KT Kepner Tregoe

Achieving Service Excellence in Major Incident Management

Most modern companies depend on technologies to such a degree that it results in a significant risk of technical issues creating IT stability problems and in turn challenge an organization's functional capabilities.

Ensuring a quick-and-effective response and having a well-conceived major incident-management process are the keys to mitigating this risk.

Major incidents are reported in the news every week – security breaches from hackers, system outages and customer data being exposed. These are just those that make headlines – countless, more major incidents occur every day that impact companies' internal operations, profitability and the flow of goods and services and distract company leaders from their core role of driving their company's agenda forward.

Dimensional Research's 2016 survey of more than 400 business and IT professionals found 82% of respondents reported that business application downtime had a significant impact on their company's revenue. The risk exposure and response to major incidents are top of mind for most executives, as they see their peers struggle to manage crisis situations – knowing that their personal career and company's future may hinge on their performance during a few hours or days.

Successfully managing a major incident can enable a company to return to normal operations quickly, preserve market reputation and minimize financial impact. Well-managed incidents might even provide the opportunity for continuous improvement by providing deeper insights and help a company to continue to accelerate towards its goals. If an incident is not successfully managed, then the lasting impact can lead to the company's demise.

The Impact of Major Incidents

Most companies have sufficient processes and resources to operate during a crisis mode for a short period of time (a few hours to a couple of days). Beyond this period, staff fatigue, issue backlogs and loss of critical control mechanisms can result in quickly declining customer satisfaction, compliance issues and reconciliation challenges that make a complete recovery more difficult, costly and time consuming (if complete recovery can be achieved at all).

Beyond the immediate operational impact, the managing of a major incident can affect customer perception and long-term confidence in the company and its products. With ever-intensifying competition from insurgents and new business models, shrinking profit margins and increasing cost of acquiring new customers, customer retention and satisfaction are critical to ensuring the sustainability of revenue. Customers understand technology problems happen – they too are technology consumers and users facing the same risks as companies.

Much like internal company operations, most customers have some level of tolerance for short-term disruptions during their interactions with businesses and in the products and services they purchase and use. Extended disruptions, poor communications and a failure to restore service in a timely fashion, however, can significantly erode customer tolerance and goodwill – potentially causing permanent damage to relationships and opportunities for future business.

> ...if it happens once, then it is forgivable; if it happens again, then heads might roll.

Both the internal operational impacts and customer reputation issues will eventually undermine the current and future financial performance of a company – with collateral damage increasing as the incident continues. Recurring issues also compound the impact of major incidents – if it happens once, then it is forgivable; if it happens again, then heads might roll. Executives are aware of this and have begun spending an increasing amount of time developing their understanding of the risks inherent in technology dependence in their business, developing mitigation strategies and preparing their organizations for the likely occurrence of major business-impacting incidents.

Incident Management vs. Major Incident Management – Why Companies Need a Different and Separate Approach

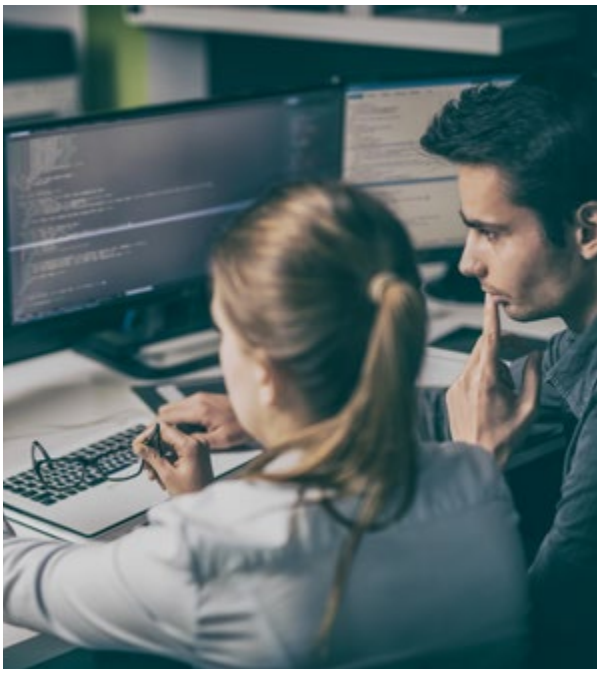
Most companies have incident-management processes in place to address day-to-day minor to moderate disruptions. These processes are built from tried-and-true customer service methods and/or based on standard IT Service Management practices (such as those found in ITIL). Incident-management processes are typically effective addressing the large volume of relatively low-impact incidents and service requests that a company faces related to its IT systems. Major incidents, however, are different than their smaller, day-to-day counterparts and require a different and separate approach.

Impact and Frequency

Major or high-severity incidents (as the name indicates) are those that have a large and significant impact on the organization. These incidents (hopefully) don't happen very often, but when they do, entire functions of the business may be affected. A typical Fortune 500 company may encounter a handful of major incidents during a quarter, compared to hundreds (or, in some cases, thousands) of normal incidents each day. A normal incident typically only affects a few users with response-and-resolution SLAs often prolonged as a means of keeping operational costs low. For major incidents, the cost of the impact far outweighs the cost of resolution and the key success factors are response time and the quality of the response to the issue.

