DISASTER AND TERRORISM PREPAREDNESS

An Examination of the State of Corporate Preparedness in the US among Eight Leading Corporations

FINAL REPORT

Prepared for

ALFRED P. SLOAN FOUNDATION

December 2005

By

The Bellwether Group, Inc.

www.bellwethergroupinc.com

Executive Summary

Companies participating in the study were generally well prepared for disasters arising from acts of terrorism and from natural or technological hazards in the US. Their state of preparedness increased significantly as a result of 9/11 and continues to do so. Most of these companies compete and resource globally, and threats to their enterprises have increased, not only as a result of the greater likelihood of terrorist acts but also as a function of their greater geographic exposure through globalization and growing recognition of disaster preparedness as an important strategic goal. Following recent terrorist attacks overseas and multiple natural disasters around the world, preparedness strategies, both globally and within the US, remain a high priority at these companies.

All participants had experienced business disruptions in the US arising from natural hazards, and more than half as a result of terrorist activity. Natural hazards and technological failures were more frequently experienced than acts of terrorism. Hazards of all types have the potential to interrupt business through the loss of people, facilities, equipment, inventory and data. Preparedness requires corporations to have the capability to deal with such losses irrespective of their root cause. Terrorism preparedness is consequently an integral part of a comprehensive disaster management program at each, but particularly important to those with critical facilities in major cities.

Preparedness strategies involved both preventive measures and reactive capabilities to minimize disruptions and were both threat-specific and general in nature. Preventive measures undertaken addressed many types of threats, including terrorism, with building hardening, access control and surveillance systems in-place at business-critical sites. Threat advisories, such as hurricane warnings, also helped companies to try and avoid, or prepare for, identifiable events; however, neither preventive measures nor advance intelligence can preclude all disasters, and, as a result, additional capabilities were also considered necessary.

Emergency Response and Business Continuity Planning (ERP and BCP respectively) represent "all-hazards" approaches enabling more effective management in emergencies and subsequently, when necessary, the relocation of critical business processes to alternate sites. While ERP ensures better damage control and helps contain losses, the availability of alternate sites and systems is vital to ensuring business continuity, since there is no guarantee that people, equipment and facilities will function following a serious event. BCP ensures an effective and efficient organizational response in the event that part of the corporate infrastructure is impaired following a disaster. ERP and BCP were generally comprehensive at all participating companies despite being introduced relatively recently at some. Additional capacity and geographic diversification of business processes are an increasingly attractive strategic alternative to increase flexibility and reduce total system risk.

Preparedness plans were typically owned by the business units but coordinated through several corporate functions (or program offices). Nowhere were the risk management, security, emergency management and business continuity functions all fully integrated within one corporate function. Given the "embedded" nature of preparedness plans, the costs associated with system redundancy, alternate sites and management time are not easily identifiable. However, taken together with the corporate functions responsible, the overall cost of preparedness is likely very substantial. Despite the high level of resourcing required, little overall cost-benefit evaluation was undertaken at many of these companies.

Many best practices in preparedness were uncovered during the study. Most are not well documented in the public arena and participants benefited by discussing these with each other. Benchmarking enabled the identification of best practices, developed at or considered by these companies, and helped them analyze their preparedness programs by increasing transparency. Use of a "Preparedness Index" further facilitated comparison and provided additional insights. The broader application of both these methodologies to other companies would enable them to identify opportunities to improve their preparedness strategies and thereby increase their resiliency to disasters.

On the whole, the companies that participated in this study are much better prepared to survive natural disasters and acts of terrorism than ever before and likely represent the "state-of-the-art" in the corporate world today. However, as always, there is more that can be done. Those that develop their capabilities to evaluate and mitigate enterprise risk from an overall perspective, integrate their preparedness functions accordingly, and incorporate appropriate best practices developed outside their enterprises will continue to further improve their overall state of preparedness.

Introduction

In June 2005, *The Bellwether Group, Inc.* received a grant from the *Alfred P. Sloan Foundation* to undertake a pilot benchmarking project on Disaster and Terrorism Preparedness in the US among a select group of large corporations. The project was completed in December 2005. The primary objectives were to:

1. Determine the state of preparedness within the participant companies
2. Identify best practices in corporate preparedness and enable participating companies a potential opportunity to improve by learning from each other
3. Ascertain whether a program of this nature could improve corporate resiliency to acts of terrorism and other disasters if conducted on a broader basis.

Eight companies participated including *Fidelity Investments, IBM, Johnson & Johnson, KeySpan Energy, Lehman Brothers, Microsoft, Pfizer and Verizon*. These companies were invited based on their different experiences with acts of terrorism, natural and non-natural disasters and geographic exposure with respect to their business locations. Collectively they represent over $300 billion in revenues, employ over 500,000 employees and have over 18,000 facilities worldwide. The industries represented include financial services, technology services, hardware, software, healthcare, gas and electric utilities and telecommunications. A significant portion of their businesses are conducted in the US, and both public and private perspectives were represented.

Bellwether undertook both primary and secondary research to identify the key issues in terrorism preparedness and determine the data required of the participants. Primary research was conducted with the *New York Police Department Counter Terrorism Unit*, *Department of Homeland Security (DHS)*, *International Center for Enterprise Preparedness at New York University (InterCEP)* and the *Combating Terrorism Unit at the United States Military Academy (West Point).* Secondary research sources included: *Federal Emergency Management Agency (FEMA), Disaster Recovery Institute International (DRII), Business Continuity Institute (BCI), American Society for Industrial Security (ASIS), Conference Board* and *Chief Security Officer (CSO)*.

