Critical IT Incident Management Best Practices:

*IT Experts on Communication and Collaboration*
The Impact of IT Incidents and Disasters

When an IT incident causes system downtime and service disruptions, your organization will feel the impact—even more so when the issue isn’t solved in a timely manner. These interruptions can lead to unhappy customers, a damaged reputation, and even lost revenue. Through IT incident response and team collaboration, you can reduce your mean time to repair and limit the impact that downtime, service disruptions, and other incidents have on your organization. Quick and accurate response information is expected by customers, which is why IT alerting and incident response is critical for organizations.

When system downtime and service disruptions occur, your customers expect quick and accurate response information and a solution as soon as possible. This means your organization should strive to improve your mean time to resolve or to repair. Perhaps the biggest opportunity to improve this area is to also reduce your mean time to know, because if you don’t know about an incident quickly then you can’t repair it quickly. The first step is to identify that there is a problem, followed by making sure the appropriate people are informed of the issue, which can be improved through IT alerting. This is critical to complete before fixing, clarifying, and validating the problem.

What’s in Your Mean Time to Repair (MTTR)?

One of the common metrics used for measuring IT incident management effectiveness is MTTR, defined as Mean Time to Repair (also referred to as Mean Time to Resolution or Mean Time to Restore). In a recent Everbridge survey, IT Operations professionals ranked “Time-to-Repair Mission Critical Systems” as one of their top three challenges.¹ How can organizations reduce MTTR? Forrester Research’s Stephanie Balaouras, Vice President & Research Director, Security & Risk, further breaks down MTTR as the sum of four distinct parts:

- **Mean Time to Identify (MTTI):** The time it takes to detect an incident
- **Mean Time to Know (MTTK):** The time it takes to identify the root cause
- **Mean Time to Fix (MTTF):** The time it takes to implement the fix
- **Mean Time to Verify (MTTV):** The time it takes to verify that the fix is working²

---

This second category, MTTK, is one that warrants some additional scrutiny. In MTTK, we ask, “What’s wrong? Who’s affected? Who needs to be involved? What needs to be communicated?” As corporate IT ecosystems, including applications, services, and infrastructure, become more complex, the MTTK process in particular becomes more difficult. In fact, for many incidents, this is the area where IT management teams spend the bulk of their time. Within MTTK are the processes of identifying and communicating with experts, escalation to ensure that the issue is being addressed, collaboration between cross-functional groups, and communication with customers, partners, and stakeholders.

**Managing Critical IT Incidents vs. Routine IT Incidents**

ITIL (Information Technology Infrastructure Library) describes IT incident priority as being a combination of two factors—impact and urgency. Impact is often measured by the number of users affected, but when the incident directly affects a customer(s), it can often be qualified as a major incident regardless of the number of users involved. If the nature of the incident either violates your customer agreement, or somehow impedes your customer’s success, not solving it quickly could have a bearing on your organization. “For us, [when customers are involved,] we are escalating immediately; we are communicating internally, and we’re communicating externally as quickly as possible,” explains John O’Keefe, Senior Director of Operations at Acquia, a software company providing products, services, and technical support for the open source CRM product Drupal.

In addition, while you may not change your incident management process for an incident that impacts your customers, you may change your communication process, and the roles involved in incident resolution.

“Severity, really for us, is just going to change how widespread we need to communicate and what teams we need to pull in,” O’Keefe explains. “If we have something that is affecting the platform, we’re going to pull our engineering team. If it’s a customer-specific application, we’re going to pull in our customer support team, and potentially our professional services organization.”

Bob Pick, VP & CTO and CISO for TMNA Services, LLC, a member of the global Tokio Marine Group, agrees, explaining that when dealing with critical incidents versus routine operational incidents, “the key differentiator in that process is not the process itself, it’s the breadth of communication, and then it’s how high it needs to either be escalated for decision making purposes, or escalated for informational purposes.”

---

While major incidents may require exceptions, O’Keefe recommends standardizing how you respond to incidents, so that you’re not determining process on the fly. With a plan in place, you can begin fixing the problem as soon as possible.

Many organizations invest heavily in mapping out process and communications for incident management. However, when a P1/Sev1 incident occurs, standard procedure is not always followed because the outage is “critical.”

