

Avoiding the War Room

BY RYAN RHODES

The term “war room” has become increasingly accepted into the often arcane vernacular of the IT world, providing insight

into the extent to which organizations depend on

their data centers for everyday business operations.

System performance degradations and outages were once relatively easy to troubleshoot and address, but now they can vitally handicap regular business operations and can require a full-blown war room response team, like something right out of “Dr. Strangelove.”

While some companies refer to their IT troubleshooting process by a term other than “war room,” such as “situation room” or “command center,” the underlying concept is essentially the same. War room refers to the process of bringing together IT professionals and subject matter experts to troubleshoot and address an unexpected performance impact or outage.

The war room has become an unfortunate necessity for data centers that have become wildly complex and increasingly inter-dependent on hardware and software from a variety of vendors. Disparate arrays of composite business applications are responsible for many front-end and back-office transactions and mission-critical operations. Supporting those composite business applications are personnel who can suddenly find themselves being called into account when something goes wrong.

Companies can take steps to reduce the occurrence and impact of IT downtime.



“War rooms are typically held when critical business applications aren’t performing or available,” says April Hickel, senior middleware and transaction management product manager for BMC Software. “The various IT professionals and other experts have to come together to determine the problem and pinpoint whose problem it actually is. So, there’s a lot of finger-pointing, with people saying, ‘It’s not me, so it must be you.’ Until the problem is resolved, the war room is the vehicle for communicating the status, what’s going on, who is working on what and how soon it will be resolved.”

While the war room will continue to be necessary, it can be costly, both in terms of lost revenue as well as IT resources being pulled away from other projects to address the immediate problem. However, while the need to quickly identify the root cause of a problem is an ongoing requirement, you can reduce the chances for convening a war room.

War Room Costs

The war room troubleshooting and problem resolution approach is more than a mere operational inconvenience; it can have an impact on almost every aspect of how you conduct business. Every second you are experiencing a performance decrease or complete outage means potential revenue loss and diminished productivity.

“When a war room is necessary, almost everything else seems to stop,” says Hickel. “Normal operations aren’t possible until the problem is isolated and resolved, so you can understand why a war room can have such a huge impact on a company and why you should be prepared when a war room is necessary.”

As a corollary to the loss of revenue, customer satisfaction can also be negatively affected during a war room scenario. Customers are accustomed to things working quickly and seamlessly online, and they become unhappy when they encounter a system or service running slowly, unreliably or not at all. Things get worse if the downtime results in a violation of existing service contracts and agreements, which can quickly lead to legal headaches.

The longer customer satisfaction is negatively impacted, the greater chance the story of the downtime will be picked up by word of mouth, the wider world of the Internet or, in the worst case scenario, become a subject for national news. If and when word gets out that a business is experiencing downtime and can’t

optimally serve its customers, there’s a chance the corporate image, something not easily repaired, could suffer.

While all these potential war room impacts are playing out, a company’s day-to-day operations and projects are often left at a standstill. Pulling the data center professionals into troubleshooting mode means those personnel aren’t working on their regular tasks. Important projects designed to push the IT vision forward are often delayed and deadlines can be missed.

IT Performance Impacts: Common Causes

Despite the cost, the war room will continue to remain necessary for any company with a vested interest in keeping its IT operations up and running at high performance levels. The intricate complexity of most IT infrastructures practically ensures some level of downtime that should be both expected and prepared for.

“I think the leading cause of performance impacts and outages stems from the fact the applications customers are deploying have become so much more complex,” says Hickel. “Just 10 years ago, if you were a user trying to take an action online, chances were you were working from a single system. Now, if you do a common task, like ordering something from a retailer or conducting a bank transaction online, you’re almost certainly dealing with many systems that application spans.”

According to Hickel, application integration and the integration of system components—as well as the infrastructure dependencies—are the primary contributing factors to downtime.

“Applications are de-coupled, certainly with the advent of service oriented architecture (SOA) paradigms and similar messaging-based infrastructures,” explains Hickel. “You’re inherently creating composite applications that are built with many different pieces. I think everybody appreciates the benefits associated with the composite application approach to building a data center. But the problem is that when something starts to go wrong—something as common as a performance slowdown—it can be really hard to diagnose where the problem is. You’re not just going to the mainframe and back or to a single system and back, but you’re going through potentially many infrastructure technologies and different server tiers to execute a business operation. I’ve seen companies with over

500 servers supporting a single application, so you can imagine how complex it can get.”

In a similar vein, a company can have complicated agreements and dependencies with various vendors and partners and their applications and processes. Those complex relationships can eventually lead to a performance impact that’s very difficult both to locate and to resolve with the associated parties and agreements.