Collection of data and validation of findings were conducted in three steps. Firstly, each participant completed a detailed questionnaire. Secondly, *Bellwether* conducted interviews with one or more parties at each company to understand their strategy and positioning. Thirdly, all companies participated in a Round Table Discussion in New York City on October 4th, 2005 at which preliminary observations, the state of corporate preparedness, taking care of employees and future initiatives were discussed.

The key findings from the project are set out below.

Disaster Preparedness & Enterprise Threat Management

Companies face many types of threats in addition to terrorism that have the potential to cause disastrous or catastrophic results for their businesses. These range from naturally occurring phenomena such as earthquakes and hurricanes to non-natural threats (often referred to as "man-made") such as power outages and acts of sabotage and terrorism. Terrorism is one of many threats with the potential to create a major business disruption but is now significantly more relevant than pre-9/11.

Managing threats and preparing for disasters, irrespective of their origin, is complex. The potential effects of both natural and non-natural threats have common symptoms of destruction or loss that can disrupt business by affecting the availability of facilities, employees, equipment, inventory and data. Being prepared requires a considerable investment in system infrastructure, additional facilities, equipment, supplies and executive time; it is no small undertaking for any corporation.

As a best practice, preparedness requires involvement from the entire corporation or, at least, a large part of it. Preventive measures can reduce the probability, or effects, of a terrorist act or other threats of a disastrous nature but cannot preclude the possibility of them occurring. Since these measures by themselves do not guarantee that a disaster can be avoided, alternate emergency management and business continuity planning are also required. Due to the commonality of the effects of terrorist acts and other types of disasters experienced or anticipated by companies, the primary emphasis in preparedness planning is undertaken from an "all-hazards" perspective. Corporate survival and value maximization require that companies minimize business interruptions by providing alternative ways to deliver products and services with the minimum inconvenience to customers. This provision of alternate delivery and servicing capabilities mitigates against disasters caused by acts of terrorism and other hazards, irrespective of their nature, and is an essential element of preparedness.

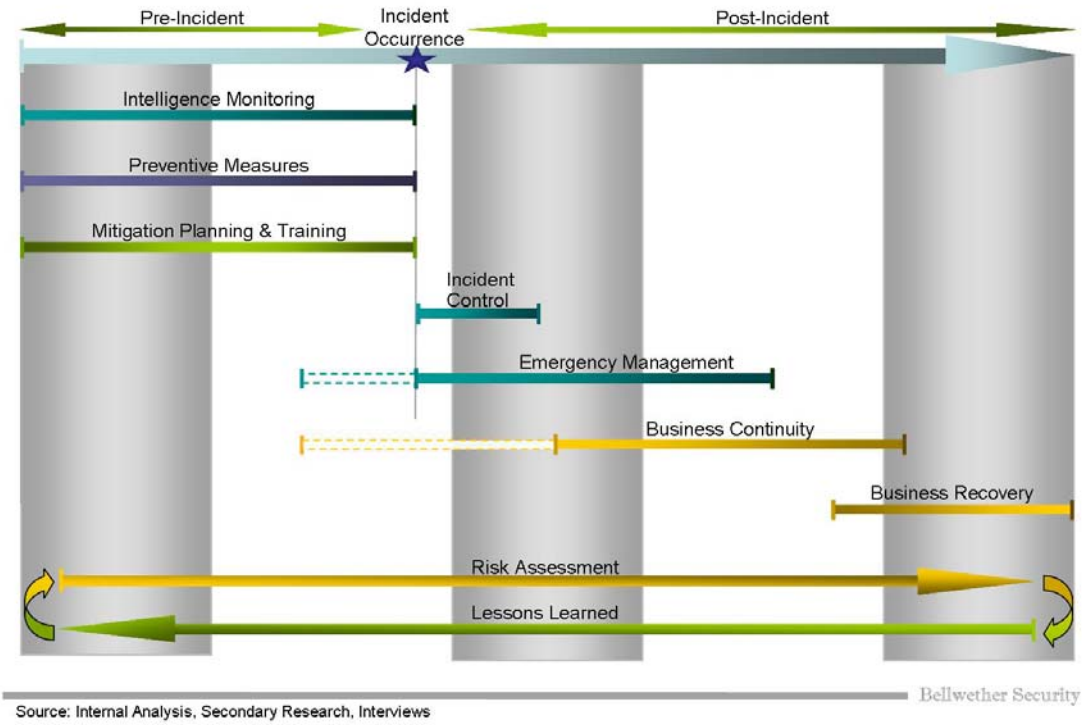
At all participant companies, preparedness coordination was the domain of several internal departments that typically worked with one and other but were not necessarily resident within a single corporate function. As a result, all companies had multiple executives responsible for different aspects of preparedness. Within the participant group, corporate security, emergency management and business continuity functions were all involved. In some companies two of these functions were performed together within the same group, but these were not necessarily the same ones. None had all three functions within the same group. Nor was there commonality with respect to which corporate function heads had ultimate responsibility. In addition to the corporate functions to which preparedness coordination was assigned, other corporate departments were also involved in preparedness planning such as facilities, legal, public relations, and human resources.

Disaster preparedness activities generally fall into two categories: activities that are undertaken in an attempt to prevent or lessen the effect of a disastrous event when it threatens, and those undertaken following an incident that serve to minimize the post-

incident and longer-term business disruption. Since there can be no assurance a facility or system subject to a disastrous event will continue to function normally, activities in both categories were undertaken by all companies participating in the study.