Skills and Who Is Involved

Service-desk personnel with limited training and technical skills are often those that must address day-to-day incident-management functions – an acknowledgment that most incidents are routine and repetitive in nature and can be effectively resolved through basic diagnostics, binary decision/knowledge trees and scripted responses. More difficult issues are routed to second- and third-tier escalation teams with technical expertise, but the goal is still to apply the least-technical (and cheapest) resources available to resolve the incident. Major incidents require a different resourcing approach. Time is of the essence; so the goal is to apply the human resources who can resolve the incident the quickest and thus avoid a prolonged period of business impact. These resources are typically highly trained (and highly paid) subject-matter experts with extensive experience and deep technical troubleshooting skills.



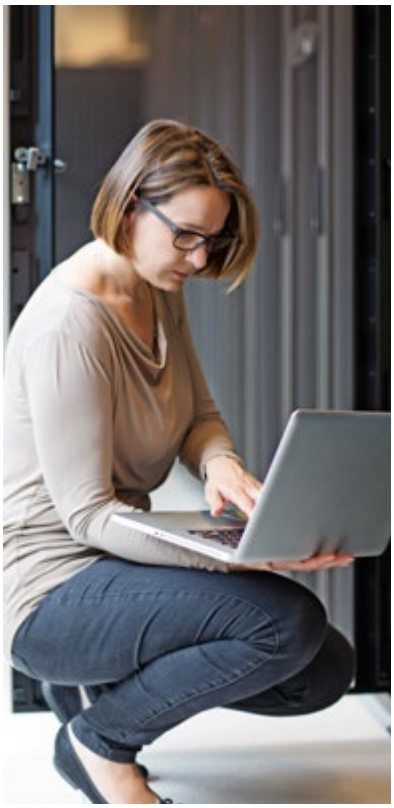
Processes

The trend during the past few years has been for incident-management processes to shift towards self-service, automation and asynchronous engagement with support staff (i.e., email interactions with staff in global call centers). This" deflection approach" is designed to optimize the incident-management process for scalability and reduce human interaction, but comes at the expense of increased time to resolve more complex incidents. Major incident processes must be optimized in almost an exact opposite way, with the effectiveness of the solution and time to resolve being most critical and de-emphasizing resource cost and automation considerations. How these processes must be optimized makes it very difficult for one to be considered a subset of the other. In addition to process confusion, resource conflicts and different priorities can cause both processes to underperform.

For a major Incident-Management process to be effective, organizations should consider 3 major stages that must be managed during short, iterative cycles, as new information becomes available: triage, diagnosis and decision making. Triage helps to assess impact and gather all available data to specify the issue and understand what resources are required for resolution (before jumping on a bridge call with 50 other people!). Diagnosis is critical to analyzing the symptoms (and possible causes, if necessary) as well as filling the information gaps to determine the most effective restoration actions. Finally, decision making relates to understanding and evaluating the options while keeping the risks constantly visible and, of course, executing effectively.

Communications

Incident-management communications are typically focused narrowly on a direct interaction between the user reporting the issue and the person or team working to resolve it. Escalation and, hence, making management aware of the incident is seen as a "failure" or exception to the initial process and adding unnecessary cost to the business.



Major incidents are different in that active and broad stakeholder communications are not only helpful for accurately assessing impact, but also help to manage expectations and instill confidence in stakeholders that the incident is under control. During many major incidents, the perceptions created by stakeholder communications have a larger role in determining the overall impact than the technical issue and associated symptoms. Effective major incident communications must target 4 separate stakeholder groups.

1. The affected user community whose activities the incident directly impacts
2. Indirectly or potentially impacted stakeholders whose confidence the managing of the incident is likely to impact
3. Internal teams and SMEs who may need to participate in incident diagnosis and resolution (this can also include vendor representatives)
4. Support and IT Management

Managing Perceptions

Major incidents often invoke emotional responses and crowd dynamics that may include a variety of influencing factors while normal incidents typically only involve one or a few users whose perceptions are typically tied directly to the incident itself. During major incidents, not only does the impact cause information to spread rapidly by word of mouth, but also it is not uncommon for idle employees to introduce into the communication mix speculation, inferences, uninformed interpretation of events, biases and sideline commentary of how the incident is being managed.

Controlling the flow of communications and managing perceptions are critical to major incident management. If the official messages from the major incident-management team are not clear, timely and provide the information stakeholders expect, then there is a risk that misinformation will overpower the official messages, resulting in greater confusion and a negative customer experience.

Executive Involvement and Decision Making

In addition to overall technical and performance impact, major incidents and the activities required to resolve them often extend across business function boundaries, causing issues of decision-making authority to arise. Major incidents almost always require some sort of executive involvement to assist in impact analysis and communications and making key decisions necessary to remove roadblocks, so the issues can be resolved. This is a high-stakes environment, where management must weigh the expected outcomes of certain actions against their risks. This not only requires clear ownership, but also clear, accessible data of what is known and what isn't known about the current incident. A major incident-management process should include cross-functional, decision-making guidelines to avoid delays and confusion while an active major incident is occurring.

