Report Summary – Unifying IT Decision-Making for Digital War Rooms

A DEEP DIVE INTO HOW TO SUCCEED IN THE AGE OF CLOUD AND AGILE

ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) Research
By Dennis Drogseth

April 2018

Sponsored by:

Moogsoft®

EMA™ IT & DATA MANAGEMENT RESEARCH, INDUSTRY ANALYSIS & CONSULTING

Report Summary – Unifying IT Decision-Making for Digital War Rooms: A Deep Dive Into How to Succeed in the Age of Cloud and Agile

Table of Contents

Report Summary – Unifying IT Decision-Making for Digital War Rooms: A Deep Dive Into How to Succeed in the Age of Cloud and Agile

Executive Introduction

The term “war room” has become a source of controversy and confusion. Many users in the industry like to point to the war room as a thing of the past, but this research indicates just the opposite. In the digital era, the war room has become more important—not less. It involves not only operations, but a wide range of other players as well, most notably IT service management (ITSM) teams, development, security, the IT executive suite, and even business stakeholders.

Of course, a lot depends on how one defines “war room.” Is it merely the dregs of a reactive landscape, where a whole host of siloed experts point fingers at each other while critical business services remain unavailable and business performance tanks? Indeed, war rooms are often defined as disastrous assemblages of finger-pointing adults caught up with siloed versions of “the truth”—all at least as interested in proving that their teams are “not guilty” as they are in actually solving the problems at hand.

Fortunately, that’s not the case as shown in this research.

This is partly because EMA took a much more open-ended approach for this investigation. The goal was to find out how teams are formed and optimized to handle major incidents and problems that require cross-domain insights. This evaluation included proactive cross-domain teams for managing issues before they become the IT equivalent of life-threatening.

As EMA examined them, war rooms can be physical, virtual, or hybrid—which turned out to be the predominant case. They can be highly automated or not, or made up of consistent, well-defined teams or not. What made them war rooms in all cases was the need for collaborative decision making across silos, and the need for urgency and efficiency in taking effective action.

As EMA examined them, war rooms can be physical, virtual, or hybrid—which turned out to be the predominant case. They can be highly automated or not, or made up of consistent, well-defined teams or not.

This report will examine the war room problem from multiple dimensions. These include roles and responsibilities (from operations to DevOps), emerging organizational patterns, technology priorities, toolset adoption and toolset issues, metrics and success rates, and patterns that indicate success or, conversely, might otherwise lead to failure.

Some of the highlights from the findings were as follows:

- In the digital era, war rooms are becoming more formalized and established overall rather than less formalized and established.
- The average headcount for digital war room team involvement is 15, and the trend is toward greater involvement.
- Seventy percent have a single organizational owner for the digital war room, with ITSM and the executive suite leading.
- Eighty-eight percent of respondents indicate that operations teams work closely with ITSM teams to enable war room decision-making.
- Fifty percent of respondents answered that effective war room capabilities are becoming more important in the digital era. Only six percent saw the war room becoming less important.
- Fifty-two percent of war rooms were hybrid (roughly 50/50 physical and virtual); only 17 percent were primarily virtual.
- Seventy-five percent of respondents feel their war rooms were transformed through automation, analytics, or both.
- On average, about 30 percent of incidents are diagnosed before they cause outages or business disruptions—and when this happens, 91 percent see the war room as being involved.

- When EMA asked about the average time to *assemble an effective team*, the average response was about 1.5 hours. When asked about *total time to resolution*, the average response was about six hours.
- On average, respondents indicated they were using 2.4 different toolsets to find and notify critical stakeholders of serious incidents. The leading two were *automated IT alerting systems* and *(direct) communication with senior management*.
- This research indicates that development is already playing a major role in the digital war room, often (in 37 percent of the cases) becoming more involved.
- Fifty percent of respondents claimed that cloud made digital war room decision-making easier, but 43 percent said cloud made things harder in the war room.
- *Advanced IT analytics*, *SIEM*, and *security threat intelligence and analysis* led as the top three technologies for war room decision-making.
- *Security-related issues, inconsistent or inaccurate data,* and *fragmented data* led as the top obstacles to war room success.

Methodology and Demographics

EMA conducted this research in the winter of 2018 across 272 respondents, with 152 in North America and 120 spread evenly across England, Sweden, and France. Company sizes were overall balanced across small, medium, and large, starting with those 250 and above.