The nomenclature ascribed to preparedness activities differed from company to company, but they are referred to herein as Intelligence Monitoring, Risk Assessment, Preventive Measures, Incident Control, Emergency Response Planning (ERP), Business Continuity Planning (BCP) and full Business Recovery Planning (BRP). *Figure 1* shows how each function interrelates before and after an incident.

Figure 1: **Components of Preparedness Management**



Source: Internal Analysis, Secondary Research, Interviews

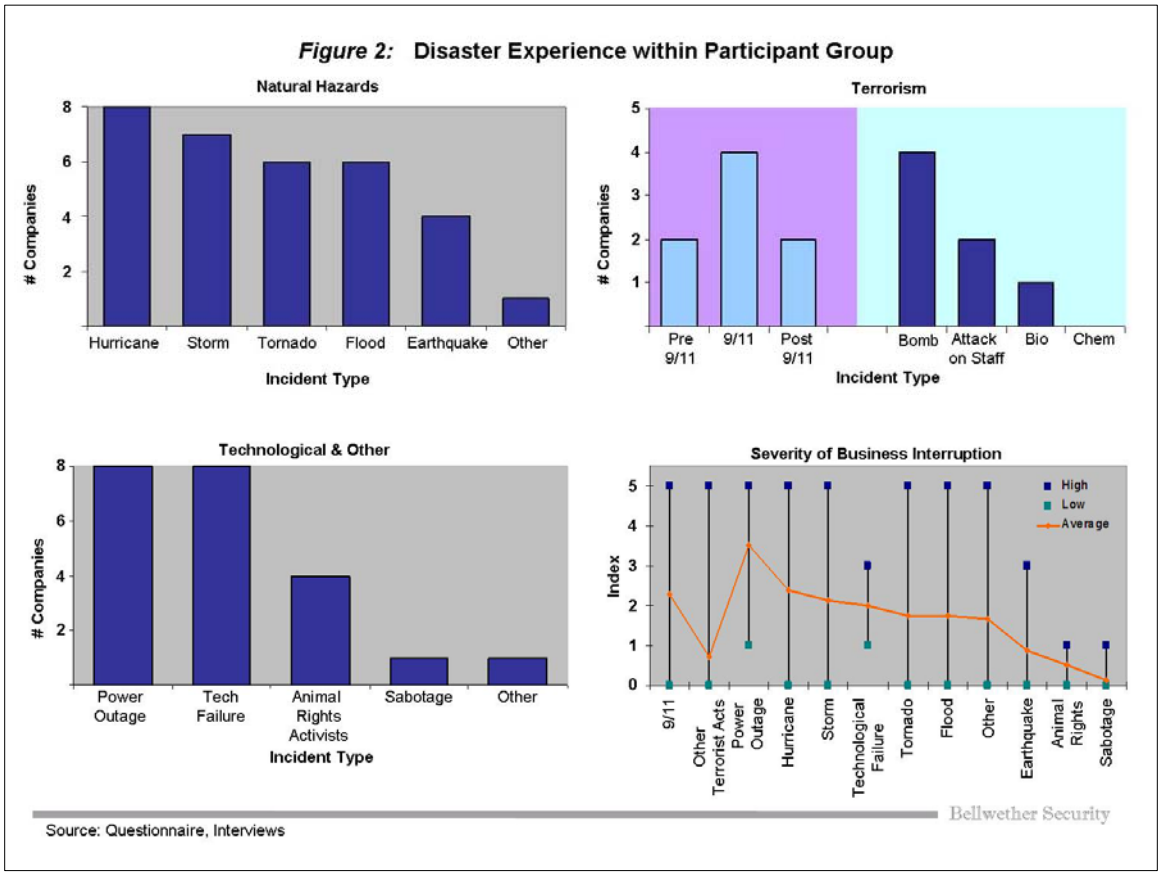
Within the companies studied, Intelligence Monitoring, Preventive Measures and Incident Control typically fell within the purview of Corporate Security. Emergency Response Planning also fell under Corporate Security in approximately half the group but was either incorporated independently, within Business Continuity Planning or business operations at others.

Business Continuity Planning was typically a separate function and resided within the Information Technology (IT) group at three of the companies participating. Risk assessment, training, testing and maintenance of preparedness plans were often conducted independently by each of the functions.

Companies cannot preclude an act of terrorism or other type of disaster befalling them, but all have made significant investments in preparation for such an event. There was, however, little commonality among the group with respect to their organizational approach.

Terrorism and Disaster Experience

As a group, the participants have had substantial experience with disasters: over 60 occurrences in 15 categories were evaluated. Terrorism accounted for nine incidents, of which 9/11 directly affected four of the participant companies. In addition to 9/11, the companies experienced five other acts of terrorism; one of which resulted in a significant business disruption. *Figure 2* illustrates the disaster experience within the participant group. Natural disasters predominate within the group's experience with most companies having experienced business disruptions arising from hurricanes, tornados, winter storms and flooding. Nearly half the group had experienced one or more disruptions from earthquakes. In addition, all companies had experienced business disruptions from both power outages and other types of technological failure. Minor disruptions were also reported from animal rights activists and other types of sabotage.



Given that all companies have had real disaster experience resulting in business disruption, their preparedness planning represents not only a business need based on

experience, but also operational insurance in anticipation of terrorism and other hazards. The possibility of a future act of terrorism affecting them in the US was viewed very seriously by these companies.

