

Throughout the WTC response and recovery, surprising problems and little known capabilities combined to present organizations with both unfamiliar challenges and opportunities for ingenious solutions. In this section we present the main lessons that emerged from our research. They pertain to the ways in which information needs, resources, technology, and policies interacted with planning, preparedness, coordination, and collaboration among the involved organizations. These lessons apply not only to emergency planning and management agencies but also to any government, private, or nonprofit organization. Throughout the remainder of the report, we include quotes from our interviews that capture the main lessons in the words of the people who experienced them. We cover five topics.

- Availability, quality, use, and management of information
- Nature, strengths, and weaknesses of available technology
- Role and effect of existing plans, programs, procedures, and relationships
- Information policy issues
- Communicating with the public

### Availability, quality, use, and management of information

*"Although we have always thought data was important in an emergency, I now think probably it is second only to the first responders' courage."*

Information to support the response was a critical concern. For everyone, information needed to be relevant, sufficient, accurate, timely, and accessible. For first responders, it also needed to be constantly updated and usable by people in extremely hazardous conditions. None of the information resources used in the response and recovery had all of these qualities, and many compensating compromises were made to get information into the hands of those who needed it in a form that would help and not hinder their activities or safety.

#### Relevant data

*"What you need to be prepared for in an emergency, what you have to have prepared, is the data elements that go into supplying field forces with the data they need to respond."*

Relevant information, that is information suited to its intended use, was needed to support emergency and recovery operations of all kinds. Ideally, this information would be organized in a way that is easily accessible and readily usable by those who need it. However, many interviewees told us they lacked a useful understanding of critical information systems and data sets that would be relevant to either immediate response or long-term recovery. This understanding was developed in a limited way on the spot and the result was often frustrating and fraught with gaps and inadequacies. Available information was often out of date, at the wrong level of detail, or incomplete. Analysts and managers spent a great deal of time and energy trying to evaluate and improve the relevance of these data resources but, as one interviewee observed, "a crisis is not a time to be making decisions about data processes."

Relevant information about some topics could not have been acquired in advance because the information pertained to the event itself. For example, the need for aerial imagery to assess the extent of damage and understand how to approach the rescue effort and fires on the debris pile at Ground Zero demanded that new data be captured. This was accomplished by using fly overs of the site with both standard and advanced forms of photography and remote sensing. In this case, the data could not have been gathered in advance. However, interviewees noted that knowing in advance **how** to acquire and distribute such information would have been of great value.

In addition, relevance was an ever-evolving concern because the nature and priority of information needs changed over the course of the response and recovery. While immediate emergency response required information to support rescue activities and deal with imminent danger, later work depended on detailed information about equipment, organizations and individuals on the site, victim identification, service offerings and locations, buildings in the surrounding area, public health threats, and other topics.

Interviewees offered several strong recommendations for increasing the amount and usability of relevant information. They emphasized the need for all organizations to create and maintain complete inventories of data resources and information systems. Had these existed, emergency managers and supporting organizations would have been able to direct their attention immediately to data analysis, rather than to data search and evaluation. This was not at all the case in the WTC response. Even routine hazard information, such as chemical fact sheets,

was unavailable and this lack of information contributed unnecessary uncertainties for the response and recovery workers about the conditions of the site and surrounding area.

Others described how prior agreements about predefined initial information products, including standard reports and maps, would have aided both decision makers and the public. Lacking these, multiple versions of reports and analysis were invented as the event unfolded. According to one respondent, "There [were] problems ... collecting . . . data on the site because none of the templates and the formats had been prepared ahead of time, none of the coordination between the gathering bodies had been worked out ... It all had to be done on the fly." Respondents said that basic decisions about report topics, frequency, formatting, size, color-coding and so on could all be made in advance. While these pre-defined information products would surely need to be amended to fit a particular event, they would form a sound foundation of well-understood relevant information for a variety of users and uses.

