

# **DISASTER RECOVERY** *JOURNAL*

Disaster Recovery Journal

Contents

Summer 2003 - Volume 16, Issue 3

## BIOTERRORISM

### **Preparing Your Organization For a Terrorist Attack**

By DR. IVAN WALKS

On March 30, 2003, three subsidiaries of a U.S. corporation were the target of a bioterrorism attack. Twenty employees at various locations throughout the country received a letter containing a fine white powder. What if this was your organization? Are you prepared to respond and protect your employees, their families and the communities they live in?

This was the scenario for a mock disaster exercise sponsored by E Team and facilitated by Borden/Lee Consulting during the DRJ Spring World 2003 Conference in Orlando. The goal of this exercise was to simulate a bioterrorism event, introducing and training private and public sector personnel on how to prepare for and respond to such a threat.

As former chief health officer for the District of Columbia during the anthrax crisis in 2001, I experienced first-hand the strengths and weaknesses of the Washington region's disaster response planning. Believe me, whether you are in a corporation or a local, state or federal agency, disaster pre-planning has immeasurable benefits. Most companies and public agencies have a crisis plan – the challenge is turning a static, paper-based plan into action (action that is flexible and well thought out, with built-in reflexes and resources). Based on my recent experience in Washington, I have found that the key to a successful response is the ability to communicate and share information quickly and fluidly with the appropriate people at the right time in order to make the critical decisions the situation demands. This requires pre-planning and ensuring that personnel are familiar with procedures before a big crisis occurs.

At the DRJ conference, 175 individuals representing small, medium and large U.S. companies and local public agencies from the City of Orlando and Osceola County participated in the mock disaster

exercise. The exercise involved a scenario in which weapons-grade anthrax was mailed to various employees working for three different subsidiaries of a major corporation. The software that was used as the core communications infrastructure for the exercise supports the incident command system (ICS), an organizational structure and set of functions that have been established by the public sector to effectively respond to emergencies of any kind. Increasingly, ICS has been adopted by corporations as well to guide their crisis management processes. Recently, the secretary of the Department of Homeland Security recommended to the president a consistent nationwide approach based on the ICS (referred to as the National Incident Management System) for all domestic incidents. The president endorsed the plan.

The ICS method enables those responders involved to immediately activate pre-established guidelines and areas of responsibility, access detailed lists of resources, and quickly identify both human resources and availability and location of equipment and supplies. Invoking a chain of command with clearly defined areas of responsibility helps insure that the responders have the initiative throughout the disaster – eliminating the confusion and lost time that often puts the responders in a catch-up mode where mistakes and bad calls are more prevalent. During the exercise, each participant was assigned a role within one of the three subsidiaries or the parent company, and then charged with figuring out how to respond to the incident. Each company location had its own emergency operations center equipped with a computer. The computer was enabled with a crisis management software solution that provided for collaboration and overall situational awareness of what was happening at all locations. As part of the exercise, I was hired by the parent corporation to act as consultant in advising the organization on how to respond to the anthrax attack. The mock disaster exercise represented four days in the life of the organization. Each day the participants were given a list of updated scenarios and questions to facilitate their responses. Every emergency, crisis and bioterrorism attack is unique. How people elect to respond to each incident is also unique because decisions are based on personal experience, location, timing and the exact nature of the incident.

The exercise below will give you and your organization the opportunity to evaluate how prepared you are to respond to and recover from a bioterrorism attack. As you put yourself in the participant's shoes, try and answer the question: Is your organization prepared to respond to the following scenario?

### **Scenario Background**

Unbeknownst to the mock disaster exercise participants, two employees working for the organization belonged to a radical extremist group with an international network. They have contaminated paycheck envelopes with anthrax powder, targeting random employees at various company locations with the goal of shutting down the organization. It is important to note that while fire

department personnel can perform preliminary screening tests on site to see if a substance is anthrax, the results are not always accurate. It takes up to 48 hours to get definitive results. Thus, a company must respond immediately and take actions assuming the substance is indeed anthrax.

### **DAY 1**

- Twenty letters containing anthrax are received at company locations throughout the country.

- Thirteen letters are opened in the workplace. Three letters are opened by employees at home.

Questions posed to responders:

- What immediate actions should be taken upon notification of the letters containing a powdery substance?
- What critical information needs to be communicated and to whom?
- What impact will emergency response agencies have on the local facility and the corporate headquarters?