Risk Assessment

The process of assessing risk at each company was generally undertaken by each of the functions involved in corporate preparedness. Risks associated with facilities, equipment and business processes were evaluated by the security, emergency management and business continuity functions independently, but often not integrated or coordinated. Although all companies had a corporate risk office, these were typically focused on currency and commodity hedging, insurance, etc. Typically they did not take the lead in assessing threats from a preparedness standpoint, although they reviewed preparedness plans in some cases.

Most companies assigned criticality ratings to both facilities and business processes based on the importance of business function to the enterprise overall. For example, company headquarters, datacenters, trading floors, and research and development laboratories were deemed most critical, while sales offices and smaller administrative functions less so. Most mapped their facilities by size, location and the business processes conducted at each. This methodology resulted in a criticality scoring enabling each facility to be grouped (typically into one of three tiers) to identify the appropriate level of mitigation. Business continuity functions were more typically focused on business processes and systems reflecting their IT roots. Criticality ratings were used by participating companies in conjunction with corporately determined guidelines and policies addressing the appropriate mitigative response. Although less common, a few companies mandated the response as a corporate requirement based on the rating. This was generally considered a preferred practice.

Since 9/11, all participating companies believe they are now more likely to experience incidents with the potential to disrupt their business and have enhanced their risk assessment procedures in response. Assessment of their vulnerabilities and the potential impact (from terrorism and natural disasters) on their businesses has been considerably more robust. Despite this, risk assessment was still approached in many different ways within these companies. Quantitative methodologies and cost benefit assessments were generally less prevalent with the exception of a few companies. Although there was no common approach, companies had done a good job of focusing their planning and resources around core business areas and identifying requirements to survive potentially disastrous situations arising from terrorism and other threats.

Half the companies participating in the survey had automatically linked their corporate response to the DHS threat advisory system and half had not. Of those that had, responses were aligned with Orange and Red level advisories. Companies that were not automatically linked stated they would take the advisory into consideration along with other factors and determine their response based on this broader set of facts. Actions considered include: travel restrictions, stay-at-home directives (particularly for non-

essential personnel), facility closures and the relocation of certain business processes. Each company had different needs based on its industry, configuration and geographic footprint and had tailored its response accordingly.

The risk assessment process varied considerably from company to company. It was undertaken independently by most preparedness functions and often not fully integrated within each corporation. Given the significant resources allocated to preparedness overall, as well as its importance, it is likely that companies could benefit by integrating enterprise risk management better and coordinating it at a more senior level.

Preventive Measures

Preventive measures are those investments that are made to reduce the probability of a disastrous incident occurring, such as flood barriers, or to reduce the effect should such an event occur, for example, window film to reduce flying glass from an explosive blast. They represent a first line of defense in corporate preparedness along with the gathering and evaluation of intelligence related to incident probability, such as hurricane warnings, storm and other threat advisories.

Given the wide range of threats companies face and the commonality of effects that can occur, companies have concentrated their investments into areas that mitigate multiple threats wherever possible. This makes their efforts both more effective and efficient. For example, back-up generators and batteries mitigate many types of natural disaster as well as technological ones such as power outages. Disaster kits and designated facilities to "shelter-in-place" help protect employees in several different types of emergency situations and are becoming more prevalent throughout these companies. Access control and surveillance systems help reduce the likelihood of traditional security concerns such as theft and workplace violence, as well as deter potential acts of sabotage and terrorism. Procedures addressing threatening calls, background checks, mail processing and deliveries have also been enhanced at many companies. Many of these preventive measures mitigate terrorism in addition to other threats, although some are specific to it.

All companies increased expenditures in preventive measures post-9/11, and most continued to do so in 2004. Increases were reported across-the-board with access control commonly reported as being the most enhanced preventive measure. Other building hardening measures for example, barriers, glass reinforcement, and additional guard services were also employed particularly at critical and locationally-sensitive facilities, i.e., major cities, specifically in response to terrorism.

One of the more challenging areas for companies has been that of ensuring compliance with corporate security policies within multi-tenanted buildings where the company is not the owner or anchor-tenant. Frequently, tenants have different security needs, and leases pre-date recent enhancements to security policies. Renegotiation and a willingness to fund enhancements or invest in parallel systems were often required. The difficulties with multi-tenanted buildings challenged these companies in applying their own security

polices in such situations. Municipal code addressing security will definitely help, but this is slow in coming and will not address every company's need.

Post-9/11, all companies significantly increased their investment in preventive systems and procedures; however, since they cannot preclude the possibility of a disastrous or catastrophic event befalling them, they have also invested substantially in Emergency Response and Business Continuity Planning.

Emergency Response Planning

Companies have generally adopted an "all-hazards" approach to emergency management. This is considered the most effective and efficient method given the commonality of effects and overall business need to continue operating and/or recover quickly.

All companies had Emergency Response Plans (ERPs) and Incident Command Systems (also referred to as Crisis Command Systems) in place. Ownership of these plans typically resided with the business units and core business functions but was coordinated at the corporate level. In about half the companies, coordination was directed by the corporate security function. In some cases, companies had a dedicated emergency management office which incorporated business continuity. Incident or Crisis Command Teams were generally widely represented with members (and alternates) designated from Security, Safety, IT, Operations, Legal, Human Resources, Public Relations and Facilities/Real Estate departments. Either upon or before (where warnings are received) declaration of an emergency or crisis situation, these teams convene to manage the corporation's response.

