Best Practices
for Faster Critical IT Incident Response

By automating communications, you can significantly improve your speed and quality, resulting in significantly faster Mean Time To Resolution (MTTR) — the key metric when it comes to restoring mission-critical business functions.

CIO INSIGHT

IT administrators don't need to be told that critical incident management is a hot issue. They get impassioned input on the subject from users, upper management, and even customers every time an incident occurs. And as businesses become more dependent on IT and applications become more complex and interdependent, incidents are more prevalent and more costly than ever. As a result, faster incident resolution has become an imperative.

A close analysis of the critical IT incident resolution process reveals that it has four key components:

1. Identification: Becoming aware that the problem exists, either through automated notification or user input

2. "Knowing," or Diagnosis: Determining what the incident is and getting the right resources together to address the incident

3. Fixing: Taking the necessary actions to resolve the problem.

4. Verification: Determining that the problem is resolved not only from a technical perspective, but also making sure that the business issue is solved— so that users can go back to work, the customers can again make online purchases, and so on.

Better Communication for Faster Resolution

All of these components — in particularly diagnosis — are dependent on fast, reliable communication among the parties involved. By automating communications, you can significantly improve your speed and quality, resulting in significantly faster Mean Time To Resolution (MTTR) — the key metric when it comes to restoring mission-critical business functions. This is how it works:

When a service desk receives an alert from a monitoring tool or a call comes in to a help desk from a user or department manager, the first step is to try to solve the problem locally. If that proves impossible, critical incidents are usually escalated to the team tasked with finding the quickest and safest way to restore normal operations. By that time, the affected users, partners, or customers have already become annoyed, if not exasperated. It's the critical incident response team's problem to locate an expert who can address the problem. That's where automation can make a huge difference.

Companies that automate the IT alerting process would have collected information concerning on-call individuals' areas of expertise as well as their availability, i.e., *when* they are scheduled to be on call. Information is also collected on how these experts prefer to be contacted. If desired, this information can be linked to the HR organization to ensure that experts' contact information is always up to date, and that new hires are put on the roster and individuals who have left the company are deleted.

When an incident occurs, you can identify the right expert instantly, based on the type of incident, the time of day and even physical proximity, with no need to hunt through spreadsheets or rely on sticky notes attached to the service desk console.

Once the appropriate expert has been identified, the next step is contacting that individual. Best practices for automating communication processes means supporting a variety of modes for sending notifications on a global basis: email, telephone, texting via SMS, pager, or push notifications. If the targeted individual or group doesn't respond, escalation should be automatic based on pre-determined business rules.

In addition to automating the delivery of notifications, you should also support two-way communication. This means that experts who have received a notification can easily respond, verify to the incident response team that they're working the problem and share initial impressions.

The Benefits of Automation with Everbridge IT Alerting

By automating the communication processes associated with incident management, Everbridge IT Alerting delivers tangible benefits that are extremely important in a crisis.

• **Faster mobilization.** IT Alerting gets notifications to the right people in a matter of seconds, eliminating all unnecessary delays. Furthermore, managers can track communications to make sure no one has failed to receive an important message.

"Best practices for automating communication processes means supporting a variety of modes for sending notifications on a global basis..."

• **Faster MTTR.** The mechanics of communication play a huge role in determining how fast problems get solved. Quite simply, more efficient communication equals faster MTTR.

• **ROI.** It goes without saying that IT outages cost money, and this can be quantified with relative ease. For example, if an engineering team can't work, the cost is the number of working hours lost times the fully burdened hourly wage of each engineer, i.e., salary plus benefits, taxes, and other costs. When an e-commerce site is down, the cost of lost revenue can be calculated based on average sales for comparable time periods. For example, downtime during the evening might have a greater or lesser impact than downtime during the day. But whenever an incident occurs, IT Alerting can reduce its financial impact.

• **Post-incident analysis.** Because IT Alerting tracks every communication, it enables managers to review how incidents were handled after the fact via customized reports, and gather information that will enable improved performance in the future.

Beyond Single Individuals

As anyone who has ever worked in a data center knows, one single individual can't always resolve a critical IT issue. To simplify collaboration, IT Alerting includes built-in conferencing. Team members can join live conference calls with a single touch, avoiding the time-wasting hassles associated with setting up a call, notifying the people involved, providing dial-in and ID information and so on.

While the focus of incident management is obviously to resolve the problem as quickly as possible, the affected individuals shouldn't be kept in the dark. To facilitate informing them, Everbridge also provides solutions for

users that can scale to thousands of individuals within an enterprise, agency or university community.

A Hosted Solution

The fact that IT Alerting is a SaaS solution has significant benefits for IT organizations of all sizes. Some of them are common to all hosted solutions. There are no installation headaches, no infrastructure maintenance costs, no need to deal with hardware upgrades, no capital expenditures (CAPEX). Also, no special training for the IT staff is required. With IT Alerting, implementation can be further facilitated via the use of sample templates for various scenarios that are available to help organizations quickly create their own policies.

Everbridge has made a significant investment in its unified critical communications platform and infrastructure that would be difficult for most companies to match, and has developed relationships around the world with telecom providers to facilitate quick communication via multiple modes.

With this infrastructure, IT Alerting can not only automate communication within the IT organization. It can also automate communication to key internal stakeholders and customers as well. This use of IT Alerting can help reassure all concerned that the problem is being handled, and can also help cut down on incoming calls that distract the team from its problem-solving tasks and can help alleviate, if not avoid, heavy burdens on call centers.

Conclusion

Critical IT incidents aren't an everyday occurrence, but when they occur they can have a disastrous effect on business processes, and even a company's very ability to function. By identifying, connecting, and coordinating the people who can fix these problems, IT Alerting minimizes downtime and its costs while enabling the IT organization to come through in difficult situations. ■

Note: This paper is part of a series on how companies can speed problem resolution in IT incidents through automated communications.