AN HDI WHITE PAPER | DECEMBER 2012

Communicating and Staffing for Unplanned Outages

Roy Atkinson
Senior Writer/Analyst, HDI

UBM Tech

COMMUNICATING AND STAFFING FOR UNPLANNED OUTAGES

Contents

Executive Summary 3

Section A» Planning for the Unplanned 4

What is an unplanned outage?

Who or what determines priority?

What is a Major Incident Response Team, and who should be on it?

What actions should be taken immediately during an unplanned outage?

Section B» Communicating During an Outage 5

Who needs to know what, and when do they need to know it?

How can the support center communicate with stakeholders in the event of an unplanned outage?

What information needs to be communicated?

Section C» Staffing Considerations 7

How can the support center cope with increased contact volume during unplanned outages?

What other staffing considerations are there for these circumstances?

Section D» Reviewing the Plan and Preparing for the Future 8

When should an incident response plan be reviewed, and who should review it?

How should the plan be maintained?

Section E» Additional Resources 9

About the Author 10

About HDI 10

COMMUNICATING AND STAFFING FOR UNPLANNED OUTAGES

Executive Summary

On January 2, Tina, the support center manager for XYZ Corporation, arrives at work. As she picks up the phone to retrieve her voicemail, the VoIP phone goes dead. She steps into the service desk area to look at the monitoring screens and sees that everything is red. It appears that network services are completely down. This means that email, the intranet, the Internet, the VoIP phones, the data center, the virtualized infrastructure, and most other IT services are inaccessible to end users. The support center staff will be arriving in just a few minutes. It's going to be a rough morning.

Tina pulls a red binder off her shelf and opens it to "Major Incident Response." She uses her cell phone to call the security desk's non-VoIP phone to make sure they are aware that building controls may be offline and that there is a major network outage. She then calls Chris, the designated major incident manager, on his mobile, and then runs down a short phone list, calling other members of the Major Incident Response Team. If she doesn't get an answer on their phone, she sends a short text message. Within minutes, the team has assembled.

They are gathered on a conference call using mobile devices and an outside provider. After immediate agreement that there is a major incident underway, they begin to run through a series of checklists. They quickly determine that C-level management needs to be immediately included in their notifications. After a few minutes, each member of the team sets off to complete their assigned communication tasks and agrees to reconvene in thirty minutes for an update. Tina again uses her cell phone to call the landline at the reception desk and asks for a predetermined public address announcement to be made at fifteen-minute intervals, stating that there is a major network outage, that IT is aware of it, and that another update will be announced in thirty minutes. Tina then returns to the service desk area to talk to Benny, always the first analyst to arrive.

Even in the best organizations with the best infrastructures, there are unplanned outages. Although the ultimate goal for many services would be what ITIL describes as *continuous availability* (no downtime, planned or unplanned), technical realities and the projection of substantially increased costs prevent most organizations from achieving it. Some outages are caused by technical faults. Others are caused by human error. Still others may be caused by natural disasters. The costs of unplanned outages to businesses are enormous, with estimates at *$5,000 per minute or more*.[1]

In the language of ITIL, every incident is an unplanned outage—an *unplanned interruption of an IT service or reduction in quality of an IT service*.[2] Many involve a single end user/customer and are more or less routine. Some outages, however, have a large impact, perhaps affecting the entire enterprise; these are classified as *major incidents*. These outages present challenges for the support center, especially when they involve standard communication channels such as email, intranets, and/or the network over which communications are carried. How can support centers continue to keep end users/customers informed and handle the increased volume of contacts when unplanned outages occur? What are some alternative communication channels they can use when things go wrong? How can staffing requirements be adjusted quickly when there's an outage and volume increases?

[1] Martin Perlin, "Downtime, Outages, and Failures: Understanding Their True Costs," *Winds of Change* (blog), September 18, 2012, **www.evolven.com/blog/downtime-outages-and-failures-understanding-their-true-costs.html**.

[2] "ITIL 2011 Glossary and Abbreviations," *Official ITIL Website*, modified October 5, 2012, **www.itil-officialsite.com/InternationalActivities/ITILGlossaries_2.aspx**.