Some of the other demographic highlights from the research were as follows:

- Lead verticals were *high technology software, finance and banking, high technology service providers and MSPs, manufacturing,* and *retail*.
- The average IT budget was about $30 million, but 15 percent of respondents had a budget of $100 million or more. Seventy-seven percent showed an annual budget increase.
- Twenty-two percent were directors or higher-ranked in IT with, eleven percent working as CIOs. Fifteen percent were non-IT business stakeholders, with titles ranging from *CEO* to *corporate line of business vice president* to *digital marketing officer*.

The key requirement for participating in the research was involvement in digital war room decision-making. Most of the respondents (81 percent) indicated *ongoing* or *regular* levels of war room involvement.

Organization

One of the key areas of interest in developing this research was to determine the status of the war room in small, medium, and large enterprise environments.[1] Figure 1 shows how a more formalized and established team is clearly the trend over a less formal arrangement.

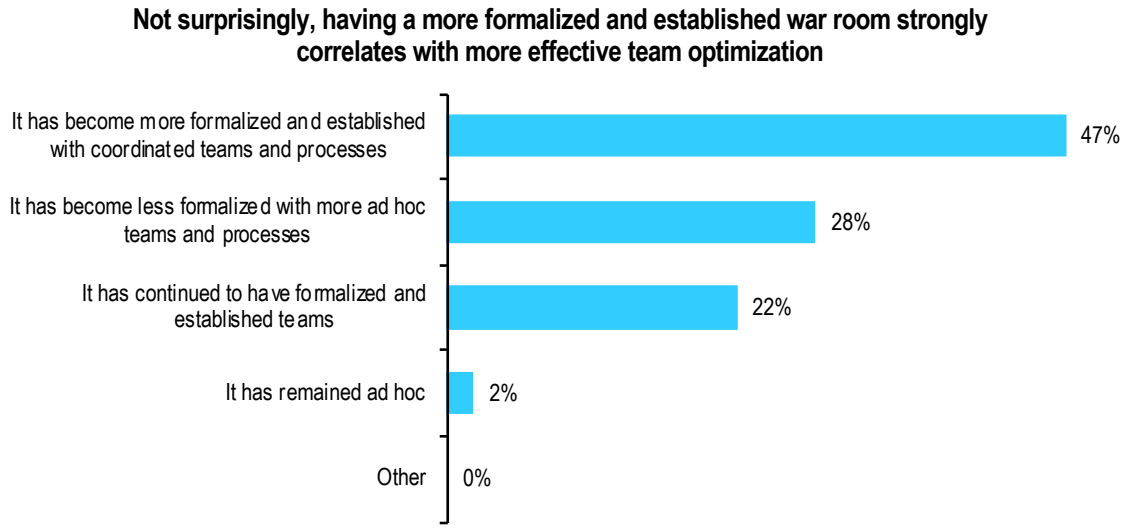

Figure 1: In the digital era, war rooms are becoming more formalized and established overall rather than less formalized and established. This is especially true of larger enterprises rather than small businesses, but the differences there remain modest.

Not surprisingly, having a more formalized and established war room strongly correlates with more effective team optimization, as well as more effective results for incident resolution overall. Some of the other dimensions of the digital war room today are:

- Across small, medium, and large enterprises, the average headcount for digital war room team involvement is 15, with 32 percent averaging 20 or more people involved.
- The trend is toward greater involvement, with 52 percent seeing more people involved, and only three percent seeing war room headcount reductions. Having more people involved also aligns well with improved war room effectiveness.

When asked if there was a single organizational owner for the digital war room, 70 percent of respondents answered “yes.” Not surprisingly, having a consistent and ongoing war room owner correlated strongly with both overall war room effectiveness and more effective team optimization. ITSM teams led in owning and coordinating war room efforts, followed by the IT executive suite, with a total of 50 percent ownership between them.

Having a more formalized and established war room strongly correlates with more effective team optimization.

1 EMA included some MSPs as well, but the differences were generally quite modest.

The notion that war room collaboration is fundamentally siloed seems to be untrue, given what respondents indicated in Figure 2. The average respondent took on almost four (3.62) roles in supporting war room decision-making, with ITSM in the lead, but with fairly close consistency throughout.

The notion that war room collaboration is fundamentally siloed seems to be untrue, given what respondents indicated in Figure 2.

