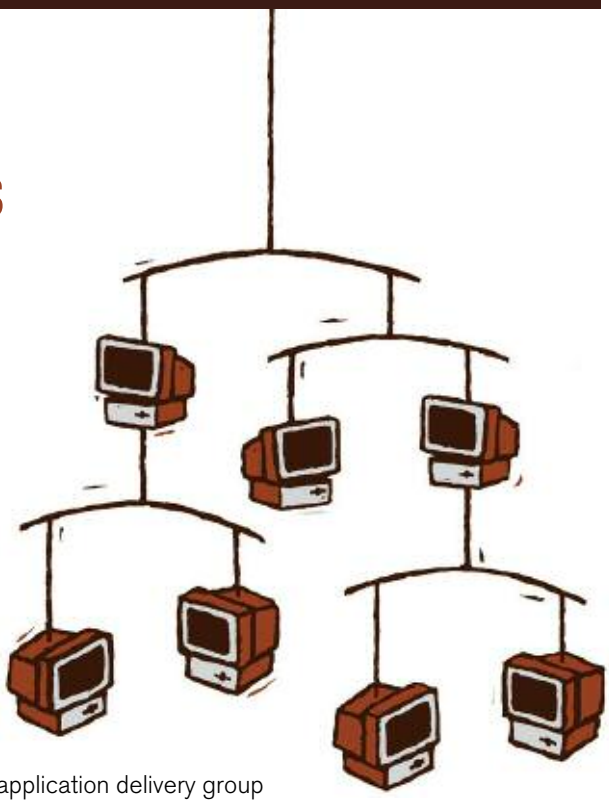
The Mandate to Integrate Operations



Jim Metzler
Ashton, Metzler & Associates
jim@ashtonmetzler.com

Introduction

One of my professional fantasies is that if you have a job in IT, then it is easy to recognize which function your role supports: you either support application development or you support application delivery. Key to this fantasy is that each member of the IT organization works in concert with other members of IT to ensure application availability and responsiveness. I say this is a fantasy because that situation isn't the case today for virtually any IT organization that I work with. To put that in context, let me explain my fantasy in a little more detail. To do so, I will use a hypothetical discussion between the application development group and the application delivery group at Acme Inc. The discussion begins in the early stages of developing a new application when Acme's development group meets with Acme's delivery group to discuss the new application. In my experience it is very rare for the development group to meet with the delivery group early in the application development lifecycle. As such, this hypothetical conversation is part 1 of the fantasy.

As part of the discussion, Acme's application development group points out that they intend to use EMC's Documentum for content management. Part 2 of the fantasy is that Acme's application delivery group has a good enough grasp of application performance in general and EMC's Documentum in particular to be able to point out that Documentum typically does not run well over a WAN. Part 3 of the fantasy is that the application development group actually takes the input of the application delivery group into consideration. For the sake of this example, let's assume that the development group has compelling reasons to go forward with using Documentum and informs the delivery group of their decision. Part 4 of the fantasy is that Acme's delivery group then determines what it has to do holistically from both a planning and an operations perspective to ensure acceptable application performance.

The goal of this IT Impact Brief is to discuss what it would take from an operations perspective to have my fantasy for IT become real. To do that, I will discuss how the role of the network manager has been changing and will draw upon a couple of recent IT Impact Briefs.

The Early Days

I can remember teaching graduate level data communications back in the early 1980s and I would spend a lot of class time detailing protocols such as RS-232[1]. Not only would I spend time on it, I would go over the meaning of each pin. While I certainly hope that no graduate level data communications course spends time on such arcane topics today, it was reasonable to do so in the early 1980s. I say that because back at that time there were two primary characteristics of the role of the network manager. One characteristic was that it focused almost

[1]RS-232 (Recommended Standard 232) is a standard for serial binary data signals connecting between a DTE (Data terminal equipment) and a DCE (Data Circuit-terminating Equipment).

exclusively on the network. For example, in the early 1980s the network manager was not concerned with firewalls and spent virtually no time worrying about the performance of an application. The other key characteristic of the job was that its focus was on the physical elements of the network. For instance, I recently spoke to a network engineer who stated that in the late 1980s and early 1990s there was no guaranteed network availability in large part because the network often broke down. He added that virtually his entire focus at that time was on the physical plant and that he spent a large part of his time running around fixing cabling problems. He pointed out, however, that the network currently runs well and hence consumes much less of his time.