**Reducing MTTK through Communication**

When a critical IT incident occurs, your goal should be to resolve it as quickly as possible—the shorter your MTTR, the better. So how do you reduce MTTR?

O’Keefe harkens back to the Forrester definition of MTTR and its four components. He says that what you really need to attack is your Mean Time to Know (MTTK). While O’Keefe stresses that a major part of improving MTTK is speeding up communication and collaboration, he cautions that this doesn’t just mean you should send out an alert as quickly as possible; you should send an alert that is specific and offers guidance as soon as you are able. In the IT space, alert fatigue is common, as there are many false alarms sent out. This is why you want to make sure your first message has meaningful information. If you send out too many false alarms, critical personnel could end up ignoring an alert that is actually real.

Application-centric incident monitoring is also critical. Your monitoring, alerting, and escalation systems all need to have an innate understanding of your application functions. This can help eliminate the delay that human response may create by creating a swifter and targeted automated response, which, in turn, can reduce your mean time to repair. O’Keefe says it is important to spend the majority of your time fixing the issue, not getting the information out—by improving the communication process, you reduce the bandwidth it requires.

In the midst of an IT incident, a lot of information must be transmitted between essential parties to address and resolve the problem. This is why it is important to provide as much critical information upfront as possible, so anything that isn’t needed to repair an issue can be ignored.

“The more information that can be provided and enriched into that automated decision making, or that lower level decision making, before it reaches an engineering level or a customer service level, the better,” said Pick.
Branko Miskov, Director of Product Management, BlueCat Networks, says having as many pieces of the puzzle as possible upfront allows you to make a meaningful, informed decision. Having this information from the start makes it much easier to resolve a problem, reducing your mean time to repair.

**Automate, Automate, Automate…but Don’t Forget Human Interaction**

Automation helps improve IT alerting and incident management, by discovering information upfront for a more meaningful response. However, Pick says that unless we’re able to get to a point of perfect code that is relatively unchanged, always thoroughly documented, with infrastructure that never needs to be upgraded, then human intervention will likely be necessary. “But the reality is that the technology landscape in any company, every company, is constantly changing,” adds Pick, “even though it may only be changing in very subtle ways.”

Miskov adds, “Part of the challenge is this idea of automating the routine things, the things that you know, and then being able to focus your energies on the harder problems and make those exceptions.” He explains, “There’s things that [customers] do, routine things that come in, and I think those types of processes can be automated.”

The exceptions to routine processes are important, says Pick. For routine processes, “we follow the decision tree that's been laid out and we use the tools at hand.” But when you get to a certain level of criticality, or business impact, “that's where there is human decision-making that comes into play.”

O'Keefe agrees: “I do have a fair degree of optimism that while we’re not going to get to 100% automation, we’re going to get very, very close.” But with change occurring all the time in the IT world, O'Keefe said you need to make sure both your automated processes and your human resources are fully prepared. “Those are things that you never can take your eye off of. That needs to be something you think about every day, every week, every month: ’Okay, change is coming, change has already come,’” he says. “Let’s make sure that everything I’ve ever done before is still relevant and is only becoming better.”

There are many routine issues that come up on a daily basis, and automating the resolution of these problems can save time and frustration. In the real world, there are too many variables to automate everything, but some level of automation is extremely beneficial. You still need to be able to get to the right person with the right information, because ultimately human beings will be needed somewhere along the line.
Mobility Trends Impact the Way You Address IT Incidents

In the past decade, mobility has transformed the way that employees around the world do their jobs. Enabled by mobile devices, more people are working from home—a 79 percent increase was seen between 2005 and 2012, according to the American Community Survey\(^4\). Mobile devices are increasingly making their way into all aspects of the workforce. In fact, with “Bring Your Own Device Policies (BYOD)”, many companies allow employees to use personal smartphones and tablets for work purposes.

These mobility trends should impact the way you handle IT incidents. “The types of communication people use these days are completely different,” says Miskov, “Depending on where you are during your day, and what you’re doing, it’s completely different as well. People will pull out their phone in the morning and check messages, on the way to work, they might have taken the train in, so they might use a tablet, and then use a laptop [when they get to the office], and then their mobile on the way home and for the rest of the evening.” This mobility and diversity of devices needs to be taken into account by IT departments when dealing with IT incidents and alerting. For example, you may be able to best reach someone on a different medium in the morning as compared to the evening. At certain times of the day, people might be more responsive to an SMS message than an email. This is an extremely important factor for IT alerting, because the speed with which you are able to reach people can impact your MTTR.