### Data availability and usefulness

*"[At] different points there was certain utility data that we needed to get, data that was considered reasonably sensitive by the utilities... We did get it but it's scary to find out that the data's just in paper form and we ended up having to digitize it ourselves. . ."*

In some cases, needed information existed but was not accessible or in usable form. In others, the amount of information was simply inadequate. As a result, emergency crews had almost no usable data during the first 24 hours after the event. For example, New York City officials estimated that only 25 percent of the information that emergency crews needed existed before the event, and most of that was lost, at least temporarily, as a result of the attack. Most of the first week was spent rebuilding pre-existing data capacity. Interviewees recommended that response planning include special attention to building and testing various event scenarios specifically to determine what data would be sufficient for a first response and how it could be organized and delivered in a timely manner.

At the state level, interviewees believed most of the data they needed already existed, but it was not always readily available or usable. They sometimes lacked written procedures for key activities associated with data selection and management, and some of the data they had lacked the detail necessary to make it immediately useful. For example, contact lists of technology suppliers were used extensively, but often contained little more than company name, address, and general categories of products. Today, those same directories are being revised to include the identity of specific individuals to be contacted in emergencies and details about products and categories of expertise that each business might bring to a new crisis.

Other essential information existed but could not be readily accessed or used. For example, the WTC site was the location of a number of hazardous materials. These had been cataloged years before, but this information existed only on paper and was located in Albany. It took days to find and make use of the information. Once it was located, the information turned out to be too general to be very helpful. Sometimes valuable information necessary for re-establishing normal operations in non-emergency organizations had been kept only on paper, such as legal files for cases in the process of litigation. This information was either destroyed or made inaccessible due to the closure of buildings that needed thorough inspection or repair before they could be re-occupied.

Nevertheless, critical information replicated in different locations did allow for quick recovery of most City services and large businesses. Thanks to planning for the Year 2000 (Y2K) date change, and to standard practices for disaster recovery, most organizations had back-up files of key data. However, back-ups were not always kept in remote locations and sometimes had to be retrieved from quarantined buildings. Sometimes duplicate data sets were not the result of planned back-up procedures or business continuity plans. Rather, data were sometimes replicated just for ease of use, to alleviate bandwidth problems, or for other business reasons. Perhaps the best known instance of this kind of duplicate data was the City's GIS base map, NYCMAP, which was replicated at Hunter College under a contract for quality control work. When the EOC collapsed and the City's IT office in lower Manhattan was closed for safety reasons, the files and associated hardware and software at Hunter College allowed for the quick and effective re-establishment of GIS data services.

### Accurate data

*"We got data from the state about underground fuel storage and freon and it turned out that this was very critical data, but the way it was captured was very vague as to exactly where it was . . . We spent days and days trying to figure out the exact location."*

Accuracy is a combination of both factual correctness and appropriate level of detail. A NYC official who was involved in preparing data about structural features, such as shafts and fuel storage facilities under the Trade Center, indicated that the existing data was vague and ambiguous, thereby rendering it mostly unusable by first responders. This kind of experience highlighted for many the need to develop and consistently employ data standards to guide routine collection, storage, updating, and delivery of building data that is accurate at various levels of detail from building footprints to wiring diagrams.

One NYC official who worked at Pier 92 told us about the earliest efforts to prepare data for responders. ". . . first of all in terms of accuracy, nobody would stand behind any of it. And that was all very clear . . . all that was being mapped to just try to get some picture of what was there and to give the first responders a leg up in terms of possible voids, maybe where there were shafts and that kind of thing. It was mostly for them to use on the site to prevent their own accident. You would not want to do that on the fly again; that's why I'm probably going to dedicate the rest of my career to getting this data now and having it, just in case."

Moreover, several respondents discussed the importance of documenting data characteristics through meta data that states ownership, provenance, definitions, limitations, data collection method, and timing, and so on. Very little meta data was available to help analysts and users understand the appropriateness and reliability of data for various uses. In addition, little attention could be paid to records management or archiving because no protocols had been set up in advance. These were low-priority activities in the first few days, although they received increasing attention as data analysis activities expanded.

