3. Focus and facilitate homeland security related research and development.
4. Encourage cooperation between consortium institutions.

The second consortium, the National Academic Consortium for Homeland Security (NACHS) comprises public and private academic institutions engaged in scientific research, technology development and transition, education and training, and service programs concerned with current and future U.S. national security challenges, issues, problems, and solutions at home and around the world. The specific objectives of the NACHS are to help:

1. Improve understanding of national security issues, especially terrorism and strategies for counterterrorism.
2. Promote development of better-informed public policy, strategy, plans, and programs regarding national security issues.
3. Develop new technologies and transition those technologies into effective, practical, and affordable solutions to (current and future) international and homeland security problems.
4. Educate and train the people required by governmental and nongovernmental organizations to effectively accomplish international and homeland security roles and responsibilities.

Both the HSDEC and NACHS have furthered the education components of homeland security into proposed standardized curriculum-based programs. To support the need for the components of the curriculum, professional core competencies should be the foundation of any program.

Once specified knowledge, skills, and abilities are acquired, the healthcare executive will be considered competent to perform within their profession. As a result, through assessment of performance competency components, healthcare organizations will be able to continually demonstrate an ability to respond appropriately to threats.[22]

Business Threat Evaluation

Every business entity should develop a sense of how vulnerable it is in the wake of a bioterrorism attack. Table 20-1 is provided as a place for many businesses to begin assessing their relative risk by virtue of their business size, location, dependence on human performance, and the mission/product/service of the entity. After the business entity scores itself on the following table, the authors suggest that a score in the moderate range (5–7 points) or above should be considered a warning for the entity to put serious resources into developing bioterrorism contingency plans.

The authors suggest that communities assess their level of risk for bioterrorism and develop appropriate contingency planning by using Table 20-2.

Table 20-1 Biological Terrorism Threat Evaluation for an Organization

Points	1. Size of Business	2. Dependence on Human Resources to Perform Mission	3. Location of Business	4. Mission/Production of Business
0 ROW 1	Very small (>20 people)	Very low	Rural area	
0.5 (half a point) ROW 2	Small (21–50 people)	Low	Suburban (Small city >100,000)	Businesses and corporations with international direct customers or suppliers, local government, food services, business and corporations with over $100 million in revenue per year
1 ROW 3	Medium (51–100 people)	Moderate	Small city (>100,000)	Minor electrical and fossil fuel interchanges and hubs/ network hubs, biomedical equipment, state government, national finance & banking, emergency services organizations (not deployed)
1.5 (one and a half points) ROW 4	Large (101–500 people)	High	Suburban (Large city)	Moderate electrical and fossil fuel interchanges and hubs/ network hubs, medical goods supply, international finance & banking, transportation, military weapons or products, food production, law enforcement, emergency services organizations (deployed), biotechnology
2.5 (two and a half points) ROW 5	Very large (more than 501 people per location)	Very high	Large city	Major electrical and fossil fuel interchanges and hubs/ network hubs, pharmaceuticals or vaccine production, mass media, food processing or central storage, healthcare, dental, veterinarian facilities and medical laboratories, mail or delivery services, national level government, armed services

(continues)

Table 20-1 Biological Terrorism Threat Evaluation for an Organization (continued)

Note: For each area (1–4) use the highest point level that approximates your business situation.

Step 1. Determine the size of your organization under #1 and write down corresponding point level;

Step 2. Determine human resource dependency level under # 2 and write down point level;

Step 3. Determine location of organization under # 3 and write down point level;

Step 4. Determine mission/industry under # 4 and write down point level; and

Step 5. Add all points together where 8–10 = high threat, 5–7 = moderate threat, 2–4 = low threat, and <2 = negligible threat; of course more preparation moderates the threat level downward,.

Table 20-3 is prepared for communities and businesses located in those communities as an indicator of approximate threat level related to bioterrorism, and the concomitant need to develop a community-wide Bioterrorism and Infectious Disease Preparedness Plan, a Community Collaboration Plan, an Infection Control Plan, a Post-Exposure Management Plan, a Workforce Education Program, and an Off-site Contingency Plan.