The consistent connection to mobile devices could also contribute to alert fatigue, says O’Keefe. For this reason, it is important that the alerts you send out about critical incidents are targeted and highly relevant. “You want to be providing people with meaningful information, but not flooding them with it, so that they’re not looking at a dashboard on their five inch screen, assuming you’re using one of the larger cell phones, and it’s a meaningless jumble of reds and yellows and green,” O’Keefe says. If you overdo it with alerts, the one that is ignored could be the message that people need to see in order to keep them informed and resolve the situation.

Mobility has many benefits, including the ability to help mitigate risk. However, it is critical to remember that it needs to be used correctly, and it if isn’t, you could be led into a false sense of security.

“I think [mobility is] very powerful, and it absolutely can help manage a significant amount of risk, but there are a couple check boxes that need to be ticked off before you can actually say it really does, in fact, manage your risk,” says Pick.

The Importance of System Resiliency to IT Incident Management

In an IT environment, some incidents are inevitable, and at many organizations, routine incidents occur on a daily basis. In addition to automating response processes to resolve incidents quickly, you should make sure that your infrastructure and applications are resilient and resistant to disruption in the first place. “There are things that are bound to happen, that we as IT professionals understand,” says Pick. “They’re just going to bite you every now and again, but with [resilient architectures] they can do so and not cause a material impact to service delivery to business.”

This is especially critical for infrastructure and applications that support customer functions. “There’s nothing more frustrating than a customer calling up and saying, ‘Oh, I have this issue,’ and then the support person replying, ‘Oh, that’s a common one,’ said Miskov. “Put the preventative measures up front,” he says, “so that when you do get an issue, it’s one that’s a lot more meaningful and one that you know you need to prioritize.”

With a resilient system in place, you can cut out a lot of noise, and IT alerting becomes more meaningful, as issues are of higher importance. With proactive measures in place to prevent issues from happening, resilient architecture across the board, and well documented response and resolution processes for both operational issues and business critical IT incidents, you can reduce customer and stakeholder frustration, and increase business success.

Key Recommendations

1. Standardizing a plan for how you respond to incidents – critical or not – can be beneficial, and prevent you from scrambling when an incident actually occurs.
2. Communication and collaboration can help reduce your Mean Time to Know, which, in turn, shortens your Mean Time to Repair. Communication during this period should be specific and offer guidance.
3. Automation is essential for incident management, but you can’t forget about human interaction completely.
4. When putting together an incident management plan, don’t forget about mobility trends, such as bring your own device and telecommuting. These two trends could completely change how you respond to critical IT incidents.
About Everbridge

Everbridge provides a unified critical communication suite that helps clients be better prepared, make better decisions, and respond quickly and confidently during disruptive events. When an incident happens, whether it’s a natural disaster or an IT service outage, we automate communications to ensure that the right messages get to the right people at the right time.

Widely recognized by analysts as the market leader, Everbridge solutions are trusted by clients in all major industries and government sectors to connect with over 50 million people around the world.

THE ONLY END-TO-END PLATFORM

- **Planning**: Everbridge is easy to set up, maintain, and organize, meaning that you’re always ready for a quick, coordinated response. Everbridge ensures that the right messages get to the right people - with the most advanced opt-in portal on the market, streamlined integration with internal and external data sources, and simple group and contact management.

- **Assessment**: When trouble strikes, you need rich insight, presented simply - so you can quickly assess potential impact and make an informed decision to avoid loss. Everbridge offers the only solution on the market that meets these demanding requirements, with the most advanced interactive dashboard in the industry.

- **Response**: In critical situations, ease-of-use can mean the difference between an effective response and a mistake that carries serious consequences. Everbridge is engineered to be simple to use under pressure, with a user interface that accelerates time-to-message and reduces the likelihood of errors.

- **Delivery**: Even during large-scale disruptions, Everbridge stays on. The most advanced platform in the industry ensures that you reach your contacts - every time. And with worldwide coverage and capabilities, including globally local calling infrastructure and data storage, we’re ready to support you wherever your people are in the world.

Visit [www.everbridge.com](http://www.everbridge.com) to learn more.