### Timely data

*"You may normally want to get 95% or 90% complete data, but it may be better to get 75% in some cases but get it out so the people can use it."*

Relevant and accurate data that is not available when needed fails to serve much purpose. As the response activities got underway a variety of new data sets were contributed by or collected from both public and private organizations. Processing and delivering this information to first responders and rescue planners in a timely manner took on extreme importance. Although everyone was concerned that incomplete information could be harmful in some way, the pressure to get information into the field was intense. One respondent commented that it is sometimes better to collect less data if it would be more usable and able to be communicated to others faster. "You don't want to give anybody bad data or bad analysis or anything like that but if the color's not quite right or the legend isn't right or whatever, that is secondary to getting the information out."

One interviewee recalled a debriefing meeting in November 2001 in which the fly overs were discussed: ". . . this digital ortho imagery, it was pretty nice and . . . you got it down to six or eight hours and it was driven down to the city . . . [But] it wasn't good enough . . . it was good for what we needed for other things but it wasn't good enough [for those first days]. I need something in two to three hours. And in fact, we took somebody with a digital camera and put them in a police helicopter to film the fire every day 'cause we just needed to see a picture of where it was. We used the other stuff . . . but we need something else; we need something much quicker."

### Spatial data and geographic analysis

*"The spatial element enables data that you have to be brought to that higher level [of usefulness] by being able to integrate it, analyze it, and present it in ways that you just can't do conventionally."*

Interviewees pointed out that an emergency is almost always a spatial event. Consequently, mapping and geographic data analysis were crucial to response and recovery efforts, and to providing public information. The visual aspects of spatial data make it remarkably versatile and suitable for a wide variety of audiences, including expert analysts, emergency response teams, policy makers, and citizens. The use of maps to convey status and safety information is one of the unquestionable success stories of the response.

Spatial data provides a comprehensive view of many different attributes of the geographical region impacted by the emergency such as physical geography, critical infrastructure, building footprints, transportation routes, and demographic characteristics. These types of information can be geo-coded (associated with an exact place) which then allows them to be combined, compared, correlated, or integrated to produce new information. According to one participant, the experience of using spatial data "led us to profoundly understand the importance of place and location and organizing data according to spatial attributes because then the data makes more sense from it being combined."

Geographic information systems (GIS) and location-based information services on the Web emerged as the most versatile analytical tool associated with the response. Fortunately, NYC had been developing its GIS base map, NYCMap, since 1998. It was created by combining aerial photos with limited information about the City's physical geography and built environment at both the surface and subsurface levels, all accurate to within 18 inches. Within a day of the event, an Emergency Mapping and Data Center was created within the EOC, drawing data from many different sources, and delivering more than 7000 maps to first responders, public safety authorities, utilities, the media, and others. These maps showed critical and ever-changing information in a readily usable way. They depicted a wide range of information from thermal photography to pinpoint underground fires for emergency workers to subway maps showing the public which lines had been restored to service.

These GIS applications made use of the City's existing investment in digital mapping and data sets, integrated with other GIS data sources pulled from many other organizations. This experience highlighted the importance of having readily available digital maps and layouts of facilities and buildings as a part of the emergency recovery templates. When they can be combined with dynamic event data these maps can become powerful tools in the hands of first responders.

However, as well as GIS performed in the WTC disaster, the spatial analysis team was far from satisfied with what they were able to do. There was no single, authoritative repository or directory of relevant and reliable geographic data that could be immediately deployed. Complete information about utilities and other critical infrastructure was not part of the existing GIS system and was not fully integrated when acquired. In addition, interviewees who conducted spatial analysis said the lack of meta data about the definitions, sources, and usability of the data forced unacceptable delays while they tried to integrate different data sources into something that was usable in the field. Finally, detail-level data for most buildings that described such characteristics as construction materials and uses simply did not exist.

### Data for use by first responders

*"Public safety professionals have years of field experience but don't have much experience manipulating data. We need to figure out ways to educate them and to make sure that they understand the technology so they find it usable."*

A variety of new technologies were made available as part of the response. However, a number of interviewees discussed the difficulties of introducing new information management and analysis tools in the midst of the crisis to first responders who are much more attuned to direct observation and action. During a crisis such as the WTC, first responders are required to make decisions in an environment characterized by extreme stress, danger, confusion, and uncertainty. To be effective in such a state, data for decision making should be presented in a familiar form that does not engender any additional cognitive burden on first responders.

