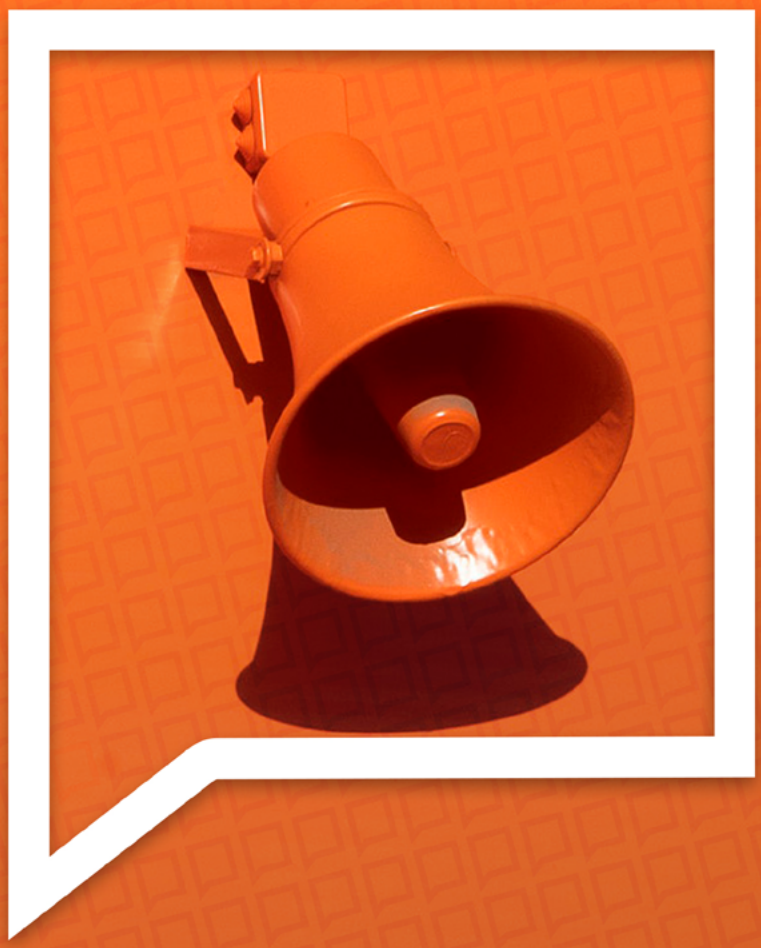
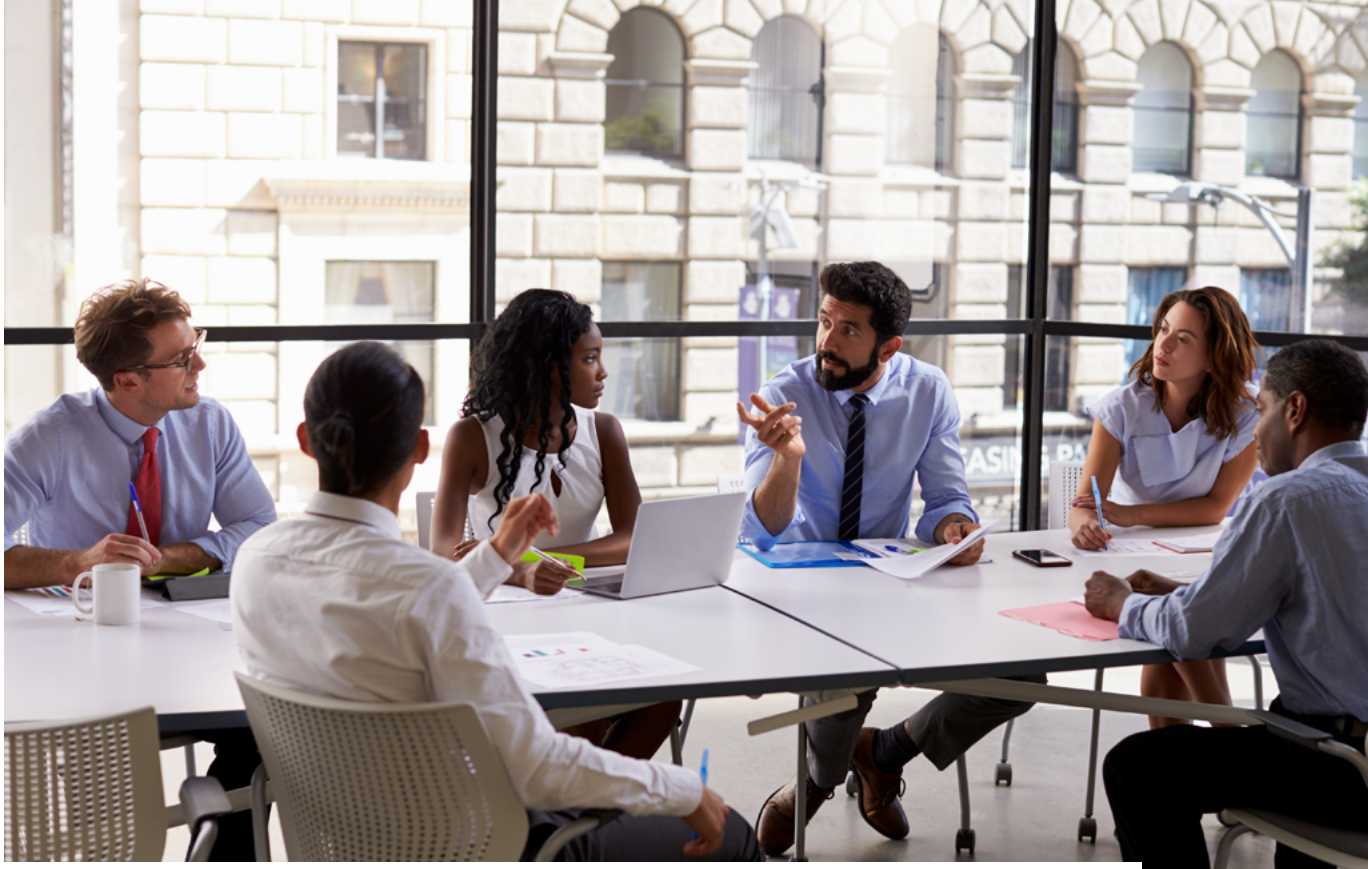