More Recently

As recently as five or six years ago the situation had not changed that much as a major component of the role of a network administrator was still to ensure the availability of the network. This narrow focus on the role of the network administrator was reinforced in part by the overall business environment. In particular, shortly after the terrorist attacks of September 11, 2001 (9/11) companies began placing tremendous focus on cost containment. Around the same time, the dot com era collapsed and companies began to seriously question the business value of IT. One of the industry leaders who encouraged this line of thinking was Nicholas Carr. In both an article in the Harvard Business Review[1] as well as a subsequent book, Nicolas Carr stated, "IT has become a commodity. Affordable and accessible to everyone, it no longer offers strategic value to anyone."

As a result of the dot com implosion and the subsequent focus on the reduced value of IT, the majority of senior business managers began to regard IT in general, and the network in particular, as a utility. Part of the perception that the network is a utility means that senior business managers expected little more from the network other than that it exhibit features such as high availability.

Given this emphasis on the network as a utility, one of the primary roles of the network manager at this time was to minimize the amount of time that it took to restore the network if there was an outage. In a recent IT Impact Brief entitled "Rethinking MTTR", I highlighted the fact that traditional fault management of network devices is notably easier than managing application performance. The point being that the need to deal with the complexity associated with managing application performance is one of the major factors driving the need for IT organizations to implement an effective integrated operations function.

[1] "IT Doesn't Matter", Nicholas G. Carr, Harvard Business Review, May 2003

Today's Environment

The IT environment has changed significantly over the last few years. One significant change is we don't hear much discussion these days that IT doesn't matter. Most of the IT organizations that I work with are busy on a wide range of activities, and in general these activities have more business rationale than did the projects that were driven by the irrational exuberance of the dot com era. For example, in the last IT Impact Brief I quoted an IT services director who stated that at one time his organization could justify an investment in management tools just based on their intuition that the tool would pay for itself. That is no longer the case as his organization now has a very formal process for evaluating return on investment (ROI). In contrast, during the dot com era many IT organizations were chartered by their company to implement a number of eBusiness initiatives and the mentality at the time was that IT organizations should not take a lot of time to plan these initiatives or else the company's competitors would overwhelm them.

Another way that the environment has changed is that most IT organizations have begun to place growing emphasis on ensuring acceptable application delivery. In fact, in a recent survey the NetScout community indicated that the area that will have the biggest impact on IT resources over the next year is improving the ability to ensure acceptable application performance.

However, getting back to the fantasy that I outlined at the beginning of this brief, I don't know of any IT organizations that truly have implemented an application delivery function. Virtually all of the IT organizations that I know, however, do have an infrastructure function. The difference is more than just a choice of words. As described above, an application delivery organization works holistically to ensure acceptable application performance across all of the components of IT. An IT infrastructure organization is usually made up of siloed groups. By siloed groups I mean that these groups work largely in isolation from each other and lack a common set of goals, vocabulary, tools and processes. The problem with this approach is quite clear – almost any component of IT could cause application degradation. Running the operations groups in silos increases the Mean Time to Repair whatever it was that caused the application to degrade. In addition, since we continue to add new functionality to the infrastructure (i.e., Wi-Fi, virtualization), over time the number of silos increases and hence the MTTR tends to increase.

To truly break down the siloes means that IT organizations need to implement an integrated

operations function. This is not a new concept. In fact, I believe that we have made a lot of progress over the last few years relative to achieving this goal. In my view many IT professionals with the title of network manager, network engineer or network administrator currently have responsibilities that go far beyond the network. For example, the network engineer that I referenced earlier stated that within his company there is a coming together of security operations and network operations. He pointed out that at the same time the network administrator is monitoring traffic looking for malware such as trojans or worms, the network administrator should also be monitoring for content violations to ensure that the organization is complying with regulations such as SOX (Sarbanes-Oxley Act) and HIPAA (Health Insurance Portability and Accountability Act).

The Stumbling Blocks

The good news is that in at least some IT organizations, the network operations group has ongoing responsibility for many facets of IT in addition to the network. This includes application performance, servers, security and storage. Unfortunately in most cases that I am aware of this morphing of roles has happened largely organically. By that I mean that the role of the network manager has typically evolved incrementally without an overall direction created and agreed to by senior management. The downside of the organic approach is that successfully implementing an integrated operations function is quite complex as it requires tools and processes that transcend the normal technology and organizational boundaries.

To put this in perspective, roughly a year ago I gave a survey to over 200 IT professionals. In one of the survey questions, the survey respondents were given a list of possible impediments and were asked to indicate which two were the most significant impediments to effective application delivery. Table 1 indicates the three impediments that received the most responses.