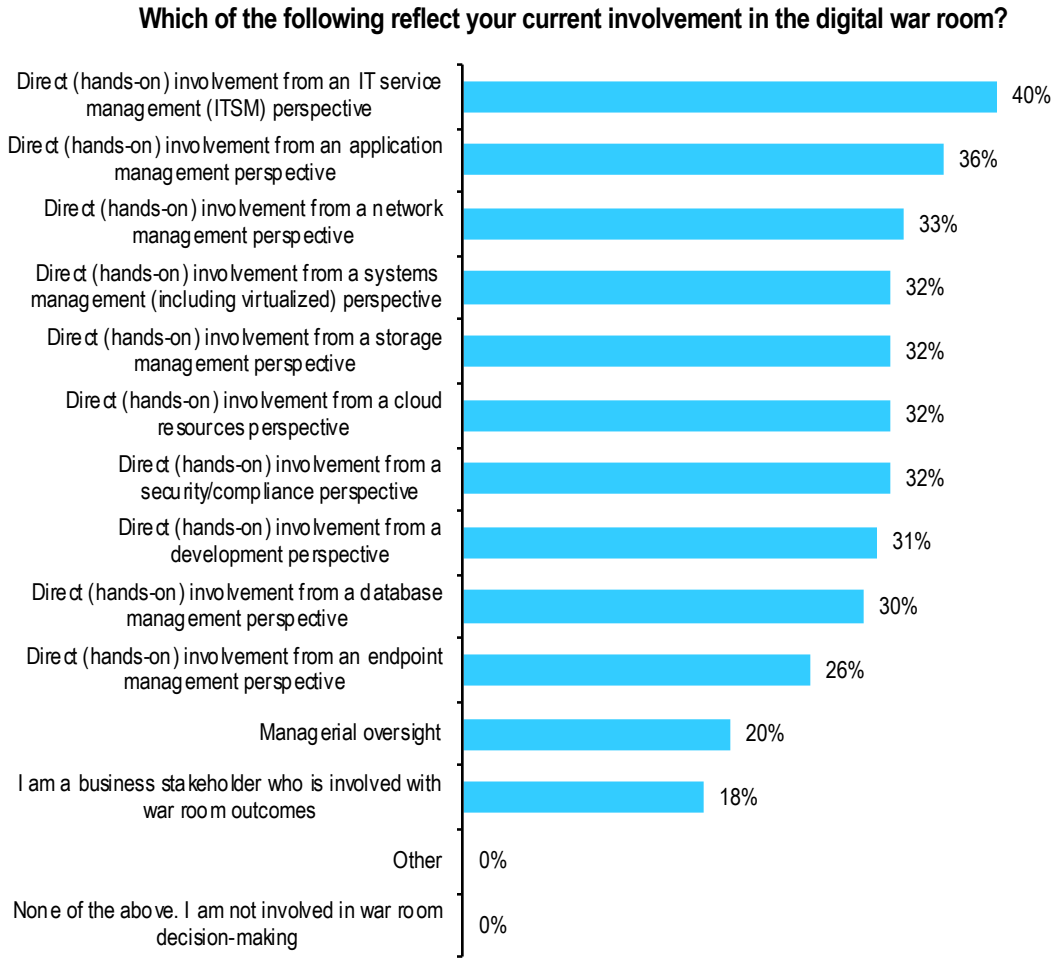

Figure 2: Respondents indicated that assuming multiple roles for war room decision-making has become normal in IT, with an average of 3.62 roles per respondent, and close alignment of areas of interest throughout. This is a sign, at least potentially, of progress in breaking through fragmented patterns of decision-making.

Some Key Strategic Perspectives

In seeking to formulate critical war room priorities, EMA targeted several areas of strategic difference. Perhaps the single most important question was a simple one: Is the digital war room gaining or losing importance? This question targeted the often-heard idea that the war room is going away, or that the war room is a thing of the past. However, while EMA hopes it's the case that war rooms in the most traditional, stereotypical mode of operation—with rampant finger-pointing and minimal effectiveness—are fading away, the role of the digital war room as a center for critical incident handling seems to be on the rise.

- Fifty percent of respondents answered that effective war room capabilities are becoming more important in the digital era
- Forty-three percent saw them staying at the same level of importance
- Fewer than six percent saw them as becoming less important (two percent had no opinion)

Perhaps it's no surprise that viewing effective war room capabilities as becoming more important aligns well with overall war room success.

The next question targeted another area of general concern—to what degree are war rooms becoming more virtualized? The answer, especially when mapped to success rates, was also telling.

- Thirty-one percent of war rooms remain primarily physical
- Only seventeen percent are primarily virtual
- Fifty-two percent are hybrid (roughly 50/50 physical and virtual)

In other words, the move to a totally virtual war room still seems elusive. Moreover, when mapped to success, primarily virtual war rooms were least effective in bringing major incidents to a timely resolution. Those mixing physical and virtual in hybrid war rooms were the most effective.

