5 Actions Proactive IT Service Desks Take To Improve Response Times

AlertFind

The biggest risk to business operations at most organizations is an IT outage – regardless of the cause. They cost North American companies up to $700 billion a year, and with every minute of downtime costing thousands of dollars, improving response times is critical.

Whether you're dealing with a service outage, a cyber attack, an insider threat or a natural disaster that shuts down your IT infrastructure, IT service desk managers can benefit from an alerting system that allows them to immediately reach all employees and protect business-critical operations.

IT is the backbone of your business operations.

Without your critical business data, how can your organization continue? An IT service desk is the front line for all service outages (including servers, applications and third-party cloud apps) as well as cyber threats (such as data breaches, IoT vulnerabilities and ransomware).

While IT budgets are climbing as more organizations view it as a necessity, major threats continue to deliver crippling blows. Even smaller incidents can cause significant problems.

For instance, consider the impact an email outage has on productivity at an organization. How will your employees communicate with customers? With each other? With suppliers? What will trying to work around this outage cost your business in terms of lost productivity?

By handling both big and small incidents quicker, and reducing time to resolution from hours to minutes, businesses save significant money in lost productivity.

Shortening response time is the ultimate goal for IT service desk management.

With the right IT alerting system and a centralized alerting strategy, IT service desk managers are better equipped to more quickly restore service and critical business functions.

