the Availability Digest

www.availabilitydigest.com

Media Communication During a Crisis

May 2011

When a disaster strikes your data center, that's no time to have to start worrying about how you are going to deal with the press. You have your hands full with worrying about the well-being of your employees if faced with a physical disaster; with recovering your IT operations, which may take days; with communicating with customers and suppliers to keep them informed; with answering panic calls from your management; with perhaps having to relocate and house employees and see to their personal needs; and with a myriad other crisis duties.

If you have not planned beforehand for media communication during a crisis, a second crisis is looming. If this is a major outage affecting millions of users or thousands of businesses, as were the Amazon cloud failure[1] and the PlayStation hacking fiasco,[2] described in other articles in this issue, there will be a feeding frenzy by the press and by the bloggers. Every publication will try to be the first with the most sensational news, and much of this reporting may be erroneous if it is not carefully controlled. Erroneous reporting can cause great confusion among other stakeholders with whom you are communicating your own message, such as your employees, your customers, your suppliers, your management, and your shareholders.

Today, a great deal of publicity regarding data-center crises comes from the growing body of bloggers. They can have a significant impact on the public, but from where do they get their information? To a small extent, it comes from inside sources; but to a large extent, it is sourced from the public press and augmented by their own imaginations and opinions. Keep the press informed, and the bloggers will be informed.

Dr. Robert Chandler, Director of the Nicholson School of Communication at the University of Central Florida, specializes in crisis communication.[3] Following the recent triple disaster in Japan – earthquake, tsunami, near-nuclear meltdown – Dr. Chandler gave several webinars on crisis communication. Though much of his focus in these webinars was on natural disasters, his points are equally relevant to any data-center disaster.[4]

In this article, we use Dr. Chandler's observations on crisis communications to discuss relations with the media following a data-center failure.

[1] Amazon's Cloud Downed by Fat Finger, *Availability Digest*; May 2011.
[2] Sony PlayStation Taken Down for Weeks by Hackers, *Availability Digest*; May 2011.
[3] Robert C. Chandler, Ph D., *Emergency Notification*, Praeger Publishers; 2010.
[4] Many of Dr. Chandler's webinars are sponsored by Everbridge, a company marketing crisis-communication products. The webinars can be found at http://www.everbridge.com/webinars.

The Stages of a Crisis

A crisis typically passes through a series of stages.

Warning

Certain types of crises give enough warning so that precautionary steps can be taken. For example, hurricanes, floods, snow storms, and epidemics can be predicted with some certainty (or at least with a probability of occurrence); and plans can be made to continue operations in the event that the crisis materializes. This can include evacuation plans, indications of when employees should not report to work, the preparation of backup facilities or facilities for temporary home offices, instructions for reporting to an alternate facility, and so on.

Other crises occur without warning. Examples of these are major equipment failures (such as a redundant storage failure), hackers, power outages, fires, earthquakes, workplace violence, and terrorist acts. Other events may give marginal warning, such as tornados and public riots.

Risk Assessment

Every good business continuity plan should have an emergency-response plan. Depending upon the pending (or existing) crisis, the appropriate internal people needed to handle the crisis should be notified and the emergency response plan activated.

At this point, all communication is internal and is sent only to the plan's decision makers. Public communication occurs during the next phase.

Response

Once a crisis actually takes place, the crisis team notifies those responsible for taking immediate action. Focus is then shifted to notifying the masses – employees, customers, suppliers, etc. This is the time to start to brief the press.

Management

From this point on, the crisis could move toward resolution; or it could get worse than anticipated. If it gets worse, it probably gets more complex; and the response may have to be modified.

During the crisis, the organization must provide regular status updates to its various audiences, including the press. Instructions may have to modified, and the outlook for resolution may change.

Resolution

Once the crisis is drawing to a conclusion, the return to normalcy must be communicated. At this time, it is appropriate to draw attention to any erroneous reporting by the press. It is also a good time to give a detailed post mortem to the press as to what occurred and how it was handled.[5]

[5] See the detailed post mortem given by Amazon, as detailed in our companion article, Amazon's Cloud Downed by Fat Finger. This is an excellent example of satisfying the press, though Amazon was criticized for being slow in releasing information.

Recovery

Focus on getting back to normal. It is now time to convert this strategy to an opportunity. Acknowledge the shortcomings in your approach to the crisis, and communicate how you are going to rectify them in the future.

Media Relations

In our introduction above, we said ”much of this [press] reporting may be erroneous if it is not carefully controlled.” But how can you control the press? The answer is that you can’t. But what you can do is to work closely with the press and to make sure that they get timely and consistent information.

That is the essence of Dr. Chandler’s advice. Working with the press may seem like an oxymoron, but one thing that is an anathema to any publication is to publish information that later turns out to be wrong. Consequently, the press will pay attention to what you are saying. But make sure that your message reflects accurately the current state of your knowledge about the crisis and that the succession of messages that you issue are consistent.