### **DAY 2**

- One letter was found unopened in an employee's office. One letter was opened by an employee in the workplace. One letter was opened by an employee at home.

Questions posed to responders:

- What is the status at each company location?
- What action will corporate headquarters take? Hire a bioterrorism consultant?
- Where is the emergency management team located and has a schedule been developed to cover the situation 24x7?
- How will you identify the employees who have opened envelopes at home? What impact will this have on those communities? What role should the company assume?
- How are you tracking the overall situation?
- How are you working with corporate, main, and local offices and with local, state and federal government to stabilize the situation?
- What information is critical at this point? How do you obtain it and ensure the right people are "in the know?"

### **DAY 3**

- One letter was opened by an employee at home.

- Several employees have begun to exhibit symptoms of exposure to anthrax.

Questions posed to responders:

- Based on the situation, what resources are required?
- What information is critical at this point?
- What is your plan for the next 24 hours?

### **DAY 4**

- Several employees in each of the targeted locations call in sick with flu-like symptoms; many others have refused to come to work out of fear they will "catch" anthrax.

Questions posed to responders:

- What is the status of the organization?
- How is information being tracked?
- How are you coordinating with local, state, and federal authorities?
- What is your action plan for the next seven days?

### **Applying The Lessons Learned**

Based on my personal experience with the anthrax attack in Washington and feedback on lessons learned from the participants in this exercise, below is a checklist of action items for organizations to assist them in preparing for, responding to, and recovering from a bioterrorism attack.

- Clear lines of responsibility and communication. Who is in charge? Take the time to identify people and positions within your organization that are responsible for preparing for and responding to a bioterrorism attack and what their roles are. Organize contact lists, including e-mails and phone numbers well in advance. The emergency team should also familiarize themselves with the corporate communications infrastructure and procedures to ensure a timely and effective response. Consider adoption of a crisis management software system to help establish clear roles and responsibilities, which can be applied to crisis situations, as well as daily resource tracking to ensure optimum preparedness.
- Real-time information sharing and collaboration. Organizations need the ability to communicate and collaborate with the right people at the right time. One-to-many, many-to-many, and many-to-one communications are critical during a major crisis. You should not rely on person-to-person contact and cell phones to facilitate a response. Organizations need to ensure they are installing collaborative software solutions using open standards that not only enable the sharing of information throughout the entire organization and to external parties, but also the control and targeted dispersion of that information.
- Levels of clearance. Pre-clearance for information access greatly speeds the flow of information and optimizes the response. Identify which company executives, managers and employees are cleared for receiving various levels of sensitive information before the event.
- Resources. Research and compile a contact database of all the resources you could possibly need, including subject-matter experts, law enforcement, emergency, equipment, non-profit support organizations and public agencies whose assistance will be needed during a response.
- Payment/credit procedures. Create memos of understanding, purchase orders, open requisitions, or credit lines with all vendors in order to eliminate the red tape when time is of the essence during a crisis. Establish a list of personnel who are authorized to order goods and services during the crisis, as well as the means of obtaining a large amount of cash.
- Risk communication. Delays, conflicting information and embarrassing retractions produce confusion and unnecessary fear. One of the great benefits of a collaborative information sharing system

is the control, timing and uniformity of information released to internal and external audiences.

### **Summary**

Simulations like the DRJ mock disaster exercise can help companies and governments see the tremendous advantages of pre-planning, as well as experience the swiftness and control that a crisis management software solution can provide. By creating scenarios, turning paper-based crisis plans into actionable solutions, and increasing collaboration and communication you can put your company in a position to minimize the chaos, damage and fear surrounding a potential bioterrorism attack.

---

Dr. Ivan C.A. Walks is senior medical advisor at E Team, Inc., a provider of collaborative software for emergency and event management, and CEO of Ivan Walks and Associates, a consulting firm that specializes in the policy and practice of Health, Human Services and Education with a focus on the specific opportunities and challenges of urban communities.

To comment on this article, go to 1603-05 at [www.drj.com/feedback](http://www.drj.com/feedback).

---

*©Copyright 2003 Systems Support Inc. All rights reserved. Reproduction in whole or in part in any form or medium without the express written permission of System Support Inc. is prohibited.*

*«BACK to the Articles Index*