



# Best Practices For IT Incident Communication

# Introduction

Even the most skilled IT departments have experienced significant downtime issues affecting customers. In fact, the [Hartford](#) reports that 36% of U.S. mid-sized businesses have been unable to meet a client need due to an interruption in their operations. Additionally, the average cost of downtime quickly adds up to \$163,674 per hour.<sup>1</sup>

This eBook provides concrete, proven recommendations to speed up downtime resolution by establishing an effective incident communication strategy. What processes and procedures do teams need to adopt? What types of automation should they adopt?

Read on to learn how to develop an incident communication approach to help you solve downtime issues as quickly as possible and improve IT team performance.

<sup>1</sup>[Datto blog](#)

# Reduce noise

During Target's 2013 data breach, staff in Bangalore, India notified Target staff in Minneapolis that an attack was detected. However, the Minneapolis team didn't take action because this serious alert was drowned out by many other false alerts. In fact, 52% of alerts were false positives and 64% were redundant alerts.<sup>2</sup>

This is just one example of a team becoming desensitized to actual serious alerts due to the overwhelming number of false or low priority alerts. Effective incident communication requires IT teams to reduce noise so teams know which alerts truly require immediate action, even when it occurs at 2 a.m. This involves reviewing past incident reports and data to develop criteria for different levels of alerts.

<sup>2</sup> [CSO Online](#)

# Automate alerting

Once the IT team determines the criteria for prioritizing alerts – such as “no action required”, low level or critical – these are used to set conditions for automated intelligent alerts. For example, team members can get automated alerts based on the severity of the problem, their role and/or their on call schedule. Managers can determine in advance how they get alerted (email, text, etc.) to incidents depending on the type of issue. Engineers can get incident instructions from an alerting app including details on the functionality that’s at risk.

By automating alerts, teams can communicate more efficiently. Critical alerts are surfaced appropriately and get immediate attention, the team has the right level of detail about the problem, know what they need to do and when to do it.

# Use smartphones over email

To dramatically reduce noise, IT teams use smartphones along with incident alert management apps. They get instant access to alert information and updates no matter where they are, and the message is not lost in email or text messages.

For after-hours issues, the app instantly alerts engineers based on their on-call schedules. The incident alert app sounds an alarm that is loud and hard to ignore – the perfect way to be notified of a serious issue around the clock.

# Use escalations and redundancies

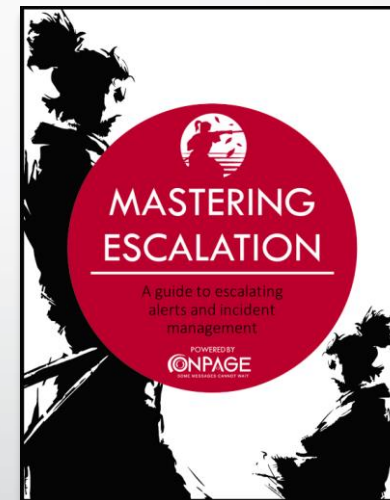
It's unrealistic to expect that every incident will receive an immediate response from the IT engineer on-call. He or she might be occupied with another task or momentarily unavailable. Consequently, escalation policies and processes are a necessary part of effective incident communication. With an escalation approach, the next person on call will be alerted when the first engineer on the list does not respond. An effective incident management solution will enable escalations after a pre-defined period. A common configuration is to alert the next person on call if the first person does not respond within one minute.

It's also important to enable multiple communication channels. Using redundant communication channels such as phone, SMS and text along with smartphone apps ensures recipients are notified in a timely manner regardless of technical issues or conditions.

# Master escalation management

For IT teams to effectively manage a critical incident, the team members need to know when to escalate the issue to someone with different skill levels or when to delegate to another colleague because the alert's recipient is busy with other tasks. For each case, it's important to know the communication procedures to follow to make an effective hand off. For details, check out this "Mastering Escalation" white paper.

[Download the white paper](#)





# About OnPage

OnPage provides an award-winning incident alert management system for IT professionals. Built around the incident resolution lifecycle, OnPage's unique ALERT-UNTIL-READ smartphone app and platform capabilities help teams reduce downtime and IT costs while improving coordination and performance.

OnPage's escalation policies, redundancies, and scheduling algorithms ensure that a critical message is never missed. Infinitely more reliable and secure than emails, text messages and phone calls combined, OnPage provides instant visibility and feedback on alerts. As part of IT service management, the solution tracks alert delivery, ticket status, and responses. The OnPage platform includes powerful integration with mission-critical systems, to help deliver optimum service levels and get the most value from IT investments, making sure that sensors, monitoring systems, and people have a reliable way to escalate anomaly notifications to the right person immediately.

To learn more, visit [www.onpage.com](http://www.onpage.com) or call 781-916-0040