COMMUNICATING AND STAFFING FOR UNPLANNED OUTAGES

Since the support center is often the single point of contact for end users/customers and is widely considered the "face of IT," any business continuity plan should cover the support center's ability to handle outages. The support center does not operate in isolation. It is one part—and an important one—of any cohesive business that offers support, either internally (to its own employees) or externally (to its business customers). The support center should not be acting alone when an unplanned outage takes place, but should become a conduit of accurate information between customers, stakeholders, and business units.

Both communications and staffing for unplanned outages may require creative thinking during the building of a response plan. They should *not* require creative thinking in the event they are needed; plans should be in place and should be executed, and they should be reexamined *post facto* to determine what worked, what didn't, and how they can be improved for the next time.

Note: Many incident response plans are drawn with security incidents in mind. The type of incident response discussed here may or may not be related specifically security incidents like intrusions or denials of service.

Section A: Planning for the Unplanned

What is an unplanned outage?

An unplanned outage is any interruption or degradation of a service which takes place outside the agreed maintenance window (if any) for that service. Unplanned outages are *de facto* breaches of service level agreements. And while avoiding unplanned outages is best, things do sometimes go wrong. How should we prepare the support center for unplanned outages? The key is thinking ahead and having a plan that covers as many alternatives as you and your end users/customers can think of.

Who or what determines priority?

Priority is determined by business *impact* and *urgency*. This is usually displayed as a matrix:[3]

		Impact		
		High	Mid	Low
Urgency	High	1	2	3
	Mid	2	3	4
	Low	3	4	5

We are primarily concerned here with Priority 1 incidents, those outages with high impact and high urgency. These are the outages that may generate large increases in call or contact volume and that demand increased response levels from all involved. Your organization should set thresholds for various courses of action when high-impact incidents occur.

[3] "Doctor," "Incident Priority: What Everyone Should Know," *ITIL Service Management* (blog), June 1, 2007, **itservicemngmt.blogspot.com/2007/06/incident-priority-what-everyone-should.html**.

What is a Major Incident Response Team, and who should be on it?

Any incident reaching both high impact and high urgency should invoke the Major Incident Response Team. Such a team should be part of any business continuity plan, and should probably include the following:[4]

- The **support center manager/service desk manager**, who is responsible for communication with the response team and reporting to customers;
- The **incident manager** (if this is a separate position from the support center manager);
- The **major incident manager**, who probably should not also be the support center/service desk or incident manager, but should be acquainted with incident and problem management;
- The **problem manager**, who is responsible for managing the search for root causes and preventing future incidents; and
- **Representatives** from all impacted areas, including end users/customers.

Each member of the team should have a predefined set of roles and responsibilities, and each should have a designated backup in the event that they are unreachable when needed.

When the actions of a Major Incident Response Team are being planned, it's important to note who the proper contacts are for each business unit, which services affect that unit, and what the effects actually are. Sometimes, these effects won't be immediately apparent. For example, in the event of a network outage, building ventilation (HVAC) may be down or impaired, and certain areas that are climate-controlled or have special ventilation requirements may become unusable. Specific information for each area should be gathered and taken into consideration for both the priority and the method of communication.

What actions should be taken immediately during an unplanned outage?

For the purposes of this discussion, there are two main considerations for the support center in the event of a major unplanned outage, namely *communication* and *staffing*.

Section B: Communicating During an Outage

Who needs to know what, and when do they need to know it?

Effective communication goes a long way toward reducing the contact volume (*call/contact avoidance* or *contact management*) during an unplanned outage and preventing what is known as a "call storm." Remember, if you've been successful at making the support center a single point of contact (SPOC), you've conditioned your end users/customers to contact the support center when something goes wrong. Customers should never be blamed or disparaged for contacting support, even though support has done its best to communicate that they don't have to.

End users/customers experience outages in different ways. If, say, your domain controllers go down, some people might not be able to log in at all, while others might be logged in and can continue to work, but can't print to any network printers; still others might lose the ability to connect to online storage or use

[4] "Doctor," "ITIL Major Incident: All You Want to Know," *ITIL Service Management* (blog), March 24, 2011, **itservicemngmt.blogspot.com/2011/03/itil-major-incident-all-you-have-to.html**.