EFFECTIVE IT ALERTS:

How To Create Messages That People Will Actually Read

AlertFind



Communication is a key element of incident management. If you're not delivering clear and concise messages, your organization is vulnerable to chaos and confusion during an IT incident.

IT service desks are best equipped to efficiently respond to incidents when they implement the proper communications process, roles, responsibilities and tools.

Although this does require upfront work in creating a communications plan before an incident occurs, it makes your job as an IT service desk manager easier in the long run and better protects your organization.

Overview Of The Communications Structure In IT Organizations

At many IT organizations, communication is a big challenge. Despite the popularity of frameworks such as ITIL and Lean, IT incidents are often handled poorly due to a lack of coordination.

An IT organization usually needs to communicate with three main groups:

1) **Internal IT support team**
2) **Business owners and employees**
3) **Customers**

The IT team wants as much information pushed to them as possible, and that's where a good IT alerting system is an invaluable tool. It should easily integrate with IT service desk solutions to keep your organization more informed.

A detailed and highly configurable IT alerting system helps guide the IT department in responding to error messages. With every IT incident, you're prepared to take a holistic approach to the issue and outline the initial structure like this:

What is the incident?	Who's impacted by the incident?	How serious is the incident?

The IT service desk manager is responsible for diagnosing the problem and analyzing the impact. Depending on the answers to those above questions, you'll have different levels of response.

If it's a minor IT issue that doesn't impact many people, the IT manager will usually handle the incident. But if it's a major IT issue with significant business implications, the business manager needs to take over.

While the IT manager is an essential communication point during any IT incident, **the business owner should be the primary point of communication during major incidents**. That's because these issues need to be communicated to employees and customers in a nontechnical manner, avoiding language that only IT people might understand.

3 Biggest Communications Mistakes IT Teams Make

As you work to improve communication, pay close attention to these three mistakes that IT teams often make:

1 Not planning for incidents:

This is almost always the biggest mistake. Whether it's business continuity or disaster recovery, planning is key to being prepared for incidents. Having a plan in place helps you handle incidents in a controlled, procedural way. Otherwise, you risk creating issues elsewhere, increasing downtime and potentially doing more damage.

For instance, IT teams have a tendency to focus on resolving the root cause, but it's more important to first identify the issue, put the workaround in, and get the service back up and running. Once service is restored, IT can then focus on fixing the root cause of the issue.

2 Producing too much or too little information:

This is a common problem for IT organizations, as they're often dealing with complex situations, such as a malicious attack or a hardware malfunction. Your goal is to be honest with the communication, even if that means the first message doesn't contain many details.

For example, it's OK for an initial message to say: "We're working to bring the system back up as soon as possible. We'll provide an update in three hours." You want to show that the issue is being handled in a controlled manner. Be sure to follow up as promised.

Avoid the temptation to provide so much information that the message becomes complicated. On the other extreme, try not to "drip out" several frequent messages about a worsening situation, as this causes people to feel more anxious about what's happening.

3 Causing panic with improper communication:

The biggest risk with improper communication is creating panic. The situation must match the communication structure put in place.

Consider a situation where you're communicating with bank customers about an IT service disruption. Sending the wrong message could understandably cause panic. But if you communicate calmly and clearly that there's no danger, and make the necessary arrangements for customers to withdraw money, you're ameliorating the situation.

Your goal is to create appropriate comfort within the client and internal audiences. Remember to focus on the whole process as opposed to just your initial communication. You may have to suffer some reputational damage initially to ensure the overall process remains under control.