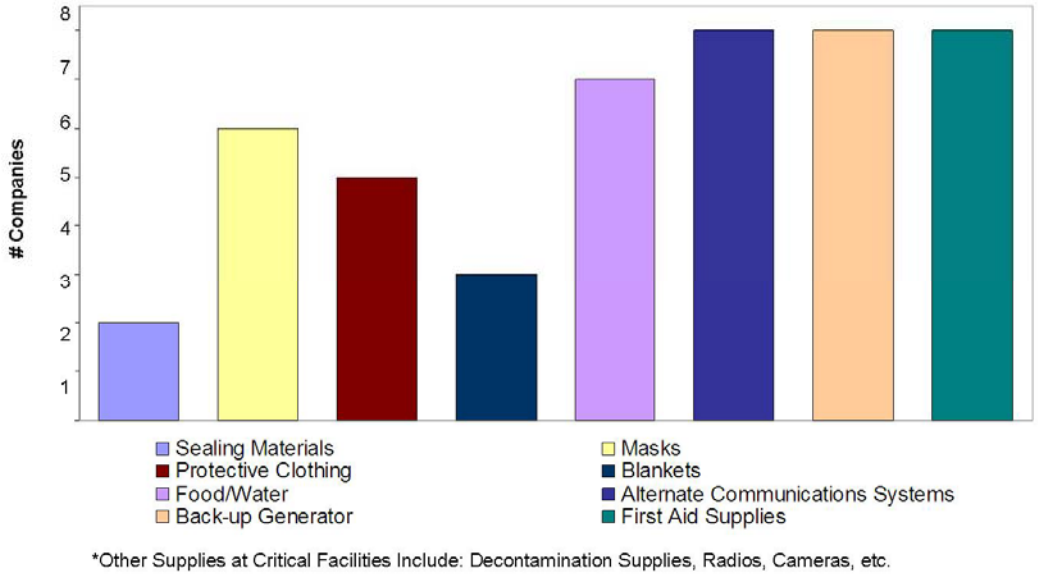
Most companies had designated command centers for critical facilities and for their corporate leadership teams. In addition, most had alternate off-site centers available to take over in the event that a critical facility is unusable. Command centers were generally equipped with independent power, alternate communications systems, dedicated seating, PC equipment and emergency communication software. All companies have undertaken tabletop exercises and many have practiced more extensive drills.

Drilling was considered very important as an addition to awareness training. Evacuation drills were performed either annually or semi-annually. Most companies have undertaken tabletop exercises and emergency drills at most critical facilities, and some did so on a regular basis. Most have performed drills involving all employees at these facilities at some time or another and about half the group has practiced drills on a surprise or after-hours basis. Most have brought in third-parties, such as local fire and EMT departments, in some drills and their inclusion is generally increasing. Senior management has been involved in drills at more than half the companies. In addition, some companies have experienced the need to convene their crisis teams in response to real situations (most recently hurricanes Katrina and Rita in the US). These companies have accrued considerable real disaster management experience. Extensive drilling is

less necessary at companies regularly experiencing real situations, since the lessons learned there substitute for those determined through simulated exercises.

Emergency supplies and emergency information kept on-hand varied from company to company. All had basic supplies and information at critical facilities (see *Figure 3*) and some kept extensive supplies at all qualifying facilities (over a minimum number of personnel). More than half the group had designated "shelter-in areas" at many of their facilities and a few had them at all qualifying facilities. Many companies distributed disaster kits to personnel and encouraged their employees to develop personal emergency contact lists for their families in the event of a disaster. While this area is still undergoing considerable improvement, these companies are currently much better prepared in these respects than prior to 9/11.

Figure 3: **Emergency Equipment and Supplies Kept On-Hand at Critical Facilities**



*Other Supplies at Critical Facilities Include: Decontamination Supplies, Radios, Cameras, etc.

Source: Questionnaire, Interviews

Bellwether Security

In general, participants had prepared comprehensively for emergencies, and their plans matched their needs based on industry, complexity and geographic footprint.

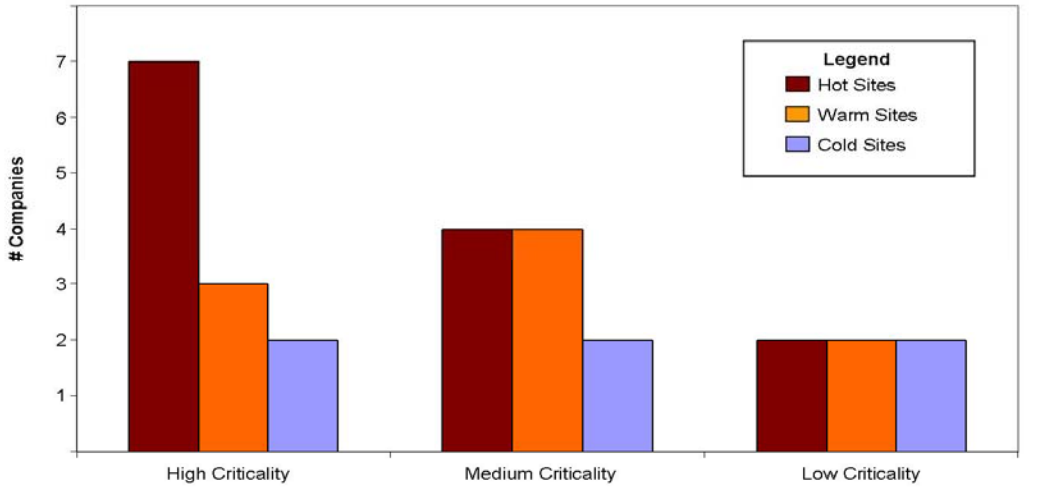
Business Continuity Planning

Companies participating in the survey varied more with respect to Business Continuity Planning (BCP) than in other preparedness functions. This reflected a number of factors. Firstly, certain companies were subject to regulatory compliance and had extensive business continuity plans for many years. Secondly, business continuity generally has its roots in IT and was originally focused on redundancy within each corporation's IT