Table 20-2 Bioterrorism Threat Evaluation for a Community—Composite

Points	1. Population of a Defined Geographic Area	2. Industrial–Production Composition of Area	3. Traveler Traffic per Year
0	>50,000	>5% of ROW 4 or 5 in Table 2	>50,000
.34	50,000–99,999	6–9% of ROW 4 or 5 in Table 2	50,000–99,999
1.34	100,000–499,999	10–19% of ROW 4 or 5 in Table 2	100,000–999,999
2.34	500,000–999,999	20–29% of ROW 4 or 5 in Table 2	1,000,000–2,499,999
3.34	<1,000,000	<30% of ROW 4 or 5 in Table 2	<2,500,000

Note: For each area (1–3) use the highest point level that approximates your location's situation.

Step 1. Determine the size of your population under #1 and write down corresponding point level;

Step 2. Determine industrial-production composition level under # 2 and write down point level;

Step 3. Determine traveler traffic in and out of your location under # 3 and write down point level;

Step 4. Add all points together where 8–10 = high threat, 5–7 = moderate threat, 2–4 = low threat, and <2 = negligible threat; of course more preparation moderates the threat level downward.

Table 20-3 Business and Community Preparation Guidance Based on Threat Level

Business and/or Community-Composite Threat Level Measure	Bioterrorism and Infectious Disease Preparedness Plan (Priority Level)	Community Collaboration Plan with Action Steps and Establishment of Command and Control Authority	Infection Control Plan, Post-Exposure Management Plan, Workforce Education Program, and Off-site Contingency Plan
>2 points	Low	Moderate to low	Moderate to low
2–4 points	Moderate	Moderate to high	Moderate
5–7 points	High	Urgent	High
8–10 points	Urgent	Urgent	Urgent

■ BUSINESS INVOLVEMENT: WHAT SHOULD BE DONE

Business leaders need to take responsibility for addressing concerns about the possibility of bioterrorist activity. Awareness is the key. Leaders should inform all their key stakeholders, from the Board of Directors to the employees, that preventive as well as response policies/programs are under way. This may take place in the form of briefings, in-service workshops, simulations and mock exercises, security enhancements, and coordination with local health facilities. Many businesses will want to develop disaster plans that help victims and their families remain in the information loop or in some cases to evacuate the workplace. If the threat level is high for the organization, a security audit by an outside firm might be in order. Additionally, the human resources department and the business center will need to have business contingency plans and backup systems to deal with business downtime. Some type of communication to the public and customers will also be essential. Additionally, work with your local community, utilizing an assessment system, such as the community preparedness scorecard.[23] There are several "critical success factors" for an organization to consider, and these should include the following:[24]

1. Workforce training (i.e., a well informed workforce)
2. Mitigation of confusion
3. Time management (time is critical)
4. Building a response capacity
5. Economic constraints
6. Coordination with local health agencies
7. Mitigation of fear and panic

Training

Training is essential for all personnel. This could be in the form of awareness enhancement or, for businesses at greater risk, actual training in disease detection and early intervention. Additionally, the training of at least one "disaster coordinator" or "health coordinator" would be important. This individual can serve as a resource person, advisor, counselor, and organizer. They also could have the responsibility for staying informed and maintaining contact networks with local health agencies. Ideally, this coordinator would receive continuing education through CDC, WHO, ACHE, or some other organization that provides periodic updates on skills and knowledge needed to be effective in this role.

Mitigation of Confusion

Mitigation of confusion is a critical success factor in managing any crisis. The natural tendency of humans in a state of confusion is to panic. If this occurs, more harm can result. Training, preparedness, and prior discussion of the range of possibilities and response scenarios all help to mitigate confusion. Fast, clear communications to all personnel is essential. No one should be left in the dark on these matters. Some organized protocols for testing and prophylaxis will help provide much needed reassurance that the business cares for its people and is taking appropriate steps. Finally, a key to avoiding confusion is the development of roles and responsibilities that are clearly understood and communicated widely.