COMMUNICATING AND STAFFING FOR UNPLANNED OUTAGES

an application that requires authentication. So if there's a general announcement that says, "You won't be able to log in," the people who can't print or the people who can't use online storage will be confused. Your announcement should say something like, "Because of a problem with our network's Active Directory systems, you may be experiencing difficulty accessing online resources such as printing and storage, or you may have difficulty logging in. IT is aware of the problem and is currently working to restore the services." Provide an estimate of the time it will take to restore the services, if at all possible. Understanding the outage from the end user/customer perspective is the first step toward providing good communication, answering the first question they will have: "How long?"

If end users/customers aren't likely to see the effects of an unplanned outage, it may not be necessary to use broad communications. Communications should be as targeted as possible. For example, if the outage affects an online application used by some departments/business units but not all, communicate effectively and rapidly with the *departments that are experiencing the outage*. Communicating too broadly may cause confusion, and may, in fact, *increase* contact volume as people seek information.

You may have to use alternate communications channels, depending on the outage. If, for example, your email system is down, email blasts are, obviously, out of play. Likewise, if your network is down, email and intranet will be out of play, along with VoIP phones, if you have them.

Some options for communication are:

- Public address announcements (unless you have a complete power outage)
- Email blasts (if email is working)
- The outgoing ACD message (if your ACD is working)
- Intranet homepage (if your intranet is accessible)
- Robocalls to extensions (if phones are operational)
- SMS text messages to mobile devices[5]
- Word of mouth/back channels
- Social media

If the outage is to critical services and needs to be communicated to the entire organization, and if email is operational, the blast should come from a recognized source (e.g., CEO , COO, CIO, director of IT, etc.). Overhead announcements should be repeated every half-hour or as new information becomes available, and should include updates to the estimated time of service restoration. ACD announcements should state the issue clearly, acknowledge that it's being worked on, and give an estimated time to restore; this estimate should be updated at least once an hour. Remember, keeping end users/customers informed is vital.

When it comes to word of mouth and back channels, let's say your network is down and your VoIP phones are out. You don't have a list of everyone's mobile phones (though someone should, by the way). So how do you communicate? Let's say Bill in IT is married to Sandy in HR. So Bill can call Sandy's mobile and ask her to start spreading the word. And Sandy has lunch every Thursday with Jackie, who runs production, so Sandy calls or texts Jackie. The informal, personal networks in your workplace can be used very effectively when necessary.

[5] There are services that you can have customers/employees opt into that will send SMS messages out in the event of major incidents or outages. SMS services may be available even if voice services are not.

Social media can be an important communication channel as well, provided that those involved know where to look in the event that you suddenly become unreachable by standard methods. For example, if your company has a closed Facebook page or LinkedIn group only for employees or customers, even if your network is down, the page can be updated and accessed via mobile device and the authoritative word can be spread.

During an outage, communicate appropriately, early, and often. Your end users/customers will want answers to some very basic questions:

- Do you know about this problem?
- How can I get work done?
- When will it be fixed?

As clearly as possible, let them know what happened, what they can do in the absence of the affected service, and when the service will be restored. The estimated time of restoration should be updated every time information is communicated. It may mean the difference between managers deciding to keep staff in the business units at work or releasing them until the service has been restored.

Section C: Staffing Considerations

Unplanned outages can be a staffing nightmare. In the absence of excellent communication, for example, consider what might happen if *no one* in your company or institution was able to log into their computer one morning. What if everyone felt it necessary to contact the support center? Your queue would become unmanageable, your end users/customers would be angry, and your analysts would be swamped. Situations like this have happened to major customer service operations when, for example, there has been a widely-reported security breach or an airline reservation system has failed. In these cases, the support centers were unreachable for days simply due to contact volume.

Depending on the nature of your business, the budget at your disposal, and the technology you have in place, there might be several ways to minimize the impact of major unplanned outages aside from the communications and call avoidance methods discussed.

Some ways to address staffing for unplanned outages are:

- Auxiliary staff provided by a third party
- Auxiliary staff on call
- Auxiliary staff in-house

Staff provided by a third party

If your budget allows, you may want to consider having an outsourcing company available to take overflow calls or contacts during high-volume periods, such as unplanned outages or planned upgrades and rollouts. If your phone system is out, for example, any external calls you receive might be directed to your selected provider, or your ACD can be set so that queued calls above a certain threshold are forwarded to this auxiliary support provider. Again, communication is vital, since you want to be giving your end users/customers correct, up-to-the-minute information.