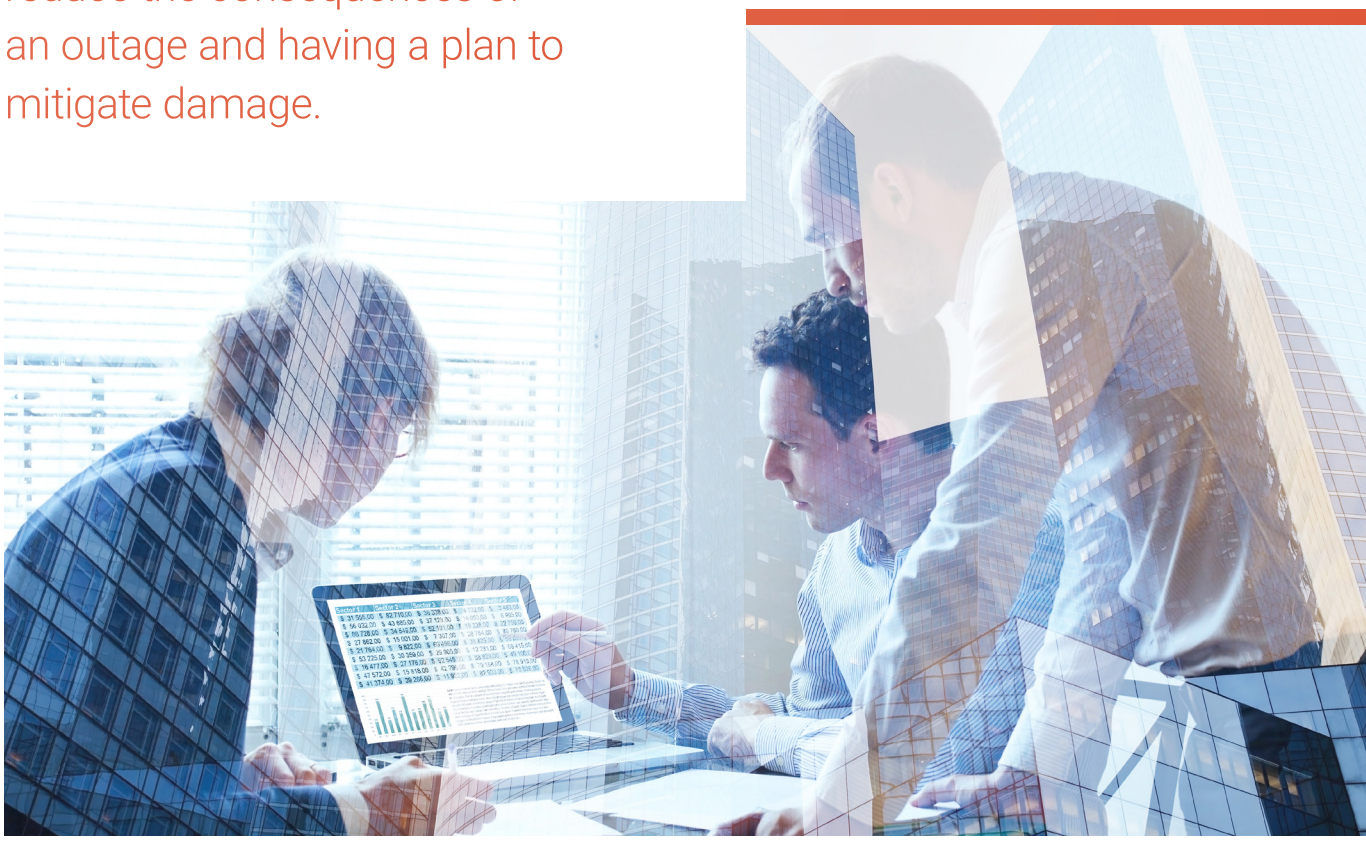
Calculating The Cost Of Downtime

For all businesses, an IT outage will happen at some point, and outages affect organizations regardless of size or sector. The key is being prepared to reduce the consequences of an outage and having a plan to mitigate damage.

Research from Gartner estimates network downtime costs $5,600 per minute. That extrapolates to more than $300,000 per hour, which highlights the severity of even a one-hour email outage.

Businesses also need to consider reputational damage, which is often harder to quantify financially but can have long-lasting consequences. Customers usually feel the impact of IT outages, even if it's just a simple delayed response. Data breaches of customer data can significantly damage a business as customer often leave after their information is exposed.

The key is being prepared to reduce the consequences of an outage and having a plan to mitigate damage.



But business leaders don't always see how IT projects aimed at decreasing response time provide direct value for the company. To help highlight that value, an article on CIO.com recommends a two-step approach:

1) Draw a picture (or a diagram) to visualize the issue
2) Provide specific downtime cost numbers

Visualizing the issue helps CEOs understand the potential impacts of IT outages, including productivity loss, revenue loss and the loss of clients. The longer the downtime, the larger the impact.

To calculate the financial impact, the CIO.com article suggests using an equation that takes into account impacted employees, their average hourly salary and the productivity impact factor. For example:

Cost of downtime:

(1,000 impacted employees)	**x**
($20 average hourly rate)	**x**
(50% productivity impact factor	**=**

$10,000 PER HOUR
of productivity cost impact

Quantifying the financial risk of downtime helps with making the business case for an IT alerting system. For example, if you're in manufacturing and your systems are down, you can't make money where you're not producing products.

Most of the time, when you do a cost-benefit analysis, the costs involved with an IT alerting system are far lower than what the organization loses from downtime and lost productivity.

Putting A Plan Into Place: 5 Steps To Reduce Response Times

Once you've highlighted the importance of shortening response time and made the business case for a more proactive approach to IT management, you're ready to start developing a plan.

Here are the five main actions IT service desks should take to improve response times:

1 Centralize IT and emergency alerting

Creating a unified alerting center for both emergency and IT notifications delivers both operational efficiencies and cost savings. By centralizing all alerting across the organization, you have one solution to handle all incidents, from service and infrastructure outages to cyber incidents and natural disasters.

Traditionally, companies have used two different systems – the IT alerting system lives within the IT organization, and the emergency notification system is run by the emergency preparedness team.

But it makes more sense to take an all-hazards approach to alerts. Generally, the IT organization has a 24-hour presence, whereas emergency preparedness is an on-call function. This type of unified alerting system gravitates toward those around-the-clock functions, allowing businesses to seamlessly blend IT and emergency preparedness into a 24/7 operation.

Any private-sector entity could benefit from this approach. Having two different alerting systems leads to duplication of effort and cost, so integrating them into one platform delivers cost savings.

Most importantly, centralizing IT and emergency alerting provides maximum efficiency to improve response times. Whether an issue is from the user, IT, the business or the cybersecurity team, this combined alerting system has the mechanisms in place for proper escalation of an incident.