Time Management

Time is critical in all matters pertaining to infectious disease. Early signs, early diagnosis, early warning to the non-infected, and early intervention all have positive implications for the decreased spread and eventual decreased impact of the disease.

Response Capacity

Response capacity may be in the form of trained personnel, along with needed equipment and proper training. It also includes working with local health agencies to develop a quick response to a crisis. There are financial considerations such as cost of training, supplies, equipment, and down time that should be part of the capacity building within the business. Some might even consider a "bioterrorism crisis reserve" for contingency planning.

Mitigation of Fear and Panic

There is no better way to decrease stress and anxiety in anticipation of a possible bioterrorism attack, and likewise no better way to control for panic after an attack, than putting in the requisite time and resources to

properly train the workforce and larger community. This should include the design of a disaster-control command center where all communications originate. When there are but a few people directing the response, it tends to minimize panic and maximize effective distribution of information.

A PREPAREDNESS PLAN

Address the following areas in the BCP:

- A collaboration plan including area healthcare; public health; veterinary, physician, and medical group practices; and law enforcement with specific preparation action steps (stockpiling appropriate levels of material, training, etc. . . .) and with the local hospital(s) addressing the planning necessities presented in Aimee Stern's "Bioterrorism" in *Hospital & Health Networks* pages 58–60.[25]
- Reporting of incidents and possible incidents and how it will be done.
- Infection control practices and procedures and decontamination procedures.
- A post-exposure management plan for employees (prophylactics and vaccines and a plan to prevent secondary infections).
- An off-site contingency operation plan.
- An education plan (prospective and concurrent to an attack) and a public relations plan.[4]

Components of an Effective Response to Bioterrorism[10]

- Establish protocols for suspicious packages (protocols are at http://fbi.gov).
- Establish a response command and control structure where critical decisions can be made (should be community based).
- Develop and implement a training and awareness program for the workforce and with local healthcare, public health, and law enforcement officials.
- Ensure surveillance systems are in place (LRN, etc. . . .).
- Implement the business contingency plan.

Cost of Business Involvement

Consider the following when preparing a budget for preparation of a bioterrorism attack, the response sequence, and the recovery phase in the BCP:

- Cost of detection devices
- Cost of personal protection devices such as masks and body covering

- Cost of vaccines and prophylaxis (Cipro, etc. . . .)
- Cost of training: training professionals, resources, and personnel hours
- Cost of constructing evacuation avenues, decontamination sites, and "safe rooms"
- Cost of temporary or permanent loss of business function
- Cost of securing substitute personnel in case of temporary or permanent loss of regular personnel
- Cost of insurance coverage: general liability, health, life, and workers compensation

It is imperative that the business entity's risk manager understands the insurance and coverage implications of each carrier's policies related to bioterrorism. Are there "Acts of War" exclusions, or any other exclusions/modifiers that proscribe or limit coverage? Will the health and life insurers cover the cost of vaccines or personal protection devices based on the business' level of threat? Planning the insurance aspects of bioterrorism should be taken as seriously as every other phase of disaster preparation.

Sample Forms for Organizational Contingency Planning for Disasters and Terrorism

The following forms (Figures 20-2–20-6) are from www.ready.gov and provide a simple, "get started" approach to thinking in terms of readiness, preparedness, and contingencies.

Open for Business Worksheet

Computer Hardware Inventory

Use this form to:

- Log your computer hardware serial and model numbers. Attach a copy of your vendor documentation to this document.
- Records the name of the company from which you purchased or leased this equipment and the contact name to notify for your computer repairs.
- Record the name of the company that provides repair and support for your computer hardware.

Make additional copies as needed.

Keep one copy of this list in a secure place on your premises and another in an off-site location.