Consequently, we heard strong recommendations for ongoing orientation, training, and practice using new technologies. This will entail finding ways to help first responders, decision makers, and public affairs officers develop an appreciation for the abilities and limitations of data-driven action. Interviewees stressed a consistent list of necessary but currently underdeveloped or entirely missing information strategies. These include organizing data for easy access, using well-understood templates for presenting information to various audiences, pre-designing basic maps using common intuitive symbols, developing and practicing familiar online applications, and adopting uniform data standards. In addition, knowing in advance what kinds of data to bring to a response would go a long way to ensure the right data is used by first responders leading to better outcomes.

During the following winter, prompted by the experiences in the WTC response, an industry consortium called OpenGIS, in cooperation with a variety of government agencies, began to explore a test bed for real time collection, reporting, and integration of remote sensing data over the Internet. Called SensorWeb, it represents a first effort to explore the ways in which advanced technologies can support the information needs of first responders.

### Data standards and information sharing

*"I saw people scrambling to put an information-sharing capacity into place . . . but you can't stop there . . . you really have to dig into the science of who's collecting what data, where, when and why before you can assume that you can throw it all together on a screen and put it out to people."*

Data coordination and integration problems quickly surfaced after the attack, persisted throughout the response, and continue into the present. The lack of data standards (and lack of policies about data standards, sharing, and

coordination) took a significant toll on the response effort. Disagreements among the various levels of government about whose data was most accurate or most suitable for different applications cost precious time in the early days of the response. For example, FEMA has spatial data that covers the entire nation at a standard scale, but local spatial data, while not always standardized, is often far more detailed and suitable for supporting on-the-ground operations. One respondent described how the physical proximity of staff from various agencies on Pier 92 helped mitigate some of these problems. The agencies represented in the EOC needed maps that required information from different sources be brought together. This necessitated decisions about whose data was best for a given purpose. Because so many organizations shared work space on the Pier, they could deal with this problem face to face, "so that resulted in standing around [in a group] and getting people to make a decision as to whose data was better. That data cleaning and integration service was very informal but ended up being the basis for a lot of trust in the product."

Nevertheless, many data sharing problems remained. Environmental health data, a source of major controversy both during and after the event, is collected at every level of government, but there are no agreed upon standards or divisions of labor that make these data resources fit for immediate integration and coordinated use. According to one respondent, "Our problem was that we had everybody doing sampling; some of them were doing sampling in the same way; some of them were doing sampling in a different way; some of them were representing the data the same and some of them weren't." Instead of having data resources that complemented one another, the environmental protection agencies were faced with either competing data or gaps where no one had collected information before.

Moreover, intergovernmental and internal agency conflicts developed around the nature and form of information to be released to the public about environmental health risks. Both political and scientific concerns caused delays and resulted in little useful information being disseminated in the early days of the crisis. In this case, the City and federal environmental protection agencies were involved in monitoring and collecting two different types of local environmental data (asbestos levels and air quality levels). It was essential to integrate these two sets of data with the local GIS data in order to make dynamic zoning decisions that affected the movement of citizens and relief workers. However, this was extraordinarily difficult due to the nature and quality of the data and the lack of agreement about how to report it.

One respondent spoke at length about the importance of data standards and the difficulties associated with not having them. "What I was watching [were] folks from different agencies at all levels of government. . . having a complete inability to relate their data to one another. Neither in terms of who was collecting it and when it was collected, how it was being collected, how it was being analyzed, what it meant, definitions, terms . . . the whole thing was really quite unfortunate. . . It's a major, major issue that affects our ability to respond in emergencies, but it also affects our ability to optimize resources and share information and make good investments."