While IT complexity may be the most obvious cause of events necessitating a war room, other factors can also contribute.

Companies that lack at least some investment in middleware management are at a considerably higher risk for downtime occurrences. Middleware management acts as a defensive solution that can continuously monitor key transactions and business services. Continuous monitoring can allow companies to more quickly determine where a problem is located and how best to resolve it.

How a company conducts business can itself impact IT performance. If a complex business service requires a single transaction to be processed by myriad IT applications, and an unexpected jump in requests for that service come through, performance can drop considerably while those requests are processed. A war room may have to be convened after such an event to determine what happened and how to streamline those business services.

The sheer volume and diversity of the users and groups that access a company’s IT infrastructure can also degrade performance or cause a full-blown outage. After all, people make mistakes, and the more people who access a system, the bigger the chance someone will perform an action that unexpectedly—or intentionally—brings the whole system crashing down.

Perhaps ironically, another contributing factor to downtime is the limited personnel and financial resources dedicated to maintaining and updating IT infrastructures. Even considering the huge expenses that can be incurred with a war room, companies often insist that their IT departments do more with less.

“One thing we’re really hearing from our customers is this emphasis on business agility and the pressure to achieve 24-7 availability,” says Hickel. “These forces are pressing IT organizations to deliver better performance all the time. And they’re not looking at increasing IT budgets or manpower. That’s a complicated balancing act, and it’s often unsustainable in

the long run. Eventually, something somewhere in the system is going to experience a problem.”

Adding to the irony, when a problem occurs and a war room is necessary, having limited personnel resources can lengthen the troubleshooting and repair process, incurring that much more in terms of recovery costs.

Avoid the War Room: Prepare for War

While the war room will remain a specter that you will certainly confront at some point, you can take steps that can dramatically reduce your chances of experiencing serious downtime.

Most companies already have infrastructure monitoring solutions built into their IT environments, which is a good step toward overseeing operations from a technology-specific point of view. The challenge lies in extending that technology-specific monitoring to encompass the application, so that you are managing in a way that is meaningful and delivers value to the business. A holistic view gives you a better understanding of how the components of a business application or service work together, enabling you to proactively prevent downtime by finding anomalies and improving overall performance.

“As the application paradigms have evolved and have become constructed of all these different constituent parts, it’s important that the monitoring—starting at the component level and moving all the way up the stack—can correlate the information and show the big picture,” says Hickel. “I think most customers want to see how the infrastructure supports a service or application. We’ve seen an evolution in our customer base from purely monitoring technologies or applications to following business transactions across the infrastructure. These are the customers who can diagnose and prioritize problems most quickly.”

After implementing comprehensive system monitoring, companies can better pinpoint areas that could pose problems, and that data can help to build a troubleshooting checklist to better streamline the process if a war room must be organized. A checklist can also help craft policies and processes designed to quickly diagnose and prioritize problems on the fly.

Beyond system monitoring and testing, consider investing in a solution that monitors and manages application performance across the infrastructure. Middleware management offerings allow you to automatically and precisely pinpoint and diagnose

performance problems and quickly resolve composite application and infrastructure issues across complex environments. They can determine what and how many transactions or processes have been affected. Middleware management offers a valuable defensive tier for reducing the occurrence and duration of downtime and providing continuous monitoring of key transaction and process operations.

“Our customers ask us how they can not only do a better job of managing their infrastructure, but also how they can tie that management to their applications and ultimately deliver a higher value back to their business,” says Hickel. “Middleware management tools can really deliver in all those areas, and they can be customized to a wide range of IT infrastructures serving multiple industry segments.”

Less Room for the War Room

The sheer complexity of data centers practically guarantees some application, somewhere within the IT labyrinth will experience performance degradation or an outage at some point, so a war

room is a necessary option to keep on the table. However, with the right planning, monitoring and vigilance—and the appropriate hardware and software solutions—you can regard the war room as a weapon of last resort rather than the first one drawn.

By staying current with new technologies and implementing comprehensive system monitoring and application management solutions, you can minimize the potential for downtime and decrease the impact should a war room be necessary.

“The decoupled and asynchronous nature of many IT infrastructures, and the fact these technologies are being used to link unlike applications—those are the characteristics that increase the risk of downtime and complex troubleshooting,” says Hickel. “It’s definitely a challenge to monitor and manage it all, but it can be done with the right tools and planning. You won’t eliminate the war room entirely, but you can avoid a lot of the costs associated with it, if you’re prepared.”

Ryan Rhodes is a former managing editor of *IBM Systems Magazine*, *Mainframe edition*.