Challenges in Event Management

JASON PAREE

Jason works for CACI Inc. as the release and deployment process owner for US CENTCOM J6. His position requires managing change as well as responding to and controlling outages and issues on live, operational networks. He received his BS in criminal justice administration in 2011 but switched career goals and is currently an MBA student. jasonparee@gmail.com.

Inherent to providing and managing IT services is having to deal with occasional outages, issues, and security concerns. These types of events, while inevitable even on the most reliable networks, can wreak havoc on a service provider's reputation if not handled and communicated properly. Customers of IT typically do not understand the guts of providing service. They know they turn on their computer, open Word, surf the Internet, or communicate using email and chat. In general, they do not understand nor do they usually care what makes it work. This changes, however, when those services suddenly stop working. At this point, a process by which to manage these occasional events and communicate about them effectively with the customer comes in handy.

I work for an IT contracting company that provides services internally to a specific command within the Department of Defense. Our environment is a complex hybrid of several autonomous, secure networks supported by a litany of technologies, from Cisco Nexus 7K routers to virtualized desktops spread out over several domestic and international locations servicing more than 5000 active users. In addition, the customer's requirements usually come fast and with little time for planning. It is a difficult environment in which to manage changes or outages while remaining flexible to the customer's needs.

During the past two years, we worked very hard to develop, enforce, and maintain a streamlined change deployment process, which has paid huge dividends in providing a reliable and stable IT environment [1]. With that process firmly in place, it was time for us to turn our attention to the management of major outages, issues, or events. This need to manage events as they occurred was born out of frustration felt by both our company's and our customer's leadership. Too often, our leadership didn't get the information they needed when they needed it. In addition, our troubleshooting was often poorly communicated and coordinated, resulting in significant inefficiencies. Technicians would work on things other groups of technicians were working on, wasting time and effort and lengthening the downtime to the customer and users. To make things worse, communications were not being centrally managed, which led to confused messaging and inaccurate data. Regular updates to the customer were not reliable or required from any one person, and so the customer would receive conflicting information. Needless to say, all of these problems created the perception (sometimes rightly) that our technicians were not working cohesively, reliably, or efficiently. In short, it made us look unprofessional and uncoordinated.

A few months ago, my operations manager approached me about setting up a new process to rein in our efforts when responding to "events." We decided on the name "Event Management" for the process by which we would make this happen. Once we began planning, we quickly realized how much more difficult this would be to implement than we had previously thought. It would require:

◆ Participation by the customer and all the technology leads

◆ A new tool to track the details of the events

◆ New personnel to provide support 24x7

◆ A documented process detailing the procedures to follow

In addition to these challenges, we needed to make cultural changes to prevent the customers from going directly to the technology leads for answers (as was previously the case) and convince them of the value and need for the Event Management team.

The Beginning

My first task was to market the idea to the customer and ensure their buy-in; otherwise the whole idea was pointless. I spoke with their watch officer, the position closest to the concept of event management and the person who would usually go out and collect information about outages and issues. The watch officer is a customer-owned position, which creates unique challenges for dividing roles and responsibilities between us (the contractors) and the customer. However, after explaining how this approach would provide a one-stop-shop for them, allowing them to simply rely on our team for information rather than run around asking people, they immediately bought into the idea. And why not? We just made their job much easier by providing a single, central point of contact for all ongoing events.

After we got cooperation from the customer, we set out to build a small team of people to provide coverage. Because this process wasn't built in to the original contract, the customer had no obligation to support us in funding the extra personnel. As a result, I had to work with the operations manager to find extra positions within the division that could be repurposed for this new role. This was a difficult task because, as you would expect, these contracted positions do not hang from trees, and money is tightly budgeted. In any case, we were able to find open positions that we could shuffle around to make a team. Unfortunately, we could only muster three positions, which limited our ability to provide complete coverage. Instead of the originally intended 24x7 coverage, we settled for 24x5. Once we had a team, we turned our attention to scratching out some rough procedures on how the process would work and how responsibilities would be divided.

Writing out the procedures involved a lot of consideration since there would have to be requirements built from several areas, including the service desk, the technology leads, the operations manager, and the event manager. At the request of our operations manager, we held an off-site meeting with several key technology leads to rough out some basic procedures. This was enough to get us off the launch pad. The procedures included requirements for how and when to notify Event Management of an issue, when updates were expected, and how Event Management would communicate and escalate issues. The next day, I emailed all the key leads and gave them a simple flow of how the process would work, and I continued to draft the official procedures.

Once we had a small team with decent coverage and some semblance of procedures, I worked to develop tools by which to track and communicate outages and issues as they occurred. I ended up going simple and using a glorified Excel spreadsheet posted on the main page of our SharePoint site. This made tracking easy, simple, and available to everyone. In addition, we developed specifically formatted emails to communicate the details of outages. These emails have specific information requirements, formatting requirements, and a defined distribution list. The intent is to provide a consistent and reliable product that all key stakeholders can use and understand, including our government customer, the company leadership, and relevant technology leads. At this point, we had addressed many of the practical and tangible problems. The hard part was and continues to be the cultural shift in implementing the process.

Cultural Norms

The most glaring problem of all, and one that will most likely continue for the long term, is the change in cultural norms. The technology leads are accustomed to a certain way of doing things and to not having to explain themselves to external groups. The watch officer is used to reaching out to technology areas directly rather than going through an intermediary. The operations manager is used to hearing directly from individual leads and reaching into their teams for answers and to give directions. All of this has to change and be retuned to utilize the Event Management team to coordinate efforts, understand the problem, and provide accurate outage reporting and a general sense of organization and leadership during an outage. The Event Management team must assert itself as the "belly button" of information. In addition, we must prove ourselves capable of managing the efforts of several teams, communicating status and maintaining awareness of the problem at hand. The operations manager has to support this team and avoid reaching into the teams directly. This kind of management support is critical to the team's ability to succeed and reach its objective. The technology leads will have to get used to providing more detail about outages and allowing the Event Management team to have more visibility in their areas. This is another cultural change that will require the support of and enforcement by the operations manager.

Currently, we have a formal process document outlining all of the requirements and buy-in from all the key stakeholders. Thus far, we have successfully built positive relationships with many of the technology areas and with the customer watch officer. This has allowed us to foster a viable environment by which the process can take root. As previously noted, 24x7 coverage has been a little trickier than originally assumed. We have settled on 24-hour operations Monday through Friday with a stand-by schedule for weekend coverage. Generally, we have made a lot of progress toward developing the process and creating an environment in which the process can take hold.

Conclusion

If we can make this process work, it has the potential to pay huge dividends over time. The company will have centralized, dedicated management and communications during an outage, issue, or security event. In addition, the customer will have only one place to look for answers instead of getting several different answers from several different sources. This approach has the potential to provide political benefits as well. The customer will have a positive perception of the company's ability to provide singular communications and reliable reporting during an outage. In addition, the presence of the team provides a certain level of customer confidence in the company's contract team, which has an intangible value.

This type of management function and process is in fact very valuable for any IT service-providing entity. Providing a single point of contact to collect information, facilitate and coordinate efforts, and provide a conduit for management oversight of troubleshooting efforts allows for more efficient operations and better customer service. Organizations can gain much by utilizing a central presence for which all key stakeholders can find reliable, consistent, and authoritative information.

Resources

[1] Jason Paree and Andy Seely, "The Evolution of Managed Change in a Complex IT Enterprise," ;login:, vol. 39, no. 1, February 2014: https://www.usenix.org/publications/login /feb14/evolution-of-managed-change.