or business stakeholders
3. Assigning the right people
4. Tracking the major incident throughout its lifecycle
5. Escalation upon breach of SLAs
6. Resolution and closure
7. Generation and analysis of reports

Information Age also suggest that in the case of major incidents, IT teams should "adopt a no-approval process for solving major incidents."[5] Typically, resolution plans need to be blessed by upper management and executive level staff but when time is of the essence, the approval process may hinder progress in a way that adds to the negative impact on the business.

Below is an example diagram from IT@Cornell appropriately titled the Central IT Major Incident Procedure.[6] The diagram maps the major incident resolution process within the organization. Although each major incident is going to present a different set of challenges, having a major incident plan and process in place saves time in the long run and helps limit the negative impact for any business.

Example Map of Cornell University's Incident Resolution Process



Source: https://confluence.cornell.edu/display/itsmp/Central+IT+Major+Incident+Procedure

3. Identify the adequate resources and establish focus/priority level

Whether your organization has a dedicated incident resolution team headed by an incident manager or an ad hoc team of subject matter experts from various departments, the best resource for the job should be working to solve the problem. Each member of the team should be trained on the major incident process and should know their role. The table on the next page displays a roles and responsibilities chart from IT@Cornell:[6]

everbridge
IT ALERTING

Role	Main Activity
CIO	Being informed of major incidents, may elect to engage a crisis manager.
Crisis Manager	Manages crisis resolution and recovery, crisis communications.
EMCS (Energy Management and Control System)	Responsible for certain operational monitoring of CIT services from 6 PM to 6 AM weekdays and all day on weekends and holidays.
Incident Manager	Manages incident resolution and recovery, engage CIT communications; provide information for communications, may elect to engage a crisis manager.
IRT (Incident Resolution Team)	Perform an initial investigation and diagnosis, identify any new problem(s), resolve the incident and recover the service.
IT Service Provider	Responsible for providing value to customers in the form of services.
Service Desk	Manages incidents and service requests and handles communication with the users, the service desk "owns" any incident or request management tickets, responsible for certain operational monitoring of CIT services from 6 AM to 6 PM weekdays, excluding holidays.
Service Owner	Act in the capacity of incident manager.
SST (Service Support Team)	Provide support for incident resolution, may form part of an incident resolution team.
Support On-Call	Engage CIT Communications if the service owner has not, send communications only if CIT communications is not available, if no other options are available, assist Service Owners in securing people for the Incident Resolution Team.

While the previous table is just an example of different roles and responsibilities involved in Cornell University's Central IT Major Incident Procedure, a strict designation of who is responsible for what helps to streamline the resolution process for any organization. Depending on the size of the IT team and scope of its service management, roles and responsibilities will differ.

> ***Smaller organizations will tend to aggregate a few roles into one job definition, while larger organizations will elaborate sub-roles for each major incident type, customer or technical expertise field.*** – 20000 Academy

3. Communication is Key – Get Resources Working on the Issue as Quickly as Possible and Keep Relevant People Informed

Communication throughout the various stages of the major incident lifecycle is fundamental in streamlining the resolution process. First, as stated in recommendation three, the proper resources need to work on restoration but that is only half of it – they need to begin the process as quickly as possible. But what if the team is dispersed across the building, the state, or even the country? What if certain team members use email while others are more likely to response to text? When a major incident occurs, a communication method that quickly connects the right on-call IT personnel with the right information allows for quicker collaboration and therefore, faster resolution. IT teams should be armed with a proper communication tool that allows facilitates this quick collaboration.

Senior management must also be made aware of the IT incident so they can take the appropriate business actions. Critical incidents might bring about procedure changes, resource reallocation and priority shifts. Senior management will sometimes need to act quickly to implement policy changes in order to limit the business impact of major IT incidents. The faster senior management is informed of the major incident, the faster they can make the proper business decisions.

To even better streamline the resolution process, customer communication cannot be neglected. Often times, the customer is omitted from the communication loop which has potential to create more back-log and overwhelm the service desk. Timely announcements, notifications and status updates should be sent to all relevant stakeholders, including customers, on a regular cadence that will help alleviate confusion and concern. Information Age suggests having a "dedicated line to respond to major incidents immediately and offer support to stakeholders" and using "the fastest means of communication, such as telephone calls, direct walk-ins, live chat, and remote control desktop, instead of relying on email."[5]

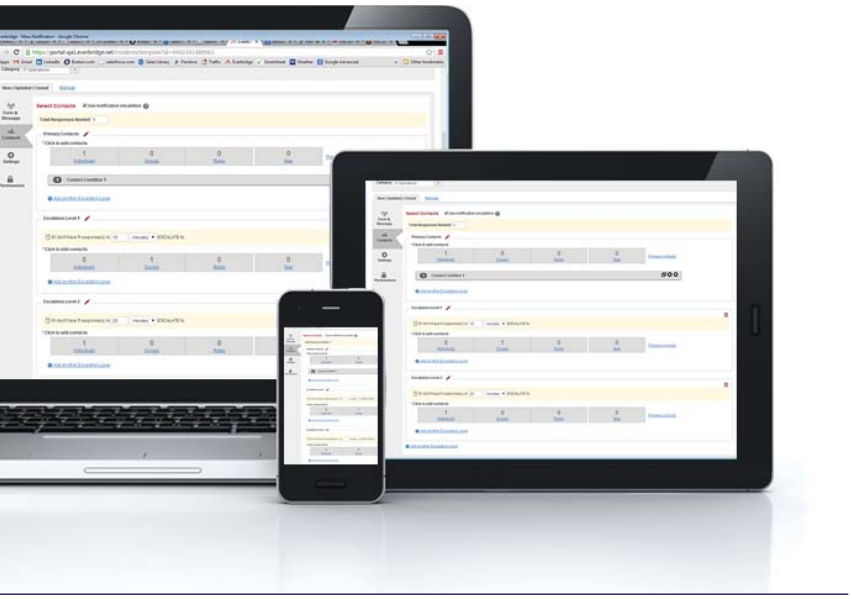
everbridge
IT ALERTING

Optimizing Communications

What most companies do not recognize is that communication during the resolution process has the potential to save quite a bit of money. Companies tend to see a huge return on their investment when they have a communication plan in place and a communication tool that allows IT teams to collaborate and keep stakeholders up to date.

Everbridge IT Alerting helps IT teams streamline and automate the way IT teams communicate during major IT incidents, in turn streamlining the resolution process. Everbridge's cloud-based solution ensures that IT teams can quickly notify and communicate with their key members during major service disruptions when every minute counts. IT Alerting provides automated intelligent notifications, automatic escalation of alerts, on-call scheduling, mobile alerting, self-service mobile app and integrates with ITSM platforms, including ServiceNow and BMC Remedy. The solution connects the right on-call personnel with the right information, so they can hop on a conference bridge quickly and fully focus on restoring service and limiting the negative impact of incidents on end-user satisfaction and even revenue.

To learn more about streamlining your critical incident resolution process with Everbridge IT Alerting visit www.ITalerting.com.



Refrences

1. http://www.bmc.com/guides/itil-incident-management.html
2. http://www.theitsmreview.com/2012/02/planning-major-incidents/
3. http://www.itskeptic.org/content/what-itsm-major-incident-itil-doesnt-say
4. http://advisera.com/20000academy/knowledgebase/major-incident-management-going-gets-tough/
5. http://www.information-age.com/it-management/risk-and-compliance/123460139/dont-panic-10-ways-manage-major-it-incidents
6. https://confluence.cornell.edu/display/itsmp/Central+IT+Major+Incident+Procedure