HARDWARE INVENTORY LIST

Hardware (CPU, Monitor, Printer, Keyboard, Mouse)	Hardware Size, RAM & CPU Capacity	Model Purchased	Serial Number	Date Purchased	Cost

Figure 20-2 Open for Business Worksheet.

Emergency Supplies
Talk to your co-workers about what emergency supplies the company can feasibly provide, if any, and which ones individuals should consider keeping on hand. Recommended emergency supplies include the following:

	Water: amounts for portable kits will vary. Individuals should determine what amount they are able to both store comfortably and to transport to other locations. If it is feasible, store one gallon of water per person per day, for drinking and sanitation.
	Food: at least a three-day supply of non-perishable food
	Battery-powered radio and **extra batteries**
	Flashlight and **extra batteries**
	First Aid kit
	Whistle to signal for help
	Dust or filter masks, readily available in hardware stores, which are rated based on how small a particle they filter
	Moist towelettes for sanitation
	Wrench or **pliers** to turn off utilities
	Can opener for food (if kit contains canned food)
	Plastic sheeting and **duct tape** to "seal the room"
	Garbage bags and **plastic ties** for personal sanitation

Figure 20-3 Emergency Supplies.

The following will give you an idea of what it may cost to develop a disaster protection and business continuity plan. Some of what is recommended can be done at little or no cost. Use this list to get started and then consider what else can be done to protect your people and prepare your business.

No Cost

- Meet with your insurance provider to review current coverage.
- Create procedures to quickly evacuate and shelter-in-place. Practice the plans.
- Talk to your people about the compan's disaster plans. Two-way communication is central before, during and after a disaster.
- Create an emergency contact list, include employee emergency contact information.
- Create a list of critical business contractors and others whom you will use in an emergency.
- Know what kinds of emergencies might affect your company both internally and externally.
- Decide in advance what you will do if your building is unusable.
- Create a list of inventory and equipment, including computer hardware, software peripherals, for insurance purposes.
- Talk to utility service providers about potential alternatives and identify backup options.
- Promote family and individual preparedness among your co-workers. Include emergency preparedness information during staff meetings, in newsletters, on company intranet, periodic employee emails and other internal communications tools.

Under $500

- Buy a fire extinguisher and smoke alarm.
- Decide which emergency supplies the company can feasibly provide, if any, and talk to your co-workers about what supplies individuals might want to consider keeping in a personal and portable supply kit.
- Set up a telephone call tree, password-protected page on the company website, an email alert or a call-in voice recording to communicate with employees in an emergency.
- Provide first aid and CPR training to key co-workers.
- Use and keep up-to-date computer anti-virus software and firewalls.
- Attach equipment and cabinets to walls or other stable equipment. Place heavy or breakable objects on low shelves.
- Elevat valuable inventory and electric machinery off the floor in case of flooding.
- If applicable, make sure your building's HVAC system is working properly and well-maintained.
- Back up your records and critical data. Keep a copy offsite.

More than $500

- Consider additional insurance such as business interruption, flood or earthquake.
- Purchase, install and pre-wire a generator to the building's essential electrical circuits. Provide for other utility alternatives and backup options.
- Install automatic sprinkler systems, fire hoses and fire-resistant doors and walls.
- Make sure your building meets standards and codes. Consider a professional engineer to evaluate the wind, fire or seismic resistance of your building.
- Consider a security professional to evaluate and/or creae your disaster preparedness and business continuity plan.
- Upgrade your building's HVAC system to secure outdoor air intakes and increase filter efficiency.
- Send safety and key emergency response employees to trainings or conferences.
- Provide a large group of employees with first aid and CPR training.

Figure 20-4 Cost of Developing a Disaster Protection and Business Continuity Plan.

Open for Business Worksheet

Insurance Coverage Discussion Form

Use this form to discuss your insurance coverage with your agent. Having adequate coverage now will help you recover more rapidly from a catastrophe.