Another strategic arena for war room change was seen when gauging the impacts of technology adoptions, especially those involving analytics and automation as shown in Figure 3.

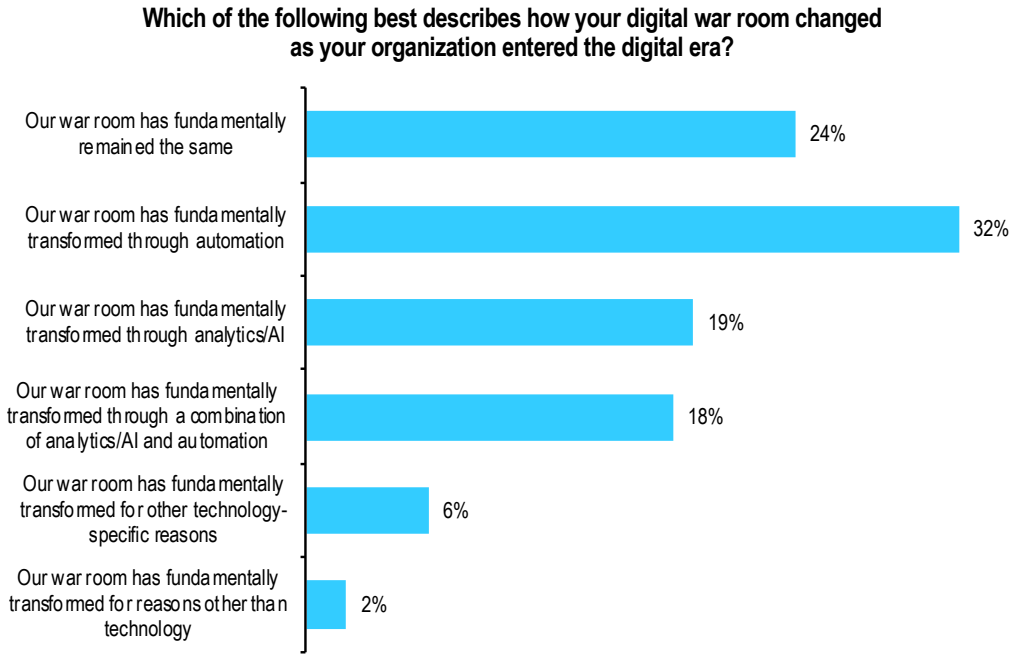

Figure 3: This data shows that 75% of respondents feel their war rooms were transformed through automation, analytics, or both, or for other technology-driven reasons. Only 2% feel their war rooms have been fundamentally transformed for reasons other than technology.

Is the Digital War Room Proactive or Reactive?

The next area of strategic inquiry was targeted at whether digital war rooms are only reactive, last-measure enclaves, or whether they provide a proactive resource for addressing major incidents before they impact the larger user community. The firm answer is that only one percent of respondents were totally reactive, and 33 percent addressed more than 40 percent of their incidents proactively.

Processes (or Lack Thereof)

In order to better understand how digital war rooms work (or don't), EMA defined five core processes. These were:

- *Initial awareness*, which events or some other type of automated intelligence usually drive, or complaints to the service desk.
- *Response team engagement and coordination*, bringing relevant stakeholders together and providing a context for them to work together.
- *Triage and diagnostics*, where problems are understood in context and then *insert noun here* can define detailed requirements for remediation.
- *Remediation*, where war room teams make active fixes to major incidents, often through change and configuration management procedures.
- *Validation,* in which testing is done to ensure that actions for remediation were successful, ideally from a business impact as well as a purely technical perspective.

This process architecture became a foundation for multiple questions.

EMA found that, on average, IT organizations are defining only 50 percent (2.57) of the relevant processes for their digital war rooms, with response team coordination in the lead. This suggests a need for more active industry education and awareness.

Although the differences weren't great, the digital war room teams who claimed they were most successful in overall incident resolution, as well as those most successful in optimizing team participation, had more processes defined than the others. The ratios were:

- 3 for the *extremely successful*
- 2.5 for the *somewhat successful*
- 2 for the only *marginally successful*

Time, Tracking, and Incident Management

Time can be the biggest factor in effective war room procedures. When EMA asked about the average time to *assemble an effective team*, the average was about 1.5 hours, which could, of course, be meaningfully damaging when a serious outage occurred. When asked about *total time to resolution*, the average was about six hours, but 20 percent took more than eleven hours. Once again, as an average, this can be concerning for incidents with major business impacts.

When asked about total time to resolution, the average was about six hours.