This problem was evident in a variety of situations. For example, multiple lists of the dead and missing compiled by different organizations needed continually to be reconciled. Multiple addresses and names for buildings was another important data problem. Buildings in lower Manhattan were inspected and re-inspected by six different government agencies before they could be declared safe and reoccupied for residential or business use. The lack of a single accepted building identifier slowed and complicated the process for all concerned. One interviewee described this issue: "The primary difficulty was not knowing the total story of any one facility. So a facility that has multiple floors, data centers, different connectivity points, different vendors supplying connectivity to that building, you couldn't know at any one point in time, is this floor up? Is this floor down? Do we have a connection? Do we not? All of that trickled in as people started touring the buildings and finding out what was working and what wasn't." This experience prompted the City government to embark on a building identification program to reduce or prevent such problems in the future.

## Nature, strengths, and weaknesses of available technology

There is an important technology story in the WTC response. Technology failures, technical experiments and innovations, and professional expertise and ingenuity all played noteworthy roles.

### Telecommunications infrastructure

*"[The loss of the ] Verizon central office was very much a single point of failure for most of our network and most of the City's network... in fact it continues to be an issue today that -- regardless of your vendor, for example, for long distance telephone or data communication service -- they basically lease space or run over Verizon's network."*

The WTC event highlights the importance of defining what constitutes network redundancy and how it should be incorporated into network infrastructure planning. Clearly, having separate service providers who use the same physical infrastructure does not guarantee redundancy or high levels of network availability. Communications networks that were thought to be separate were actually running on the same infrastructure. The Verizon central office at 140 West Street, extensively damaged and rendered inoperable on September 11, was a major telecommunications hub for the City and some of the surrounding region. Although many organizations in the City bought their telephony and Internet services from different providers, nearly all providers ran their services over the same physical infrastructure. The protection organizations expected from separate service providers was therefore never realized. In addition, to a large extent, cellular telephone service depended on antennas atop the Trade Towers. When these were lost in the collapse, neither cellular nor land line telephone services were available for most of lower Manhattan.

A NYC official described the impact on his agency in this way: "We lost phone connectivity and data communications connectivity to all of our downtown locations . . . south of Canal Street. I would say that approximately 2000 to 2500 of our 6000 employees [and] about 2000 of our 4000 network users are south of Canal Street. So we identified that 27 of our 43 locations city-wide were without wide area connectivity . . ."

The impact was not restricted to those locations south of Canal Street but various other sites throughout the city which in some manner or form tied back to the Verizon central office . . . So that's why our impact was much greater than just downtown Manhattan. For the majority of these sites, not only did we lose T1 connectivity but we also lost our ISP and ISDN backup . . ."

Because most telecommunications and utilities in the United States, including New York City, are privately owned and operated, little information about them is shared or coordinated and no comprehensive picture of their relationships exists. Although these systems are often thought of as independent, 9/11 vividly demonstrated that they are actually highly interdependent with each other and with other services. Given this interdependence, the scope and nature of restoration expands in unpredictable ways depending on the seriousness of the attack. Thus, restoring services in an expeditious manner required an ability to quickly determine whether, how, and where these systems could be untangled to be reactivated independently. To coordinate these processes, managers need to have available—in a form accessible in an emergency—inventories of systems and capabilities, plus contact information about employees with the knowledge and skills to do the job. In this case, those charged with restoring services had to work with very inadequate information, setting and re-setting priorities as they learned the extent and nature of the entangled systems. For state agencies alone, more than 2000 circuits serving 40 agencies were damaged or destroyed. Service for public health and safety agencies took top priority, but the process was arduous and unpredictable, and adjusted frequently according to new information gathered in the process of recovery.

Despite these extreme problems, network restoration was still remarkably good under the circumstances for at least three reasons. First, large data networks are designed to be resilient and re-routing could be accomplished for many circuits within hours or days. Second, key operators (primarily Verizon) and government officials were motivated to get the system working as quickly as possible, for obvious reasons. They used every business and knowledge asset available from their own resources and their suppliers to accomplish this. Third, clever means were found to circumvent and compensate for losses of regular network connectivity. The prime example of this third reason may be the City's use of the Ricochet system, a defunct wireless Internet access system that was temporarily restored to operation to provide networking capacity for responders. The Nextel cellular telephone network, which combines cell and radio capabilities, proved to be particularly resilient and useful as well.