Auxiliary staff on call

For some industries, it may be a viable option to have a number of home-based workers who are on call in the event of a call storm, and who can log into your systems and provide support from their homes or other remote locations, equipped with suitable computers or thin clients. This option requires a large commitment of funds and may not be available in the event of certain types of outages.

Auxiliary staff in-house

In many organizations, having in-house auxiliary staff may be an option. You may need to temporarily move level 2 and 3 analysts to the front line to increase your capacity, but take care not to handicap your organization's ability to solve the problem that's causing the increased volume. You may even want to reach out to your "power users"—people with specialized knowledge around the company or institution—to have them as distribution points for current information, or even as additional frontline staff. This, of course, will require approval from the managers in each area.[6]

Section D: Reviewing the Plan and Preparing for the Future

"The best time to plant a tree was twenty years ago.
The second best time is now."
—Chinese proverb

When should an incident response plan be reviewed, and who should review it?

There's no time like the present to begin a thorough review of your response plan, if you have one, and no time like the present to begin building one if you do not. The IT incident response plan shouldn't be separated from the business's incident response or business continuity plan (if your business has one) but should integrate with it at every level. When there is an interruption of service, the business is at risk.

This is something that's always stated but not always understood: *Senior management support should be obtained and maintained for your incident response plan.* Your plan will touch many business units and you will need acceptance and cooperation from all involved. You'll be less likely to be successful without the support of management at higher levels.

Immediately following an unplanned outage, the entire response team should review and update your plan. While the successes, failures, and lessons of the most recent outage are top-of-mind, you can make improvements.

[6] See Bill Weyrick, "Service Management, Meet Emergency Management," *SupportWorld* (March/April 2012), pp. 41-44, for one example of how this was done during a major implementation. (Available online at **www.ThinkHDI.com/~/Media/HDICorp/Files/SupportWorld/2012/MarApr12/SW_MarApr12_Weyrick_EmerMgmt.pdf**.)

How should the plan be maintained?

Once your plan has been modified, each member of the team (and other stakeholders) should receive an approved, updated version. All documentation should be accessible both online and offline. Though it's difficult to maintain and control offline documents, it's necessary—in the event of a major incident, online documentation may be inaccessible and therefore useless. You should obtain any final approvals for the plan as rapidly as possible, and get it in place. Part of your plan's documentation should be a list of every element involved and every copy that needs to be updated. If your organization has a document control system, use it. You may wish to partner with departments that have document control or document management specialists and follow their practices and procedures.

Section E: Additional Resources

The Gross Staffing Calculator (available online at **www.ThinkHDI.com/~/Media/HDICorp/Files/Library-Archive/Gross-Staffing-Calculator.xlsx**) can provide you with a way to estimate the number of analysts needed to handle various call volumes. If you have records of past outages' call volumes, you may wish to use those numbers to see how many analysts would be required to handle the high contact volume of a major outage. Your budget will very likely not allow for that expansion, but you may obtain useful information if you are seeking to have auxiliary or expanded staff at hand.

To learn more about document control, visit The Institute of Document Control's website at **www.document-control.org**.

COMMUNICATING AND STAFFING FOR UNPLANNED OUTAGES

About the Author

Roy Atkinson is HDI's senior writer/analyst. He is a certified HDI Support Center Manager and a veteran of both small business and enterprise consulting, service, and support. In addition, he has both frontline and management experience. Roy is a member of the conference faculty for the HDI 2013 Conference & Expo and is known for his social media presence, especially on the topic of customer service. He also serves as the chapter advisor for the HDI Northern New England local chapter.

About HDI

HDI is the professional association and certification body for the technical service and support industry. Facilitating collaboration and networking, HDI hosts acclaimed conferences and events, produces renowned publications and research, and certifies and trains thousands of professionals each year. HDI also connects solution providers with practitioners through industry partnerships and marketing services.

Guided by an international panel of industry experts and practitioners, HDI serves a community of more than 120,000 technical service and support professionals and is the premier resource for best practices and emerging trends.