When it came to *tracking and auditing* to improve war room performance, 65 percent claimed they did this consistently, and 33 percent claimed to do it only sometimes. A mere two percent said they never do it. Those who were extremely effective in optimizing war room performance were far more likely to track and audit their efficiencies than other groups.

EMA also wanted to know how well the role of *incident managers* is defined in current war room environments. Our data shows that incident management is the leading process for managing overall war room interactions. Only 21 percent indicated that there was another role associated with coordinating war room team response and efficiencies, and those respondents tended to cluster in smaller enterprises. Moreover, having an incident manager, or an incident management team, strongly correlated with overall war room effectiveness, as well as in war room team optimization.

Technology Priorities for Alerting and Optimizing War Room Teams

EMA didn't want to stop at looking at the processes alone, but also wanted to clarify the technology choices companies used for alerting, assembling, and empowering war room teams to work together. The answers showed a complex list of options, suggesting both active exploration and an ongoing need for innovation.

When asked about the initial process of identifying relevant stakeholders and resolvers, an automated IT alerting system scored the highest, as can be seen in Figure 4.

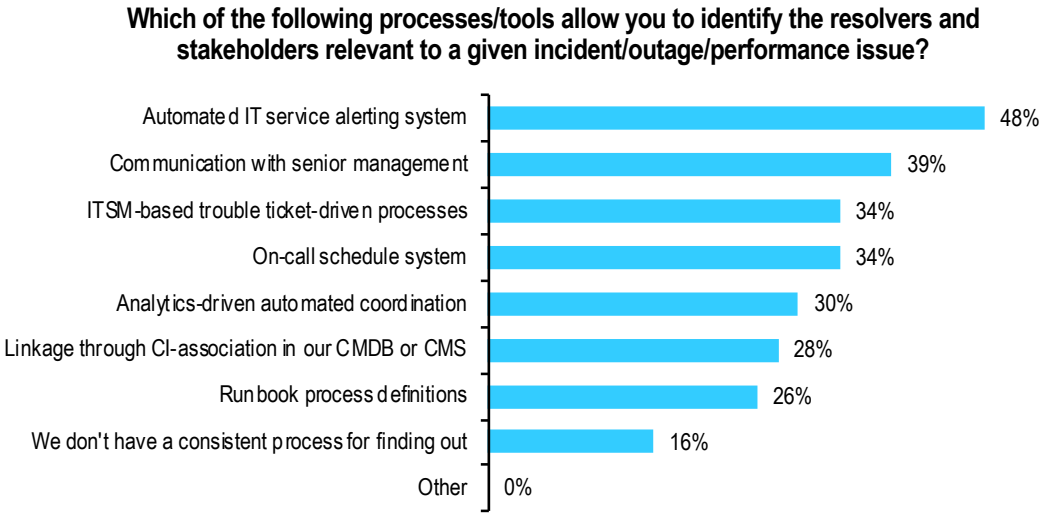

Figure 4: On average, respondents indicated using nearly two and a half (2.4) different toolsets to find and notify critical stakeholders of serious incidents. The leading two were automated IT alerting systems and (direct) communication with senior management. The latter, in particular, suggests incomplete levels of automation and awareness as a kind of search-and-find process.

Applications and DevOps

One of the most critical areas of interest for EMA was the advancing role of agile and DevOps in impacting traditional war room behaviors and priorities. EMA wanted to know if development was bypassing the digital war room or becoming more engaged.

Figure 5 shows that a significant number (37%) indicated that development was becoming more involved. There was also a strong alignment between development becoming more involved and those who were extremely effective in optimizing war room outcomes.

One of the most critical areas of interest for EMA was the advancing role of agile and DevOps in impacting traditional war room behaviors and priorities.

