

SUNGARD

FROM THE FRONT LINES

Executive Brief Series

Lessons Learned During Mock Disasters

OVERVIEW

A tanker truck carrying hazardous chemicals has just overturned on a highway near your headquarter facility. It's unclear whether or not the toxic gas is leaking into the air. The impact to your organization is unknown and the situation is ever-changing. One thing is certain: your incident management team needs to be called into action. It's up to them to assess the situation and then determine and execute the appropriate response. They need to demonstrate smooth collaboration and communication. They need to address all the possible impacts on your organization's physical, technological and human resources. The safety of your employees—and the future of your company—may be riding on it. Are you 100 percent confident in your team's ability to address such a crisis?

For many organizations, the answer to that question is, "We're just not sure."

One of the best ways to test—and refine—these capabilities is through an incident management exercise. These can run the gamut from high-level walkthroughs to full-scale, interactive simulations. The latter—in which the team responds in real-time to a fictional, but continually evolving, incident—is the best method for testing preparedness. SunGard Availability Services has conducted numerous walkthroughs for individual organizations, as well as full-scale simulations for both individual organizations and conference groups.

Walkthroughs can help organizations think through the myriad of steps required. But, to truly test an incident management team, a mock disaster is the best approach. During every simulation SunGard has facilitated, participants have come away with a greater sense of their teams' strengths and weaknesses—as well as their own individual capabilities. Although many organizations are well prepared to manage an incident, almost all leave a simulation having learned at least one critical lesson.

In this executive brief, SunGard has compiled the recurring lessons learned during the simulations we've conducted. Many of these "lessons" may seem like common sense. But, you'd be surprised just how often they arise when sleeves are rolled up and the pressure is on.

CREATE A SUCCESSION PLAN

When an organization participates in a mock disaster, the top-level managers on the incident management team usually shine. They typically have undergone training and are knowledgeable about the plan and their roles in executing it. In addition, they tend to be strong leaders accustomed to performing in high-pressure situations.

Without a doubt, a well-trained executive team is a good thing. But, what about the level of management just below? During a real incident, many of your top managers may not be available. They could be away on business or vacation; they could be injured—or worse. When simulating the absence of key members of an incident management team, weaknesses often emerge. That next layer of management often has not undergone the same level of training.

Management redundancy is a must. Therefore, you need to create a clear succession plan—and then deliver training to make it workable.

COMMUNICATE, COMMUNICATE, COMMUNICATE

Everyone knows good communication is essential to success—whether it’s “business as usual” or a crisis situation. Yet, communication is one of the most common reasons organizations fail to respond effectively to an incident. (And, those who uncover communication challenges during a simulation are the lucky ones.)

When SunGard facilitates a disaster simulation, all relevant parties are literally in one room. Even when communicating is as fast and easy as walking a few feet, many incident management teams still rely on assumptions. The result: during simulations, teams duplicate efforts on some activities while neglecting other important steps. But, inadequate communication and reliance on assumptions are easily resolved when everyone’s gathered in the same room. Just imagine how the dangers of miscommunication multiply during a real-life incident.

Don’t assume that your incident management team knows how to communicate effectively. During simulations, several organizations have realized that team members lacked a standard method of communication. If you have more than one tool, which one should be used at time of incident? It’s important to answer that question before you’re facing a real situation. Test your team’s ability to communicate and collaborate—whether members are in the same room or geographically dispersed. Chances are, you’ll identify some weaknesses that need to be addressed.

HOW DOES AN INCIDENT MANAGEMENT EXERCISE WORK?

In conference or mixed-company settings, SunGard provides participants a sample abridged incident management plan. When a specific company is engaged in a simulation, they use their own internal plan.

Simulations are typically played in phases or rounds. Information is provided at the start of each round to each team, so that no one team has all the information. As the simulation progresses, additional information is provided in three ways:

- Facts or new risks and threats are typically introduced as simulated news broadcasts.
- Information that defines some internal scale or context for the participants—either to the group as a whole or to selected teams—is provided by the SunGard facilitators.
- Substantial information is “created” by the participants themselves, based on whom they communicate with and their own actions and decisions during the exercise.

SunGard-facilitated simulations present realistic, ever-changing challenges—giving individuals and organizations a chance to test their ability to manage situations as they evolve.

STANDARDIZE AND TEST YOUR CRISIS MANAGEMENT TOOLS

As you test your team's communication skills, you may realize that inconsistent tools are creating unnecessary confusion. A lack of standardization is more than just inconvenient; it can be just plain dangerous during an actual crisis. To be effective, you need to use one management tool and one notification tool. That way, your team will receive the same messages at the same time—and everyone will be in synch on the “when, where and what” of your crisis response.