What Each Team Should Cover In Your Communications Plan

In a tiered support system, each line plays an important role in an ensuring the right communication during an IT incident. Here's what should be covered at the different levels:

Zero Line

This is for your automated services, such as a password change that doesn't require involving a person. While automation can save time and money, be careful about automating too many services, especially if you need feedback from users in your organization.

If you do a total cost of ownership (TCO) analysis, you'll usually find that the issues created by automating too heavily eliminates any savings. With IT alerts, you're aiming to inform people and prompt them to take action. When messages aren't tailored to each unique situation, you create more problems and fail to deliver on the primary goal of communication.

First Line

This line is all about getting the business up and running again by finding workarounds to issues. It usually consists of junior-level people who aspire to become specialized.

You should work to nurture and grow your first-line IT team members, as they can play a key role in bridging the gap between the business and IT. Attrition rates are usually high on the first line, as they're not technical roles. However, **these roles are highly important for improving communication.**

Second And Third Lines

This is where you'll have your specialized resources. The second line is usually looking at specific systems in the IT organization, such as database or network administrators, while the third line is more strategic and often consists of architects.

These highly skilled IT team members work on root cause analysis of issues and process improvement. Since these specialized people are often critiquing their own work, good management is needed to ensure efficiency on the second and third lines. People on these lines should also be available for IT maintenance work as well.

Sending Alerts At The Right Frequency

How often you should send alerts depends on the impact the incident is making. If it's affecting a small part of the client community and work can continue, you'll need few communications. Simply alert people about the issue, provide workaround solutions and notify them when the situation is resolved.

For more serious issues, such as a power loss at your data center, you'll want a broader communication strategy with more frequent messages. You can also have staff on-site to provide support. This is a must-have for major events like disaster recovery, where you need someone who has an established relationship with the business involved.

The business environment today is significantly different compared to even a decade ago. There's a heavy focus on meeting stringent service-level agreements (SLAs) and key performance indicators (KPIs).

As a result, **it's critical to build the appropriate relationships before an incident occurs.** Incident management can't happen in a vacuum. Building relationships in advance helps you respond to IT incidents more efficiently.

How To Avoid 'Alert Fatigue' When Sending Messages

Each message you send should contain new and valuable information. Don't send the same IT alert multiple times.

Write your alerts so they're brief but informative, highlighting the issue and any steps you want people to take. Think about your audience, message and mode as you write alerts:

AUDIENCE: **Who is the alert going to?**	An IT alerting system allows you to target only those people affected by a location-based or system-based event.
MESSAGE: **What should the alert say?**	Your goal is to help people, so use easy-to-understand language.
MODE: **What channels are you going to use?**	Ideally, you'll have the option to send messages across multiple channels, from email and text to mobile app push notifications and pagers.

When necessary, restrict communication to the appropriate level. An IT alerting tool allows you to target messages to specific groups. This helps to avoid "alert fatigue" and reduces the chance an alert will be missed with general company-wide messages.

The best alerts stick to the facts. Before sending messages, take a few minutes to understand the scope of the incident and gather all of the information. Sending inaccurate information will only confuse people and make the situation worse.

As an example, if a data breach takes place, send out an alert to immediately notify people about the breach and advise them to take specific protective steps, such as logging out of the system. Then let them know when to expect follow-up communication.

Don't use automated messages for critical business issues. In those situations, people want to feel a human interaction.

Resources And Tools For Structuring Communications

All of the IT service management frameworks, such as ITIL and Lean, have communication elements built into them. They're also built on the same best practices – identify the stakeholders, determine the best medium to reach them and choose the frequency of communication based on the severity of the incident.

ITIL is more mature than Lean, which is closely associated with cost-cutting. Regardless of which framework your organization uses, you want to focus on responsiveness and agility.

An IT alerting tool is a valuable resource for keeping people informed during an incident. You don't have to worry about people missing messages when email is down, because alerts can be delivered via multiple channels, including text, voice call, fax, mobile app push notifications and pages.

With auto-escalations, no time is wasted assigning an issue to a team that can fix it. If an on-call resource doesn't respond, the incident alert goes to another team member until it's picked up.

Here's the key takeaway:

While using IT tools is essential, the IT service desk needs to always be in control. It's tempting to rely on automated messages, but that's not a good communication strategy for handling incidents.

To deliver clear and concise messages, you want your people on the IT service desk making decisions around diagnosing problems, analyzing the impact and sending messages that keep people informed.

Effective IT alerts start with your communication plan for incident management. With the right foundation in place, you'll be prepared to create effective messages that people read and take action on immediately.

About the author

John Degura is an experienced business and IT professional with a demonstrated history of consulting in the information technology and services industry.

He is skilled in business strategy, business administration, product management and service management, and has experience using Agile methodologies, PRINCE2 and ITIL.