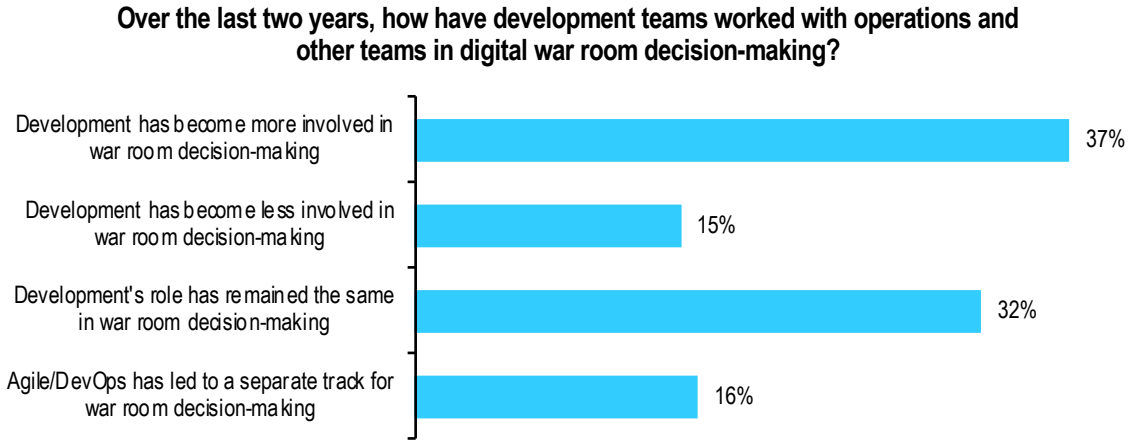

Figure 5: EMA research indicates that development is already playing a major role in the digital war room, while often becoming more involved.

General Technology Requirements

EMA was also interested in seeing exactly which technology adoption priorities were leading among existing war room teams and buyers, directed here primarily at the last two processes: *triage/ diagnostics* and *validation.*

Figure 6 provides a long list of options with advanced IT analytics at the top, but with a very gradual gradient showing how closely many technology priorities are aligned.

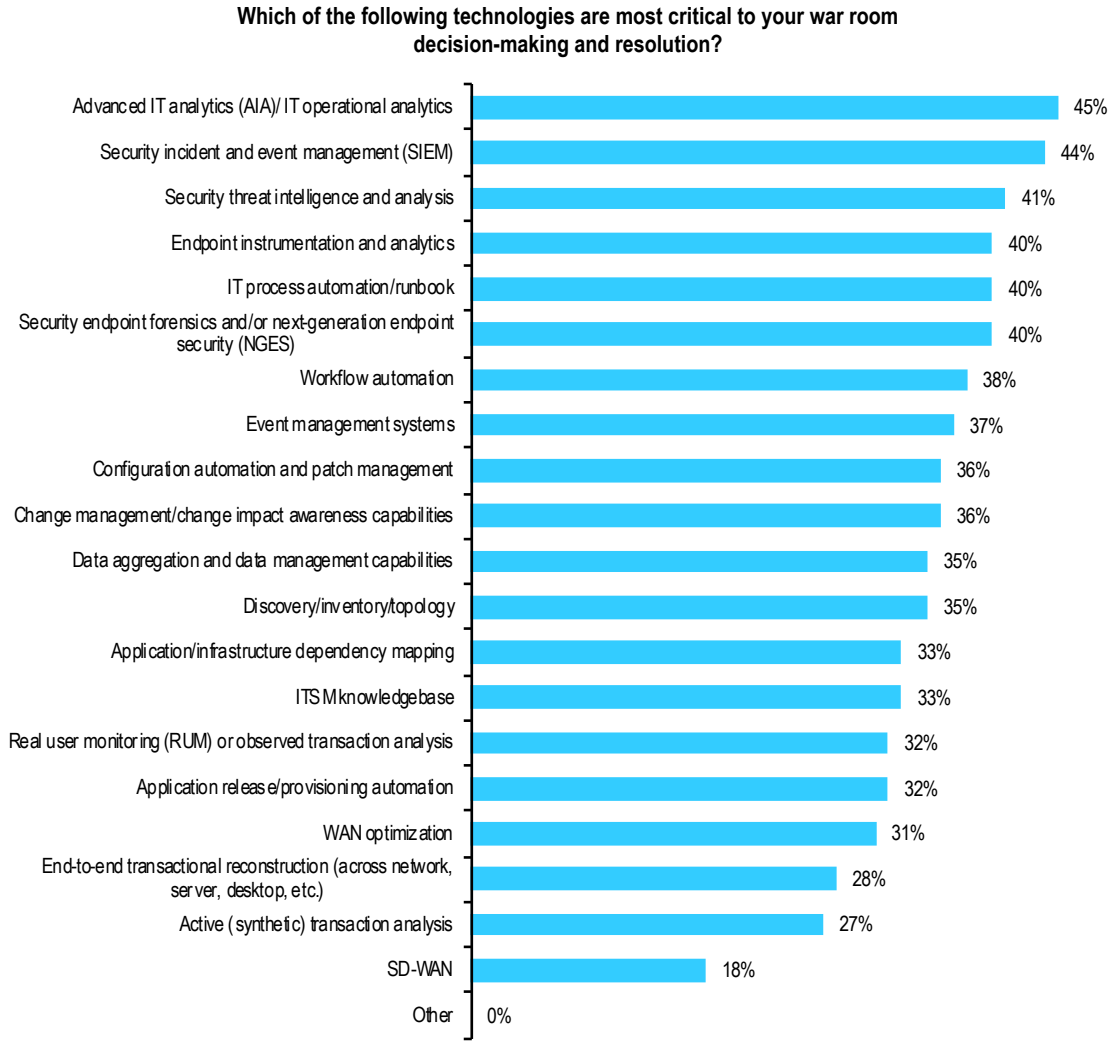

Figure 6: Advanced IT analytics, security information and event management (SIEM), and security threat intelligence and analysis led as the top three technologies for war room decision-making.