There's a corollary to tool standardization: Once you have selected tools for use by incident management teams throughout your enterprise, make sure they can handle high levels of demand. Imagine discovering—during a crisis—that your tools crash when the number of users spikes. That's an issue you need to explore and resolve before any incidents occur.

With the heavy workloads IT staffs face, standardizing and testing the performance of your crisis management tools may fall to the bottom of the list. But, tackling this effort before a crisis strikes is an investment worth making.

TIE ALL YOUR PLANS AND POLICIES TOGETHER

If you're a small organization with only a local or regional presence, this common problem may not affect you. But, if you're part of a large company—with thousands of employees operating in numerous regions of the country or the world—you need to absorb this lesson. As a result of their incident management exercise, many organizations have realized that their corporate and location- or business unit-specific plans simply are not in harmony.

SunGard conducted an interagency incident management exercise for a branch of the U.S. Government. As part of the simulation, similar issues emerged. Although the agency had a formal, written policy, some representatives knew about it; others did not. As a result, those “in the know” assumed that everyone would operate under the established policies—which didn't happen. This response, with pockets of compliant reaction, created a great deal of confusion. The same often happens in the private sector when a multinational corporation has disjointed plans and policies.

You must ensure that all plans and policies “roll up” appropriately. You need to clearly define how the various teams will work together— as well as who will maintain authority, accountability and control. Uncertain that your organization's plans would mesh during a crisis? The least risky way to find out is through a disaster simulation exercise.

REAL-WORLD RESULTS

According to Tina Brown, Director, Continuity Services and Crisis Management for Cingular Wireless, a SunGard-led situation management exercise:

- Provided training and practice opportunity for key Cingular Crisis Management Personnel and Executive team on:
 - National Security/Emergency Response and Emergency Response Management
 - Activation of the Crisis Management Team
 - The Cingular Crisis Management Plan and software
 - Crisis Management Team responsibilities
 - Crisis Management Center operations and procedures
- Identified improvement opportunities in Crisis Management/Emergency Response planning efforts
- Validated functional crisis plans
- Provided a foundation for the ongoing development of a robust Business Continuity and Crisis Management Planning capability for Cingular Wireless

THINK THROUGH THE DETAILS—INCLUDING BUSINESS USERS' NEEDS

It's not unusual for business or operational groups to rush through their portion of a continuity or availability plan. They're eager to mark it as "complete" on their lengthy to-do lists. Of course, that won't matter when an incident occurs. At that point, everyone will be wishing they had invested more time and effort into building a plan—and testing to ensure its effectiveness.

During an exercise, it will quickly become apparent who has rushed through plan development and who has paid careful attention to the details. Groups that fare well in simulations are the ones that have proactively invested time and effort into thinking through the details. The rest are usually scrambling!

Although there are details associated with all aspects of incident management, one of the most often overlooked is the people aspect. Many teams simply have not thought through the specifics of their employees' workspace needs. Some have made assumptions about using office space at other company locations—which may or may not be available or usable during an incident. And, even if a facility is available, that doesn't guarantee that your business users will have all the resources they need to keep your business moving.

In addition, we've worked with several organizations whose employees assume they'll be able to work from home following an incident. The fact is, the required computing resources—such as virtual private network (VPN) tunneling—are often not immediately available.

And, even if they are, data may be at least 24 hours old—and employees may not have ready access to the hardcopy files and notes from their regular desks.

As they say, the devil is in the details—and that's certainly true during a simulated (or real) disaster. Start thinking through specifics; the number of holes in your current plan may surprise you.

SUNGARD EXPERIENCE

We have conducted simulations using the following scenarios:

- Cyber terrorism
- Building fire
- Gas refinery explosion
- Traffic accident with hazardous materials evacuation and response
- Train derailment with hazardous materials evacuation and response
- Radiological disbursement device (a.k.a. "dirty bomb")
- Liquid natural gas leak with area evacuation
- Low-grade nuclear device detonation with wide area electro-magnetic pulse (EMP)
- Hurricane

"Cingular was able to immediately leverage the lessons learned in this exercise to support the preparedness and recovery efforts for Hurricane Frances, which significantly impacted our operations in Florida."

—Tina Brown, Director, Continuity Services and Crisis Management, Cingular Wireless

BE PREPARED FOR EMPLOYEE RELATIONS AND COMMUNICATIONS

Imagine a dirty bomb, chemical spill or biological strike affecting your facility. Which employees will you send in to repair your physical infrastructure? How will you assure them of their safety and well-being? How will you assure other employees of their health and safety? There are no easy answers to these types of questions. However, you must think them through.