infrastructure. It is only more recently that business continuity planning has been more widely undertaken as a corporate practice. Some companies only began to practice it beyond IT after 9/11, and their processes and capabilities are considerably less developed than those that have been doing it for longer. Thirdly, some companies are more "mission-critical" and have combined their BCP functions with Emergency Response Planning with the result that blended capabilities have different features than when practiced separately. These factors have all contributed to the greater degree of variation observed around the manner in which participating companies ensure business continuity.

All companies had a formal BCP program office. Business continuity plans were typically owned by the business units and coordinated through this office. The extent of system redundancy and availability of alternate processing capabilities and sites depended on regulatory requirements, the maturity of the function, and the nature of the business and related cost constraints. The criticality of business processes and of facilities in general drove business continuity needs. All companies had hot sites available for critical processes/facilities and some for lower-criticality units. Warm and cold sites are less expensive to maintain and were more prevalent as back-ups for lower criticality processes/facilities. Companies are increasingly building additional capacity and system redundancy into new facilities to diversify their geographic footprint and provide greater operational flexibility in emergency situations. *Figure 4* illustrates the use of hot, warm and cold sites by facility criticality.

Figure 4: **Availability of Alternative Sites by Type and Facility Criticality**



Note: One company did not respond

Source: Questionnaire, Interviews

Bellwether Security

Business continuity planning was generally found to be robust with comprehensive redundancy policies in-place, recovery objectives articulated and alternate processing sites designated. Most also had emergency contracts in place and maximum permissible outages assigned. Some also had entered into mutual-aid agreements, although this was

less appropriate in some industries than in others. Many companies had undertaken rigorous assessments of the business continuity capabilities of their third-party service providers, while others stated that this was an important component of their future planning. Clearly, to the extent that companies are critically dependent on third-party suppliers and have not evaluated their ability to continue to supply and provide services should a disaster strike, they may be vulnerable despite thorough preparation within their own enterprises.

Maintenance procedures pertaining to business continuity were generally represented as robust throughout the group. All companies routinely backed-up critical business information at off-site locations. Business continuity testing was more variable across the group despite being very thorough at some. Full scale and functional disaster simulations were only performed widely and frequently at about half the group. Plans for full business recovery following a disaster were generally less comprehensive. Certain companies had not addressed full recovery at all; those that had generally included it within business continuity. Only two companies had detailed plans for business functions considered less critical in the short-term such as training, professional development and other human resource activities.

Generally, companies were more advanced with respect to their IT continuity but have invested more heavily in broader business continuity capabilities post-9/11. Business continuity planning is time-consuming and requires significant resources. For those who have engaged in this more recently, there is still much to do.

Organization and Management

In general, there was no common organizational model for preparedness within the companies studied. All companies had dedicated corporate functions responsible for security, emergency response planning and business continuity. Two had combined ERP and BCP under one roof, while ERP was the responsibility of corporate security at most of the rest. BCP was managed by IT at three companies and typically by Corporate Services or Operations elsewhere. Only in one company did any of these functions report directly to the President. At the others, preparedness functions reported in through the General Counsel, IT, or a corporate administrative function, such as Chief Compliance Officer. With a few exceptions, the CFO was typically not responsible for any preparedness function at the corporate level.

Regular preparedness briefings were common communications with business units but were more typical on an "as necessary" basis for senior corporate leaders; only one company provided a regular report to its Board of Directors. Preparedness plans were audited internally at half the companies but externally at fewer. They were reviewed by internal risk management or insurance underwriters at over half the companies. Sign-off procedures differed and were not standardized within the group.

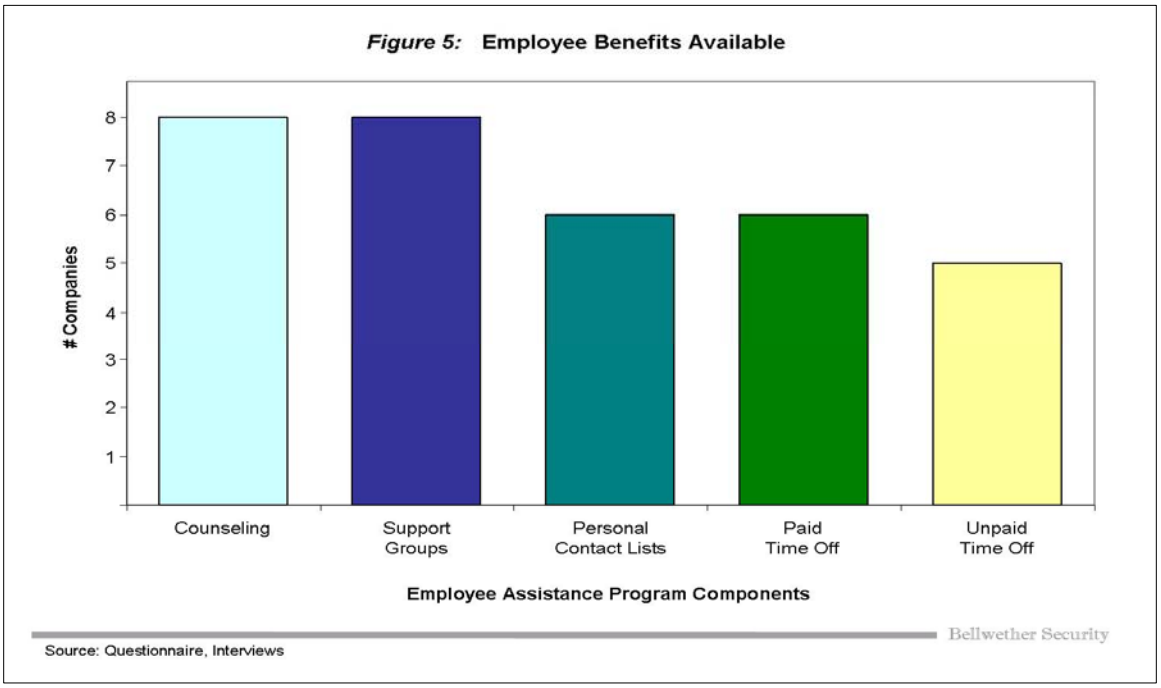
Corporate preparedness as a practice is relatively new in its current form at many of these companies and not fully integrated into day-to-day activities. All companies undertook their preparedness activities in-house and little was outsourced.