War Room Metrics and Obstacles

In order to move forward by measuring their progress, digital war room teams need to leverage effective metrics in seeking diagnostics and measuring their overall effectiveness. In Figure 7, *mean time to restore* and *mean time to collaborate* were the two least invoked metrics, indicating that priorities sat squarely on diagnostics and triage among respondents.

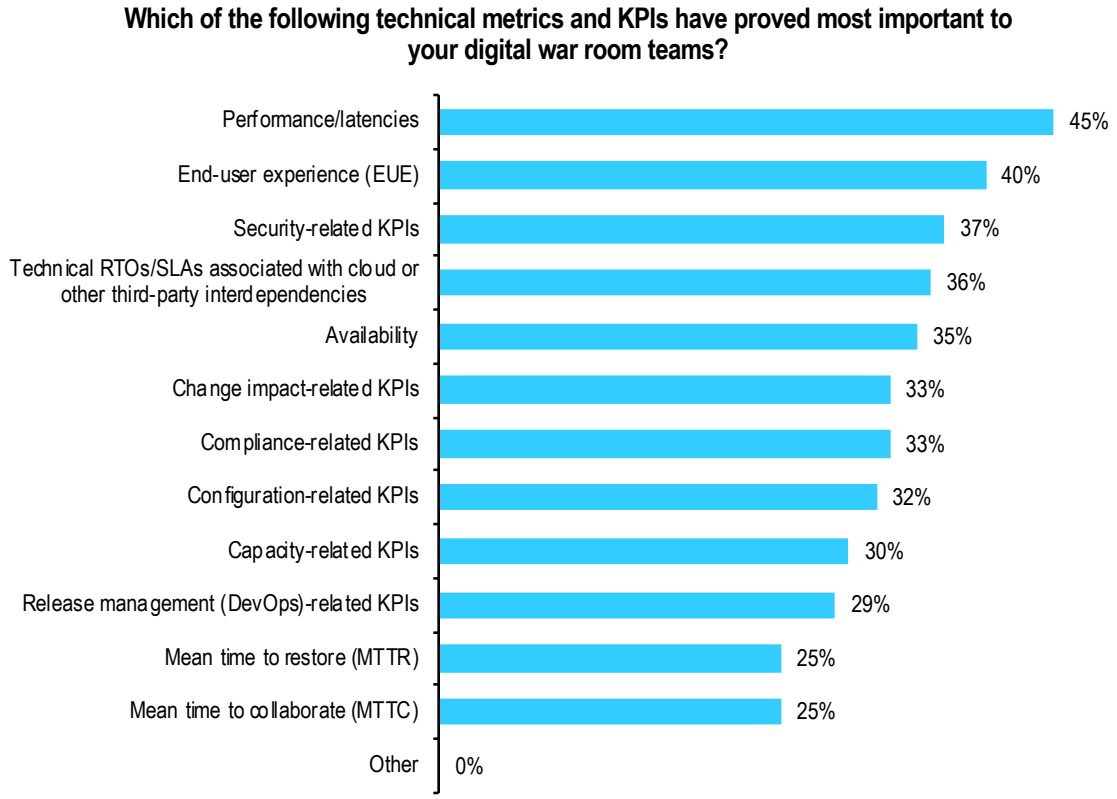

Figure 7: Metrics are critical to war room success. Performance latencies and end-user experience top the list for their critical diagnostic values. The average response indicated usage of about four technical or performance-related metrics per war room.

When it came to business-related metrics, *team performance* and *employee productivity* were ranked highest. The top five were:

1. IT team disruption (36%)
2. Employee productivity (31%)
3. Industry compliance-related metrics, tied with cost-related external SLAs (with service providers) (27%)
4. Service desk OpEx cost savings (26%)

When asked about the most significant obstacles impacting effective war room performance, the top seven were the following:

1. Security-related issues (34%)
2. Inconsistent or inaccurate data, tied with data fragmentation/separate views in separate silos (32%)
3. Reactive versus proactive insights (31%)
4. Lack of automation, complexities due to cloud-related resources, and cultural and political issues within IT (all tied at 29%)

EMA consistently sees data issues as a major roadblock to many initiatives, impacting virtually all other outcomes, and often reinforcing siloed views versus more unified, cross-domain insights. Security issues are also clearly on the rise, as can be seen throughout many of the findings in this report. And finally, automation is key in accelerating awareness, team-building, diagnosis, and remediation.