Mitigating Symptoms May Be Challenging; Addressing Causes Can Be Even More Difficult

The challenges of major incident management don't end when service is restored. As with normal incident-management processes, the primary objective during a "live," major incident is to mitigate impact and take corrective action to return the business to normal operations. Understanding root cause and implementing

actions to prevent the issue from re-occurring falls under the purview of problem-management processes. With the heightened business impact of a major incident, it is commonplace for executives to follow up actively to ensure that root cause is identified and preventative actions implemented in a timely manner.

In many cases, the executive expectations of problem management are unrealistic, with the challenges two-fold.

1. Moving past the symptoms of the incident and identifying true root-cause. Amid the confusion of managing the active major incident, critical diagnostic information is often lost or destroyed, impeding root-cause identification.
2. Securing support and prioritization for preventative actions and implementing fixes once the business has returned to normal operations. While the business is actively impacted, there is often a "do-whatever-must-be-done" attitude that quickly disappears once service is restored.

To avoid these two pitfalls, a highly integrated, major Incident- and Problem-Management process is required, where critical "cause information" is actively secured and documented and service improvement continues. Only then can true IT stability be achieved during a longer period of time.

Compliance vs. Mitigating Impact

Persistent abuse of data and technology have caused governments and regulatory agencies across the globe to impose a broad set of compliance requirements on companies to ensure the security, fidelity and proper management of certain types of technology and data. To maintain and verify compliance with these regulations, most companies have implemented a series of process and system controls to ensure individuals' actions are consistent with company obligations.

During a major incident, these controls can become cumbersome and inhibit effective diagnosis and resolution of the situation.

When this happens, company leaders and support staff are often faced with the choice of "breaking the glass in case of emergency" – bypassing the control mechanisms and risking regulatory non-conformance or maintaining the control mechanisms and prolonging the impact of the incident.

Depending on the situation and the nature of the controls being bypassed, this decision could have regulatory consequences and impact the future performance of the company. This is the business equivalent of the choice emergency-room doctors must make when faced with saving the patient vs. saving a limb. A company's

This is the business equivalent of the choice emergency-room doctors must make when faced with saving the patient vs. saving a limb.

major incident-management process must take that into account and provide a clearly defined policy and exception processes should bypassing them must be considered. In most cases, regulatory agencies will accept well-documented exceptions as a sufficient substitute for normal control mechanisms, so planning ahead is critical.

Most major incidents are temporary situations and a company will (hopefully) be able to return to normal operations, which includes process and system controls for compliance. In addition to the immediate impact of bypassing compliance controls, companies must consider the challenges and implications of re-establishing the control mechanisms after they have been bypassed for some time. After the incident is resolved, this may require a number of follow-up activities that are likely to be costly and time consuming. It's important to consider them when making a "break-the-glass" decision.

Activities include

- Data reconciliation
- Documentation of control procedure exceptions
- A compliance audit
- Formal review of control procedures to ensure regulatory compliance was maintained during the incident
- Verification that any issues of non-conformance are promptly addressed

Don't Wait Until It Is Too Late!

Company leaders can't control when major incidents will happen, but they can control how the company manages and responds to major incidents. Overall service excellence, which includes an effective and well-understood major Incident-Management process, is the key to responding to the incident quickly, resolving the immediate impacts, preserving company reputation and mitigating the operational and customer risk.

The major incident process should be separate from the process for managing normal day-to-day incidents and be optimized for speed and effective resolution in addition to thoughtful and timely stakeholder communications. During an active incident, support staff and executives should rely on major incident management to help them take control of the end-to-end process and guide their activities through:

- Understanding the incident and symptoms
- Mitigating the impact and managing risks
- Making sure decisions are visible and data-driven
- Assessing possible causes (if necessary)
- Managing perceptions and expectations
- Returning to normal

Achieving Service Excellence in Major Incident Management

Managing major incidents well may not be as compelling to many IT and support executives as, for example, new change initiatives, but managing them poorly can certainly be disastrous. As the industry-leading problem-solving company, Kepner-Tregoe has been working with customers to improve their capabilities to manage major incidents in operations and IT for more than 60 years, and to help them achieve service excellence.

Christoph Goldenstern

VP of Strategy & Service Excellence

Christoph is a consulting leader with 20+ years of experience helping organizations in the areas of strategy, operational and service improvement. As a member of KT's executive leadership team and global VP of Strategy and Service Excellence, he is responsible for KT's business strategy as well as its solutions for IT Service Management andTechnical Support.

cgoldenstern@kepner-tregoe.com
Office: +1 609 252 2900

KT's data-driven, consistent and scalable approach to Incident, Problem, and Change Management is helping companies deliver a world-class customer experience and increase stability by reducing downtime, issue recurrence and cost of service. To learn more about how Kepner-Tregoe can help your company implement and improve major Incident-Management processes, visit http://www.kepner-tregoe.com or contact the KT problem-solving experts at info@kepner-tregoe.com.