Several different functions contribute to corporate preparedness within participant companies. Resource allocation might be more efficiently accomplished if these were coordinated within a single corporate function rather than across several.

Employees and the Workplace

All companies were extremely concerned about the well-being of their employees and had undertaken a number of measures to help them before, during and following a disaster that could affect their families. Participants regarded their employees as their "biggest asset". Helping prepare them to deal with a disastrous situation at home was an important component of enabling them to contribute as fully as possible at work.

As part of preparedness planning for employees, companies have encouraged personal contact planning for their families, developed work-at-home polices and capabilities where appropriate, issued personal disaster kits, planned transportation alternatives, and involved their employees in awareness training and emergency drills. Participating companies indicated that they would assist with personal relocation, provide counseling, organize support groups and allow time-off to help affected employees recover as quickly



as possible. Companies often cited the ability to contact employees, ascertain their status and direct advice following a disaster as a continuing concern despite the enhanced contact technologies available.

Figure 5 demonstrates the number of study participants prepared to offer services and benefits to employees before and following a disaster. Companies also considered other benefits such as personal loans, assistance with relocation, etc. on an "as needed" basis.

While not all companies had undertaken support planning in all areas, all had substantial programs available and were far better prepared to help employees with their personal needs than at any time in the past.

Best Practices

All companies had developed or incorporated best practices within some aspects of their preparedness planning. Every company employed specific practices or processes that enable them to perform better in certain areas. Many of these were developed in response to specific incidents or circumstances not experienced by others. These practices are characterized by superior performance reflected in lower cost, higher effectiveness or both.

Numerous best practices were reported in many categories by participants both within their enterprises and at other entities with which they had familiarity. These categories included threat warning systems, access control, air protection, crisis management, risk assessment, surveillance, employee protection, business continuity, perimeter protection, mailroom and delivery security, communications and training. Several best practices were identified by the group within each category. For example, those applying to access control included a single global access card, visitor ownership, third-party supported x-ray capabilities (for bag checking) and biometric authentication. Examples for other categories are included in Appendix A. No company participating in the study employed all the best practices identified, but most employed many of them.

Each company determined what was appropriate from their own point of view by assessing whether the anticipated benefits warrant the investment and on-going expense associated with the practice. Companies participating in the survey had an opportunity to identify and evaluate best practices performed at their peers. The roundtable discussion provided a forum to do this and certain participants found the best practices put forth at the roundtable forum valuable in enabling on-going dialog between themselves. The merits of each best practice require careful evaluation by companies to determine whether they are appropriate under each specific set of circumstances.