Conclusion

The notion that the war room is a thing of the past would seem, itself, to be very much a thing of the past. The data here speaks out strongly as to why, but logic can also come into play—and the reasons are multiple.

The notion that the war room is a thing of the past would seem, itself, to be very much a thing of the past.

First of all, in many cases, IT silos still remain fairly siloed. Pure-play efficiencies across IT teams on an ongoing basis are still a longed-for result, not a present-day reality. In the face of this still very real present-day reality, the need for a disciplined, well-focused, cross-domain team to handle major incidents remains ongoing.

Secondly, while technologies are advancing, no single suite or solution can be expected to be a cure for the unplanned. IT teams still face ongoing challenges in dealing with cloud, agile, security needs, and the pressures of IT and digital transformation.

Finally, what's becoming apparent from the data in this report is that the digital war room is evolving, or at least *can* evolve, to become a proactive resource to help IT become more responsive to changing IT and business needs. The digital war room can ensure that both unplanned and planned disruptions can be effectively accommodated, while building a community of stakeholders attuned to the accelerating demands of agile, business transformation, and cloud assimilation and optimization. In this new era, the war room then becomes a place where the speed bumps from new business processes and business and IT initiatives can be accommodated, addressed, and ultimately minimized. In this sense, the digital war room stands in the spotlight as a representation of a new, more dynamic, informed, and automated IT.

EMA Perspective on Moogsoft AIOps

Moogsoft AIOps was designed with the single-minded focus to enable IT operations, site reliability, DevOps, and application support teams to industrialize their ability to manage complexity and change. As such, Moogsoft AIOps stands out as an industry leader in both understanding and empowering virtually all the processes surrounding digital war room success.

Some of Moogsoft's standout values include:

- Moogsoft AIOps analytics deliver unique strengths in correlation, anomaly detection, machine learning, and self-learning heuristics. The Moogsoft AIOps inference engine allows concise, actionable situations to be drawn from millions of data points in real time. The inference engine deduplicates events, analyzes entropy (i.e., prioritizes non-recurring events), breaks messages down into tokens and words for whitelisting and blacklisting analysis, and then correlates events.
- Moogsoft AIOps effectively integrates automation with its analytics and "Situation Room" diagnostics. Once a situation is created, Moogsoft AIOps builds a unified workflow to support its Situation Room team collaboration. Then, based on the resolving steps, Moogsoft AIOps can be configured to automate future actions based on similar situations, or "Situation Mapping."
- Moogsoft AIOps' algorithms identify the team members who were instrumental in resolving a given issue, creating a roster for future situations with the same characteristics. In other words, the software identifies and assigns situations to experts from across teams to quickly resolve them.

Problem isolation and triage can occur across the entire IT data center and/or cloud infrastructure. Using sophisticated algorithms to aggregate and analyze millions of events in real time and correlate them into clustered "situations," Moogsoft dramatically reduces the mean time to detect (MTTD) of service-impacting incidents and reduce the mean time to remediate (MTTR) by helping operators hone in on probable root cause.

With no rules to define, and no business logic or configuration and topology models to create and maintain, the administrative impact to data center staff is minimal, so additional workloads could be absorbed with no need for additional operations headcount.

With Moogsoft, there are significantly fewer surprises. AIOps feeds into our automated notification software, and it even helps pull together the right people for incident response management teams, when needed. In addition to a lower MTTR, our P1 incidents have decreased by 60 percent since Moogsoft was rolled into production.

EMA interviewed an international bank.

About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (EMA) is a leading industry analyst firm that provides deep insight across the full spectrum of IT and data management technologies. EMA analysts leverage a unique combination of practical experience, insight into industry best practices, and in-depth knowledge of current and planned vendor solutions to help EMA's clients achieve their goals. Learn more about EMA research, analysis, and consulting services for enterprise line of business users, IT professionals, and IT vendors at www.enterprisemanagement.com or blogs.enterprisemanagement.com. You can also follow EMA on Twitter, Facebook, or LinkedIn.

Corporate Headquarters:
1995 North 57th Court, Suite 120
Boulder, CO 80301
Phone: +1 303.543.9500
Fax: +1 303.543.7687
www.enterprisemanagement.com

3695-Moogsoft_SUMMARY.060618