Insurance Agent:_____

Address:_____

Phone:_____ Fax:_____ Email:_____

INSURANCE POLICY INFORMATION

Types of Insurance	Policy No.	Deductibles	Policy Limits	Coverage (General Description)

Do you need Flood Insurance? Yes_____ No_____

Do you need Earthquake Insurance? Yes_____ No_____

Do you need Business Income and Extra Expense Insurance? Yes_____ No_____

Other disaster-related insurance questions:

_____

_____

_____

_____

Figure 20-5 Open for Business Worksheet.

Sample Business Continuity and Disaster Preparedness Plan

❑ PLAN TO STAY IN BUSINESS	If this location is not accessible we will operate from the location below:
Business Name	
Address	Business Name
City, State	Address
Telephone Number	City, State
The following person is our primary crisis manager and will serve as the company sokesperson in an emergency.	Telephone Number
Primary Emergency Contact	If the person is unable to manage the crisis, the person below will succeed in management:
Telephone Number	Secondary Emergency Contact
Alternative Number	Telephone Number
Email	Alternative Number
❑ EMERGENCY CONTACT INFORMATION	Email
Dial 9-1-1 in an Emergency	
Non-Emergency Police/Fire	
Insurance Provider	

Figure 20-6 Sample Business Continuity and Disaster Preparedness Plan.

CHAPTER SUMMARY

The threat of natural or terrorism disasters having a negative impact on business is perhaps greater today than ever before. The integration of the BCP into the strategic plan of the company can add real value by aligning all the key departments and staff around company issues associated with disaster preparedness. The threat of biological weapons is more real in today's society due to the limited cost of their production, the availability of the production knowledge through the Internet and other sources, and their ease of dissemination once produced. All businesses should evaluate their threat level based on the nature of their business, their size, and the community in which they are located.

For prompt and better response to disasters of such nature, the BCP has to identify collaboration with the local, county, state, and/or federal agencies and healthcare providers in the business area to understand what their capabilities are in handling such attacks. For the organization's BCP to be successful, it should include workforce training, mitigation of confusion, timely identification of the event, building a response capacity, coordination with local health agencies, and mitigation of panic using the command control center where all communications are coordinated.

References

1. Homeland Security Act of 2002.
2. Ledlow G, Johnson J, Cwiek M. Bioterrorism and business: Think globally, act locally. In Delener N, Chao C. (eds.) *Global Business and Technology Association International Conference; Beyond Boundaries: Challenges of Leadership, Innovation, Integration and Technology*. 683–693; 2002.
3. Breithaupt H. Toxins for terrorists: Do scientists act illegally when sending out potentially dangerous material? *EMBO Reports*. 2000;1(4):298–301.
4. Leach DL, Ryman DG. Biological weapons: Preparing for the worst. *MLO Med Lab Obs*. 2000;32(9):26.
5. Dennis C. The bugs of war. *Nature*. 2001; 411(6835):232–235.
6. Kortepeter MG, Cieslak TJ, Eitzen EM. Bioterrorism. *J Environ Health*. 2001;63(6):21.
7. Sandström G. A Swedish/European view of bioterrorism. *Ann N Y Acad Sci*. 2000;916(1):112–116.
8. Henderson DA. (2000). Bioterrorism. *Int J Clin Pract*. 2000;115 Supplement 115:32–36.
9. Hagstad D, Kearney K. Bioterrorism: Reacting promptly and appropriately to a highly infectious, invisible agent. *Am J Nurs*. 2000;100(12);33.
10. Canada Communicable Disease Report (IM). General Collection. 2001;27(4), February 15, 2001-02- 28 10:19:14, ISSN: 1188-4169.
11. Geiger HJ. Terrorism, biological weapons, and bonanzas: Assessing the real threat to public health. *Am J Public Health*. 2001;91(5):708.
12. Lawler A. The unthinkable becomes real for a horrified world. *Science*. 2001;293 Sept 21:2182–2185.