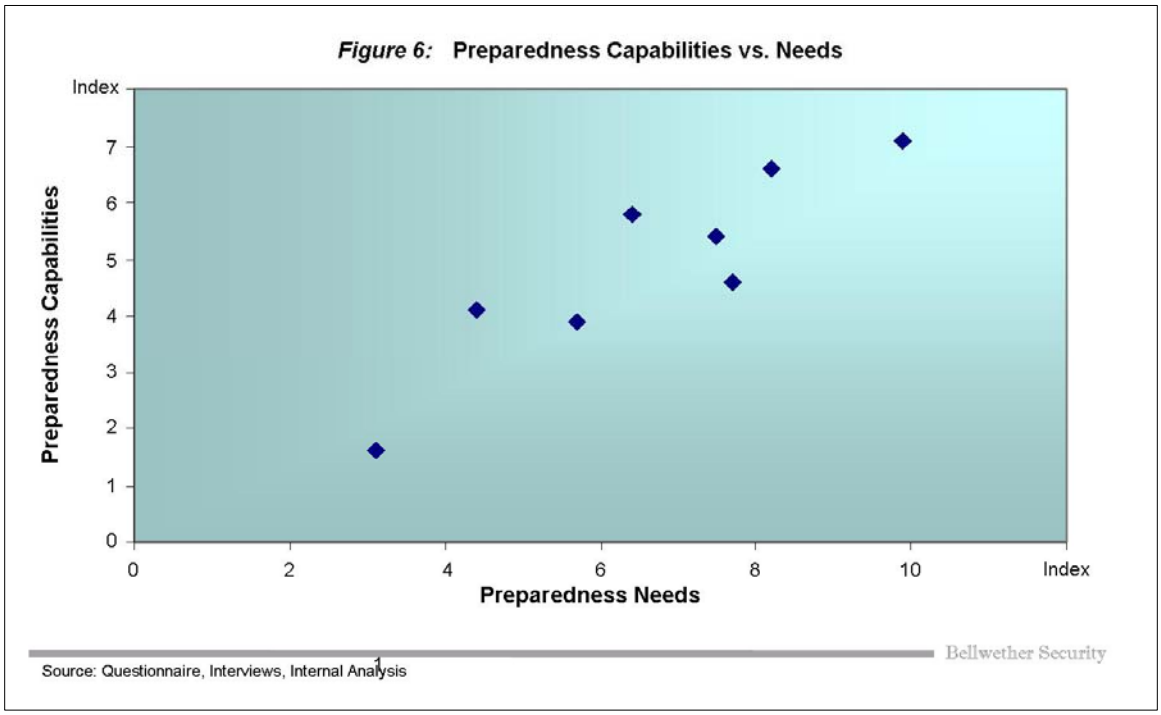
State of Corporate Preparedness

Companies have substantially different needs that determine how they must prepare for and manage potential terrorist acts and other types of natural and non-natural disasters. These differences come about as a result of the different industries in which they compete, different infrastructures, the concentration of business processes and their geographic footprint, particularly where they are in downtown target city locations. The number and type of facilities, business processes conducted, number of employees and

regulatory compliance requirements were all considered important determinants of corporate need.

In accordance with these different needs and their ongoing experience with disaster situations, companies have organized their responses with different emphases. For example, larger, more complex entities have more extensive and complex preparedness strategies and capabilities in-place. Financial service companies have more extensive business continuity infrastructures. Companies with critical facilities located in major cities are more concerned about terrorism than those located more remotely. Those dependent on complex supply chains are more concerned with the security of third-parties than those less dependent. The extent and sophistication of the preparedness functions reflects these different needs.

Figure 6 shows each company's aggregate preparedness capability in relation to their needs. Companies participating in this survey had preparedness capabilities in place consistent with their complexity, geographic footprint and regulatory needs.



The application and refinement of this methodology into a Preparedness Index allows companies the opportunity of gauging their degree of preparedness overall. This could be very useful to companies outside of this study in determining whether it would be appropriate for them to undertake additional preparedness planning, or not. Such an index could also provide a basis for indicating in what areas additional undertakings might be most warranted by comparing the components of each preparedness function. This approach is a valuable tool in assessing preparedness and for helping companies improve their programs.

Conclusion

The companies participating in this study have all responded to the terrorist events of 9/11 and are now much better prepared than before. Terrorism is now taken considerably more seriously in the US, and together with the onslaught of recent natural disasters, preparedness is now "top-of-mind".

Development of, and investment in, preparedness programs has continued post-9/11. Larger, more complex organizations require a considerable amount of time to apply new standards and integrate them throughout their enterprises. Consequently, there is still much work in progress arising out of initiatives developed in response to 9/11.

Corporate preparedness strategies are relatively new and still in their infancy. Multiple functions are involved in preparedness, and in some cases are not as well integrated as they might be. Multiple accountabilities and organizational models abound and nomenclature is not standardized. Integration with the senior leadership process (briefings, etc.) also varies considerably. Risk assessment is fragmented, and enterprise threat management is still emerging as a corporate competency. Despite this, the participating companies probably represent the corporate "state-of-the-art" today.

Future evolution of corporate preparedness will likely involve more integration amongst preparedness functions and more coordination of risk assessment within an enterprise risk management framework. Resource allocation, efficiency and the "bang-for-the-buck" will likely all be better when this is further developed. Overall preparedness can be more effective and efficient under these circumstances.

Companies that evaluate and mitigate enterprise risk from an overall perspective, and integrate their preparedness functions accordingly, will improve preparedness overall.

Appendix A

Examples of Best Practices Reported by Participating Companies

Access Control

- Single, Global Card
- Visitor Ownership
- Supported Bag X-Ray
- Biometric Authentication

Air Protection

- Secured HVAC
- Air Filters
- Air Monitoring
- Complete Air Control

Business Continuity Planning

- Business Unit Owned/Program Office Coordinated
- Automatic Compliance Reporting
- Same 3rd-Party Standards

Communications

- 24/7 On-Duty Support
- Automated Call-Out
- IP-Based Public Address System
- Corporate Crisis BLOG

Crisis Management

- On-Duty Teams
- Dedicated Crisis Mgmt Teams
- EM Activation Protocol
- Off-Site Alternatives

Drilling & Training

- Full Scale Exercises
- Surprise Drills
- Public/Private Drills
- Iterative Training

Employee Protection

- Blast Resistant Film
- Travel Tracking
- Personal BC Plans
- Decontamination Capability

Mailroom

- Hardened Stand-Alone
- Chem-Bio Detection
- Metal/X-Ray
- Autoclaving

Perimeter Security

- Visitor Center/Busing
- Controlled Parking
- Intrusion Detection
- Smart Surveillance

Risk Assessment

- Integrated Evaluation
- Security Approved Leasing
- Business Process-Driven Criticality
- Real-time Application

Surveillance

- Integrated DVR
- Work Place Violence Program
- Smart Systems
- Regional Security Control Centers

Threat Warning

- Internal Intelligence Unit
- Radiological Sensors
- Travel Advisories
- Threat Advisory Response Manual