Dr. Chandler suggests for consideration five priorities in your messaging.

Optimal Timing

The timing of messaging is critical. If a message is released too early, it may be irrelevant. If it is issued too late or contains too little information, it may be irrelevant.

If a storage system fails, maybe it can be recovered in a few hours. If news of the failure were to be immediately released, few may care. On the other hand, if it turns out that the database has to be restored from tape, and it will be three days before IT services are restored, this is relevant and important information.

Message Content

The releases to the press must reflect your best estimate of the situation. This estimate may change as the crisis unfolds, and it is important to keep the press informed as the situation progresses.

It may be embarrassing to admit that your earlier prognosis of a speedy recovery measured in hours now appears to have changed to a recovery estimated to be days. However, if you do not immediately acknowledge this, it is going to come out anyway. If the press finds out that you knew critical information long before you released it, you will have lost the confidence of the press – and of the bloggers – who will now start to speculate on what the situation really is.

Up-to-date, consistent information will keep the press synchronized so long as they have trust in your messaging.

Maintain Control

You must maintain control of your messaging. Typically, you will appoint one and only one person to speak to the press. That person certainly can quote other officials in the company, but having a single information outlet is the best control to ensure that your messaging is consistent.

A major part of retaining control is to carefully monitor the press, the bloggers, and even your competition, to uncover any rumors or media spin. As you see your message becoming distorted, you must immediately respond with the accurate information. This is the reason that you must never get caught in a deception. Once that happens, all of your following messaging will be discounted.

Transparency

Based on our many Never Again stories, it is clear that transparency is your best weapon. The truth will eventually come out. If you stonewall the truth or attempt to deceive the press as you progress through the crisis, they may not be in your corner for the next crisis you face. On the other hand, if you are known for your honesty and transparency, the responsible press will be very supportive of the pain you currently are suffering.

It is important to communicate what you currently know, not what you think the public needs to know.

A very effective strategy that many companies have adopted is to maintain a service-level dashboard on their web sites. These dashboards show the current status of all services, Services that are in grief are highlighted, the problems explained, and the current status of recovery clearly predicted and kept updated. Dashboards are an important source of pertinent and consistent information for the press.

Optimal Delivery Channels

As we said earlier, you should have a controlled media-information channel to ensure that all messages to the public are consistent. This is typically done by designating a single person to interface with the press. All other involved personnel – including C-level executives – should defer to this contact for information.

Your messaging should be high-volume. Don’t worry about putting out too much information. Let the press filter it and decide what they want to use. You will find that each publication will pick and choose different bits of information that you provide and will cast their stories along different lines. What is important is that these stories are consistent.

Above all, be responsive to the press. When a reporter calls, talk to him or her; and be as candid as possible. Who knows, one may ask that one question that will lead to a scoop. You then have a friend for life.

Preplanned Messaging

When a crisis hits, that is not the time to have to worry about generating messaging for the press. Of course, you will have to do so. But to the extent that you can, preplan your messaging. Having skeleton messages in which you can fill in the details will be a big help when you have more important things to do in response to a crisis.

The possible causes for a crisis are typically too many to try to address upfront. In addition, there are too many crises that you may never be able to conceive (like the data center that had all of its servers confiscated by law enforcement for two days to support an investigation). Rather, focus on the impact of the crisis – impacts represent a much more manageable number.

What will you do if you lose a major system? What will you do if you lose your data and have to do a multiday recovery from tape? What will you do if some tapes are unreadable and you lose some data? What will you do if your data center is running fine, but nobody can get in (flood, pandemic, riots)? What will you do if your data center is destroyed? What will you do if you are hacked, and sensitive customer data is compromised?

These are examples of the categories for which you can create prepared messages. Each problem could have been caused by myriads of disasters, but the effect is the same.

Summary

Perhaps the most important of Dr. Chandler’s priorities is transparency. Transparency can be difficult. During the crisis, evidence may suggest one set of problems; but the root cause of the disaster might turn out to be something different. If you are perfectly transparent, you may expose vulnerabilities that may be embarrassing and that in hindsight you need not have exposed.

Furthermore, your lawyers may bring pressure not to mention certain issues if they feel that they could encourage lawsuits against your company.

However, the downside of not being transparent is inconsistent messaging. You may find yourself boxed into a situation that you described in one way but that has turned out to be embarrassingly different.

In both of our companion articles on the PlayStation and Amazon disasters, the companies were honest and forthcoming, though perhaps a little late. Sony tried at first to state that no personal information had been stolen by the hackers but had to confess later that indeed such information was compromised. They then took the position that no credit-card numbers were stolen, but that is yet to be seen. Also, they kept predicting that gaming services would be restored in days. It is now three weeks, and these services have yet to come back online.

Amazon did an amazing job of publishing a detailed post mortem of exactly what caused its multiday failure, even though the report exposed some perhaps embarrassing faults in Amazon’s infrastructure.