How To Staff A Unified Alerting Center

When staffing a unified center, you want people who excel at facilitation, communication and resource management. They need the ability to engage the right people, re-prioritize work as needed to keep the business moving and drive the incident to resolution.

Ideally, they'll also have a good working knowledge of the organization, so they know which people in IT, facilities, security and the business units to engage in specific situations.

Take an IT outage as an example. People working at a unified alert center need to gather data and disseminate information about:

- **Which system(s) is down**
- **Whether it's a total or partial outage**
- **If any workarounds are available**

As the incident matures, the alert center staff continues to communicate to provide more information, while at the same time paging out appropriate resources to respond to the incident. They keep that cycle going – engaging resources, troubleshooting and communicating – until everything is restored to normal, at which time the alert center communicates a closure.

The number of people you'll need in a unified alerting center depends on the organization and its volume of incidents. A large organization may have up to 10 people staffed at a time. The working best practice is to have at least two people, because in a 24/7 center, you don't want to have somebody alone from a health and safety standpoint.

2 Send IT alerts immediately when a threat is detected

As soon as a threat is detected, notify employees and any other key stakeholders with clear directions on protective actions. For example, you might direct them to stop using their email or to use an alternate system. In the event of a phishing attack, the ability to reach people with an urgent alert allows your IT team to isolate and remediate the threat.

With an IT alerting system, you can set up preconfigured recipient groups, so alerts go to the person or team that can take action to resolve the issue. This reduces the chance that an alert is missed with general, team-wide notifications.

You should script alerts in advance for hazards that your organization faces and ensure the alerts answer these key questions:

- What is the hazard?
- Where is the hazard located and/or who is affected?
- What actions do you want people to take?

As an example, for a cybersecurity incident, your alert might look like this:

> ***Threat:*** A data breach takes place and your IT system is hacked.
>
> ***Action:*** Immediately notify people about the breach and advise them to take protective steps, such as logging out of the system.

Make your message clear and concise. Use plain language that your audience will understand, and avoid technical terms that only IT professionals might know.

3 Use a system that contains every employee's contact information

Your IT alerting system should have a feature that ensures every employee's contact information is in your database. This helps to make sure that no employee will miss a critical update or notice about service outages or system changes.

When sending IT alerts, it's critical to prevent confusion and maintain employee productivity. You don't want to be guessing about whether you have the correct contact information. If there's a full IT outage at the organization, all employees need to be notified about any workarounds so productivity loss is minimized.

Make sure your alerting system is automatically collecting and updating employee contact data in the system's database. Relying on employees to remember to update their information means your database will always be incomplete.

4 Be able to escalate a service ticket until a support team can pick it up

An IT issue is usually deemed significant if it causes a major financial impact, reputational impact or productivity impact. Auto-escalations help with managing the notifications needed to resolve IT issues. To improve response times, it's critical that no time is wasted assigning the issue to the team that can fix it.

Your IT alerting system should make sure that if an on-call resource doesn't respond, the incident alert goes to another team member until it's picked up. IT service desk managers should be able to specify both user-to-user and group-to-group escalations.

5 Have several channels available for communication

You need to ensure alerts are delivered even if your network is compromised. That's why you want to use an IT alerting system that offers secure off-network alerts supported by redundant data centers, so you don't have to worry about communication when email is down.

Your alerts should be able to reach employees on multiple channels, including email, text, voice call, fax, mobile app push notifications and pages. Having multi-channel alerts gives you a variety of communication options in case the internet goes down and some channels are unavailable.

In addition, with two-way communication features, you can quickly get real-time information and status updates from your team, either individually or in groups.

Do Regular Training To Test Your Plans

As part of building your plan to proactively improve response times, it's always important to exercise all elements of the plan. In a unified alerting center, you may have an Emergency Operations Center (EOC) set up for big incidents, but the first call comes through your alerting center.

For small incidents, your resources at the alerting center might be able to resolve the issue without needing to escalate it. But for a bigger issue that's having a significant impact on the business, you'll likely need additional resources and have to activate the EOC.

