



Business Continuity Planning Issues Take Center Stage

By Richard A. Diamond ■ *Stradivarius Associates*

Even if things are running smoothly in your business, it's likely that you might be wondering what would happen in the event of a real-life disaster to your organization. In other words, if the lights go out, will there really be anyone home? With our troops spread throughout the Middle East and tensions continuing to be high, the risk of terrorism at home has increased dramatically. This creates a compelling need to evaluate business continuity plans to make sure that critical business systems, employees and tenants are adequately protected.

Here is a list of 10 tips for tailoring corporate contingency plans to accommodate threats in times of high alert:

1. Consider the Human Factor — Organizations should determine which employees have already been called up for military service and who might be in the future. Information about these reservists should be available through the human resources department and should be incorporated into the plan. Particular attention should be paid to whether any of the reservists hold key positions in the recovery plan. If that is the case, companies may find it beneficial to train another individual to take over that employee's recovery responsibilities.

2. Keep Tabs on Travelers — Organizations should begin to keep track of all employees who are traveling domestically and internationally. Plans should include flight, hotel, and contact information for traveling employees. In the

event of an emergency, traveling employees should be able to contact organizational representatives anytime for immediate assistance. It is also advisable for international business travelers to register with their local embassies.

3. Guard the Home Front — While many organizations may not be direct terrorism targets, their location may put them at risk. Business continuity planners need to determine how the surroundings might put them at risk for terrorism including the proximity to government buildings, landmarks, or religious institutions. Organizations should also communicate with their neighbors to ensure that if, for example, one building receives a bomb threat, all the surrounding businesses will automatically be alerted.

4. Increase Security — Organizations are also tightening security. Some are hiring more security guards or instituting stricter security measures such as making sure that all cars in the parking lot belong to employees or guests. Procedures need to be put into place that enable an organization to account for everyone — employees and visitors — on site at any given time and to make sure that all those people are aware of the emergency procedures.

5. Test the Call Tree — Organizations should conduct regular tests on their call trees to ensure that all contact information is current and that the call tree works as it should. Residents and businesses should be included in this program as well.

6. Review Alternate Site Contracts — If an organization has an alternate site contract, those contracts should be looked at to make sure they reflect the current needs of the business and are updated if necessary. It may be advantageous to speak with the alternate site provider to ensure that they have the equipment outlined in your contract or can accommodate changes to equipment needs. Also, if there are travel restrictions, key employees may encounter problems getting to the alternate site. Be sure those employees have several means or routes of getting to the site in an emergency.

7. Plan for Alternative Fuel — If the Middle East fuel supply takes a hit it could directly impact the way many organizations operate. Business continuity planners should determine how a fuel disruption would affect their company and then look at either alternative fuel sources or suppliers. On the same note, a potential fuel disruption could also affect diesel supplies. Since many organizations' emergency generators run on diesel, business continuity planners may want to build a back-up supply of diesel. (See January 2003 article in *Broadband Properties* on Fuel Cells)

8. Maintain the Plan — Make sure all employee, customer, and vendor contact information in your continuity plan is up-to-date and remind key personnel of their roles and responsibilities during a crisis. Confirm that all members of the team understand their responsibilities and create alternative

"Here is a list of 10 tips for tailoring corporate contingency plans to accommodate threats in times of high alert..."

"While many organizations may not be direct terrorism targets, their location may put them at risk."

leaders in the event your primary ones are without communication.

9. Supply Chain Reaction — A war or terrorism could be disruptive to an organization's international supply routes. Business continuity planners should review supply chain routes and determine how to reroute goods and services if necessary. Backup suppliers should be secured and ready to go.

10. Back Up Daily — Ensure that all critical information is backed-up daily and kept off site. Secure data centers offer this service and should be contracted with to make sure that all key business systems and data can be recovered in the event of loss.

Here's an extra 10 tips: Business continuity experts recommend companies take some additional measures, such as:

11. Prepare for Homeland Response — Review areas surrounding office buildings for potential terrorist targets and check with local authorities for any emergency preparations that should be made.

12. Review Escape Routes — Ensure that primary and alternate escape routes are available; they are not blocked with any materials or obstructions; and that emergency lighting is operational.

13. Check Emergency Supplies — Check supplies of water, food, medical equipment, flashlights, batteries, ropes, blankets, and tools; and update supplies as needed. Keeping an emergency or survival kit on site could be the difference between life and death.

14. Alternate Transportation — Evaluate available sources of transportation to and from the office (as well as the emergency recovery site) in an emergency situation.

15. Review Alternate Power Supplies — Test all backup power systems to ensure proper operation, in case of a

Need flexible
programming
options?

Call SMS.

We have
transport services
available for
most programming
through



Call

800.788.8388

www.smstv.com

Established 1985

power disruption.

16. Secure Voice/Data Communications — Ensure that mobile phone batteries are charged and that a charger is available; use mobile phones from more than one service provider. Make sure two-way radios have extra batteries available. Arrange for emergency alternate routing of incoming phone calls to an alternate office location. Maintain list of all employee communications contact numbers. Ensure that critical routers, servers, and switches are backed up and their capabilities are replicated at an alternate location. Ensure that all networks and network access points are secured from unauthorized access and activity.

17. Secure Electronic Mail — Ensure that e-mail servers are backed up; establish ability to recover and redirect e-mail traffic to an alternate location.

18. Secure Critical Information Systems

— Ensure that critical systems, platforms and PCs are backed up and their data can be recovered at an alternate location; ensure that systems and databases are secured from unauthorized access, viruses, worms, and other attacks.

19. Discourage Conflict Among Employees — Encourage employees to consider the sensitivities of their peers. Explain that the voicing of political opinions in the workplace is potentially insensitive and disruptive to business operations and cannot be tolerated.

20. Lastly, remain calm if the event of an emergency — Contact your local police, fire, ambulance first by calling 911. Be sure to give them correct location information.

Being prepared is more than half the battle. Now is the time to review your current business continuity plans and make adjustments based upon your company's needs. Your employees are

your most important assets. Your tenants are right behind them. This is an unusual opportunity to make sure that all of your critical business elements are protected. Remember, your company may be @ Risk. ■

About the Author

Richard A. Diamond is the President & CEO of Stradivarius Associates which specializes in business strategy consulting for public and private companies around the world. He actively consults with ImagiNet (www.imagi.net) a leading secure managed network service provider, offering a comprehensive suite of network management, online data backup, WAN and security products and services. ImagiNet has operated its "state of the art" Secure Operations Center 24 x 7 x 365 for over 17 years. He can be reached via email at rdiamond@stradass.com.



Stocking Distributor for all your cable needs

- Headend, Plant, & Fiber Design & Engineering
- Satellite, Trunk, & Drop Accessories
- Pre-fabricated Headends
- System Testing & Certification
- High Speed Data Design & Engineering

2425 East 26th Street
Minneapolis, MN 55406
612-724-4400
612-729-1300 Fax

800-328-6820

See us at:
www.dfcco.com