After all, your people are one of your most valuable assets. You must protect them to the best of your ability—and communicate effectively with them during and after an incident. You won't succeed at employee relations unless you have a strategy in place.

While you can never anticipate every potential scenario, you can avoid being blindsided when it comes to employee relations. Disaster simulations have helped SunGard's clients develop their human resources-related strategies and tactics.

UNDERSTAND YOUR PRIORITIES

The final lesson is basic: Every company needs to clearly identify and prioritize key business resources—from the employees who do the work to the physical and technological infrastructures they rely on every day. Without that knowledge, you won't be able to make the right investments when it comes to availability and continuity planning. Nor will you know the right course of action following an incident. SunGard has helped many organizations realize the fallacy of this common assumption: that when IT recovers, the business recovers. In fact, when we conducted the exercise at DRJ in 2004, attendees were primarily from IT. Although they were prepared to think through technology issues, they could not fully mount a response without input from their business unit peers.

Before you can conduct an effective incident management exercise—whether an in-depth mock disaster or a high-level walkthrough—you must have a handle on your priorities and interdependencies. That includes processes, places and people, as well as technology. If you're struggling with this, it's time to take a step back and enlist some expert help in sorting through the complexities.

OPENLY ADDRESS YOUR KNOWN VULNERABILITIES

The September 11, 2001 terrorist attacks demonstrated that it's impossible to prepare for every possible incident; we simply can't conceive of everything. While some have embraced that as an excuse to not plan, others have taken to heart another key 9/11 lesson: You absolutely must address your known vulnerabilities.

When planning a mock disaster exercise, savvy organizations ask SunGard to expose and confront their vulnerabilities. They ask us to incorporate one or more of their weak spots into a simulation. It can make for some uncomfortable moments. But, ultimately, they benefit from the opportunity to gather information and build an effective action plan—in a safe place and during a safe time.

CONCLUSION

You're heading home from the office at 6:00 on a Tuesday evening. As part of your company's incident management team, you've spent the day responding to a tanker truck that overturned right outside your headquarter facility. The team enacted the company's response plan but soon realized that provisions for employee relations were inadequate, your plan lacked a clear strategy for business users, and it failed to address a key weakness in your physical security. If this were a real incident, you'd be logging many more hours at the office. But, because the day was spent in a disaster simulation, you have the good fortune to be heading home—and your organization has the good fortune of knowing exactly why and how it must improve its incident management capabilities.

Indeed, a disaster simulation is the closest thing to a real incident—from the unexpected twists and turns in the "event" to the often unexpected actions of colleagues. It's the best way to determine just how prepared (or unprepared) your management team is. After participating in a SunGard mock disaster—whether they learned one or all eight of the lessons outlined in this brief—organizations and individuals never approach incident management in the same way again.

SUNGARD SERVICES

The SunGard Incident Management Exercise service provides a proactive means for your management and team members to test that personnel are aware, ready and equipped to perform the actions necessary to prevent or respond to a disruption to normal business operations. This service helps validate your readiness to effectively and efficiently manage incident response using your existing plans.

SunGard consultants work with senior management to identify your business priorities and develop strategies to respond to specific challenges, such as natural, technological, civil or environmental hazards. Through meetings with senior management, business unit representatives and support department managers, SunGard tailors an Incident Management Exercise that addresses the following:

- Incident detection and preliminary assessment
- Notification and escalation
- Damage assessment
- Incident command center procedures
- Support activities
- Administrative procedures
- Resource requirements

In addition, SunGard reviews your existing incident response policies and procedures and recommends changes where appropriate. We also identify gaps between the capability needed to achieve response objectives and the exercise results.

AUTHORS

This paper was based on the collective experience of SunGard Availability Services and was written with the assistance of the following SunGard consultants:

Jim Grogan, CGEIT, CISM, Vice President, Consulting Product Development

Deborah Taylor, CBCP, Manager, Professional Services

Managing Editor: Pat McAnally, Senior Director, Professional Services and Analyst Relations, SunGard Availability Services

About SunGard Availability Services

SunGard Availability Services provides disaster recovery, managed IT, information availability consulting services, business continuity management software to over 10,000 customers in North America and Europe.

www.sungardas.com

SunGard Availability Services

680 East Swedesford Road

Wayne, PA 19087

Tel: 800-468-7483

©2010 SunGard. EBS-006

Trademark information: SunGard and the SunGard logo are trademarks or registered trademarks of SunGard Data Systems Inc. or its subsidiaries in the U.S. and other countries. All other trade names are trademarks or registered trademarks of their respective holders.