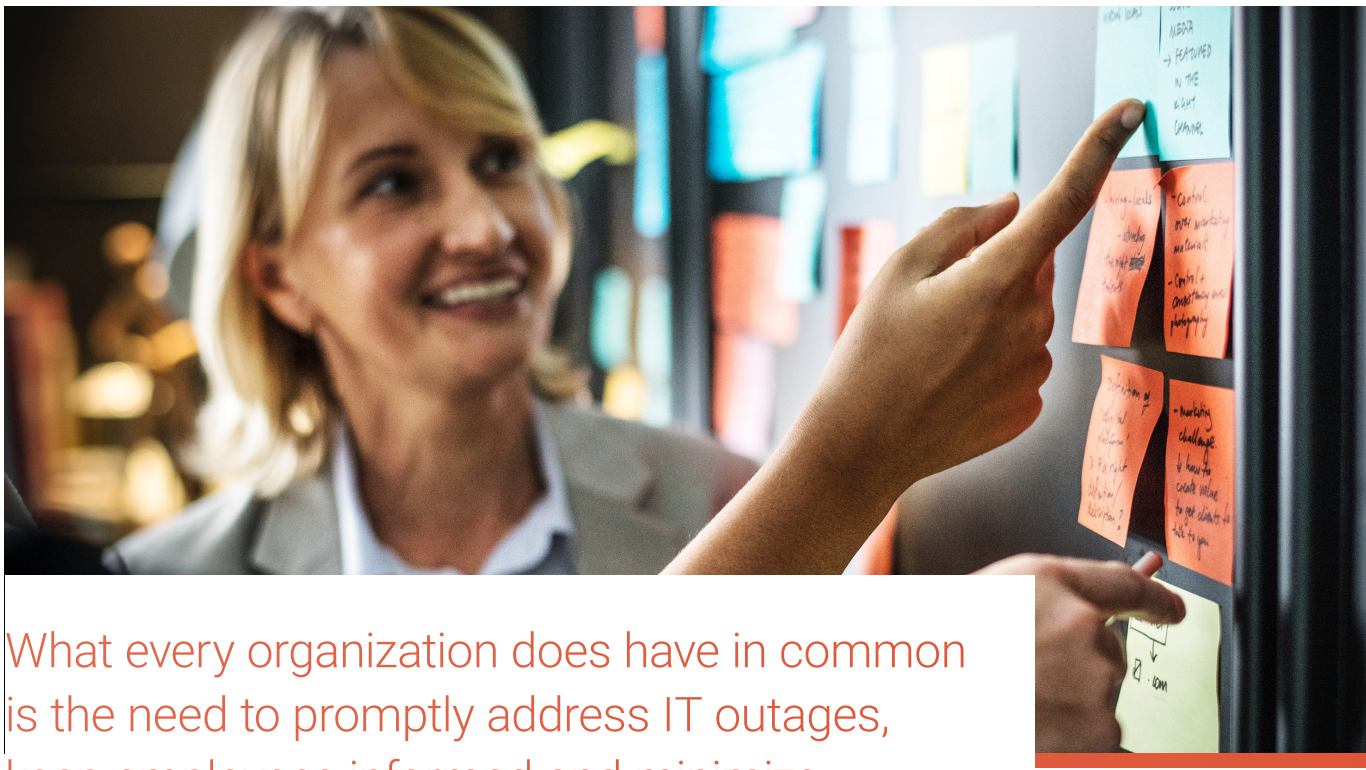
Be sure to regularly test your plans with training exercises, from the first phone call all the way through mobilization of the EOC and closure of the incident.

Use The Right Tools To Improve Notification

To limit damage and decrease downtime, IT service desk managers need a robust IT alerting system. The system should easily integrate with your service desk solution, allowing your team to take action quickly and keep the business running.

Just as importantly, your IT alerting system has to be flexible to accommodate your organization's unique needs. Do an assessment to determine specifically how IT alerting tools could benefit your organization and the best way to implement them.

You won't find an easy blueprint or one-size-fits-all strategy for IT alerting and IT service desk management. You need to find an approach that works best for your company, building a model based on your resources and business structure.



What every organization does have in common is the need to promptly address IT outages, keep employees informed and minimize productivity loss. That's why improving response times should be a top priority for every IT service desk.