Impediment	Percentage
The processes that we have are inadequate	39.9%
The difficulty in explaining the causes of application degradation and getting any real buy-in	35.1%
The tools that we have are inadequate	32.7%

Table 1: Impediments to Application Delivery

As shown in Table 1, two of the three primary impediments to effective application delivery were inadequate tools and inadequate processes. In addition, part of the difficulty in explaining the causes of application degradation and getting real buy-in stems from the lack of tools that can effectively and conclusively identify the root cause of the degradation.

In terms of tools, one of the primary tasks that IT organizations must do is to establish a strategy for instrumenting the network to gather data that can be used for both real-time monitoring and historical reporting. This strategy must provide the IT organization with the ability to:

- Gather management data from a wide range of sources
- Gather granular, consistent, and accurate data
- Enable in-depth packet analysis
- Monitor application response times
- Implement effective analytics that can identify performance and security anomalies

Relative to process enhancement, one of the ways that IT organizations attempt to implement more effective processes is by adopting a services framework such as IT Infrastructure Library (ITIL). Roughly a year ago I wrote an IT Impact Brief entitled "The Movement to Implement ITIL".

In that brief I included the results of a survey question in which we asked the NetScout community if their IT organization was moving to an ITIL-oriented approach to IT services. Their answers are shown in Figure 1.

Figure 2: The use of ITIL

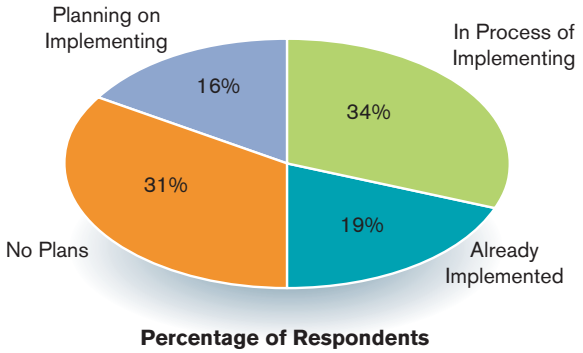


Figure 1: The Use of ITIL

The data contained in Figure 1 demonstrate the great interest that the NetScout community has in implementing an ITIL-oriented approach to IT services. As I also pointed out in that brief, the NetScout community was particularly interested in service support processes such as incident management, problem management and change management. Putting Table 1 and Figure 1 side by side presents an optimistic picture. That picture is that IT organizations know that they need to improve their processes and many of them are using the ITIL framework as a way to improve those processes.

My only concern is that the last time I went down this path it had various names such as TQM (total quality management) and six-sigma. I am not saying that those initiatives didn't provide some value. What I am saying is that those initiatives were over-hyped and in many cases delivered a lot less than were promised. It is too early to say if that will happen again with ITIL. What I do know is that the IT organizations I talk to on the topic are mixed about the value of ITIL with the optimists outnumbering the pessimists, but not by a huge margin.

Summary and Call to Action

I used to work with a network management vendor whose approach to network management was summarized by a t-shirt they used to distribute that said, "It's not the network stupid". I failed to convince that client that while that motto was pithy, it represented an outdated approach to operations. I say it is an outdated approach because it tends to reinforce the siloed approach to operations that most IT organizations are struggling to move away from.

In the introduction to this brief, I stated my fantasy about the two roles of the people who work in the IT organization. I strongly believe that an effective integrated operations function is a requirement if we are ever to reach the state where IT organizations do indeed consist of two functions: application development and application delivery. I believe this in part because without an effective integrated operations function, IT organizations will struggle to reduce the MTTR associated with application degradation. However, while it is relatively easy to create an integrated operations function, it is not easy to implement one that is truly effective. In particular, I don't think that IT organizations will enjoy those benefits of an integrated operations function without creating a plan.

Clearly a major component of the integrated operations plan has to focus on improving the processes both within the operations function as well as between this function and the other components of IT. Right now, ITIL is the framework of choice for many IT organizations that are working to improve their service support processes. I am cautiously optimistic that by using ITIL IT organizations will make at least some improvement to their key processes.

Another major component of the integrated operations plan has to focus on how the IT organization will instrument the infrastructure. Ideally this component of the plan is developed in conjunction with the efforts to re-design key processes. In particular, only after the IT organization knows how it wants a key process (i.e., change management) to flow across the entire IT infrastructure can it determine what information it needs to make this happen, and hence what management data it needs to capture in order to create that information.