NETWORKComputing

Why IT War Rooms Fail, and Why Failure is No Longer an Option

When it comes to war rooms, make AI Ops and automation work for you – and leave to humans what humans do best.

By John Gentry Published: MAY 22, 2019

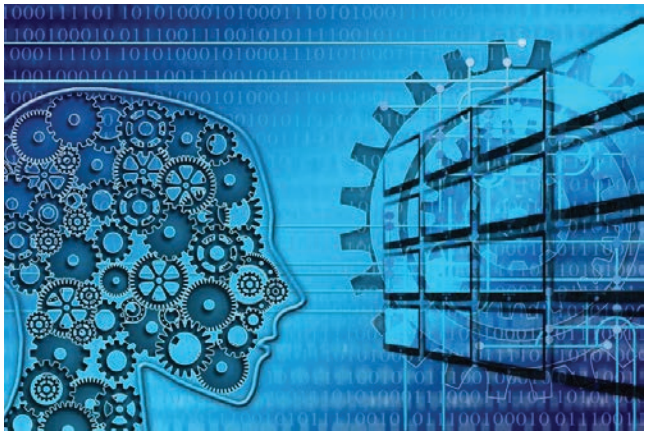
IT war rooms are nothing new. They've been around as long as industry has had IT issues and conference rooms in which to debate those issues.

Although today's war rooms are mostly virtual, their important role within IT has only increased. War rooms are beginning to mushroom, largely due to the growing complexity, scale and increased multi-vendor deployments of enterprise infrastructure. For one thing, the evolution of hybrid data centers allowed organizations to utilize cost-effective and flexible compute and storage via the cloud, while retaining the control and security provided by on-premises infrastructure. But with those gains, the scale and complexity associated with highly virtualized, hybrid and multi-cloud environments began to grow beyond human comprehension.

Complicating the problem is that enterprises often implement monitoring tools in a siloed fashion, with each department maintaining its own monitoring tools for servers, network, storage, cloud, applications, and databases. And each silo is organized and managed independently using performance metrics specific to the silo. Worse, department administrators may be unwilling – and often are – to expose the performance of their portions of the infrastructure to other silo administrators.

In such a decentralized environment, it's virtually impossible to gain a complete view of the health, utilization, capacity and performance of the underlying infrastructure supporting business-critical applications. And the monitoring tools used departmentally have no inherent "understanding" of the applications, their importance to the business, or the impact of the application workloads on the infrastructure.

Fragmented visibility inevitably leads to a lack of control over application delivery, which results in unmet service level agreements (SLAs), reactive IT, and unconstructive, silo-centric finger-pointing within IT war rooms. When this happens, costs and time-to-resolution escalate significantly, which directly impacts customers and company revenues.



Genesis of cross-silo monitoring

Ideally, war rooms lead their members to adopt a cooperative, cross-silo effort toward issue resolution. For example, when a problem arises, an IT administrator can conduct first-level triage and pinpoint where the potential problems lie. With tangible evidence of bottlenecks in their domains, other administrators can dig deeper into the performance of their own silos. Their goal, of course, is to detect and resolve a problem that occurs across silos. But what are the chances that a manual solution – that is, one that is not guided by artificial intelligence (AI) – can identify and pinpoint the root cause of the issue? In my years of monitoring infrastructure and its behaviors, I've come to two conclusions:

1) A problem often has no single root cause. It's often the result of a perfect storm of various issues such as

misconfigurations and changing workload behavior.

2) The root cause is something completely unrelated to the problem the team observes but shares some commonality with the underlying infrastructure.

To complicate matters, an issue may be remedied momentarily but ends up repeating itself over sporadic intervals – as it can when a bug is discovered and patched, but not isolated to its source and resolved. When that happens, resolution times can extend to days or weeks, or the issue can be patched repeatedly while the root cause remains a mystery.

"70% of War Rooms are responding to incidents whose underlying technical causes were not diagnosed and identified before those services were impacted," said Dennis Drogseth, VP of Research, Enterprise Management Associates (EMA).

What's more, the burdened-labor costs of running war rooms may be miniscule compared to the cost to the organization of unresolved outages, lengthy downtime, and even repeated performance issues. Lost revenues and negative impact to the corporate brand easily dwarf the lost productivity of the team in trying to identify and fix problems.

Artificial intelligence for IT Operations (AIOps), combined with real-time infrastructure monitoring, is becoming essential to proactive problem resolution. But not all AI or machine learning is created equal, and there is an increasing over-use of the terms without the depth of experience required to make them transformative. Simply throwing math at the problem is insufficient. Effective use of AI/ML, or what I prefer to call 'algorithmic intelligence,' must be informed by applied context and experience.

When an organization has an infrastructure management process in place, along with cross-silo monitoring and an AIOps platform informed by applied experience, the IT war room can deliver on its original promise: helping resolve infrastructure slowdowns or outages within minutes. When they do, war rooms fulfill their original promise of detecting, pinpointing and resolving issues rapidly. Today, AI/ML and automation are helping IT Ops teams restore services faster than ever before by identifying the probable root cause of an outage and correlating related events to pinpoint the solution.

With the help of the right insight and automation, organizations may choose to scale back the scope of their war rooms and the number of members required to run them – using tools to discover what humans cannot. Ultimately the goal should be to move beyond faster reaction and resolution to proactive problem avoidance and prevention. This is where the true value of machine learning can be leveraged in an AIOps platform. If there is a known or learned pattern to the symptoms leading up to an issue, an effective AIOps platform should recognize that pattern and apply the known resolution before any actual issue occurs.

Should war rooms be disbanded altogether? Probably not, because they can play a critical role that only humans can provide: notifying both internal and external stakeholders of an issue, communicating the context and implications of the issue, and notifying all stakeholders when the issue has been resolved.

"Having both senior executive presence and an ongoing/formal 'war room' with more well-defined processes also argues for success," added Dennis Drogseth of EMA.

In short, when it comes to war rooms, make AI Ops and automation work for you – and leave to humans what humans do best.