### Back up and restoration of data and IT services

*"We had the data but we did have a problem with being able to utilize it, because we didn't have a redundant set of hardware."*

For all organizations, information technology capacity and redundancy are particularly important assets in an emergency. These can be classified in terms of hardware, software, networks, and the physical locations of facilities. On the hardware and software side, for instance, the New York City Office of Emergency Management's (OEM) IT functionality was lost when 7 World Trade Center, which contained the EOC, collapsed. OEM retained its software and data, and was able to load that material on machines and networks installed by the NYC Human Resources Administration (HRA) at Pier 92. This effort demonstrated that a loss of hardware is less important than the loss of software and data if two conditions are met: software and data are properly backed up and maintained off site and it is possible to obtain the requisite hardware on short notice.

Nevertheless, the destruction of IT resources in the WTC created two related challenges. One was the need to replace the functionality of the technology lost in the collapse or otherwise made unusable due to restricted access to many buildings. For example, some government agencies lacked back-up hardware on which to restore lost data. Consequently, even when they had data and software readily available to restore operations, they could not quickly resume business. One NYC official recounted the problems of recovering from the loss of access to the agency's buildings: "... the data was backed up off-site. We had immediate access to the data, but we didn't have the hardware or the alternative data center that we could restore this data to, to continue operations. So this impacted [continuation of our regular] programs ... In some cases, our staff walked up 25 flights of stairs in buildings without power, to retrieve hardware so that we could bring them to alternative sites and get them going again."

The second challenge was to identify and put into operation the new facilities and services (such as mapping) needed to respond to the demands of the emergency itself. The GIS operation in the City had not been a central feature of the emergency operations plan, but after only a day or two it became very apparent that spatial data analysis could be extremely valuable for many aspects of the response and recovery effort. The creation of the Emergency Mapping and Data Center on Pier 92 occurred rapidly with government leadership, volunteer effort, and private donations augmenting a cadre of City staff experts. In fact, the entire IT infrastructures of Piers 92 and 94 were built in this way.

### Internet

*"Are schools going to be open? Are the subways running? ...NYC.gov became an important source of information for that."*

From the beginning, the Internet worked when other networks failed. The World Wide Web and Internet telephony were critical in the early hours after the attack when both wired and cellular telephone service failed massively. The Internet provided telephone and text messaging service to key City officials, was used extensively to keep citizens informed of progress, and was the basis for emergency management applications that allowed workers in different locations doing different jobs to collect and transmit information to shared emergency management applications. The Internet technology was used for internal communications in the EOC as well, which set up its telephone system using voice over IP (Internet Protocol) equipment. Text messaging and e-mail were also critically important to communications among the involved organizations. Experts credit the decentralized nature of the Internet with much of its resilience. However, they also caution that electrical failures and interdependencies between Internet and telephone infrastructures pose ongoing risks for future emergencies.

NYC.gov, the City's public Web portal, was an important source of information for the public during the crisis. Although access to it was interrupted by the collapse of the towers, re-routing of the network was accomplished within hours. Usual applications were replaced with information to keep the public informed of the situation and its effect on their daily lives. Despite tremendous user demand, the site operated smoothly. NYC.gov, a relatively new resource, had been built with a capacity much larger than was necessary for the normal flow of traffic. Therefore, during the crisis, it routinely handled a tremendous volume of news-seeking traffic, which reached four times its peak of usage prior to the attack.

### Wireless, mobile, and remote technologies

*"We got a line of sight ... We put up two antennas and they were back [in operation] because we were shooting across the airways. It worked so well, we kept it. It's now our backup."*

Wireless computing and communication capabilities were essential although not widespread. While "line of sight" is a major obstacle in a high-rise city, wireless networks were used effectively to bring some City agencies back online. The connectivity achieved in these cases was excellent and has since been adopted as a backup technology by at least one major City agency. Thanks to this experience, the use of wireless communications, a technology most had not yet worked with, has been greatly expanded since 9/11.

Much equipment used in disasters is mobile – carried by individuals or installed in trucks, buses, and other vehicles. Use of global positioning systems (GPS) has become more widespread since 9/11 as emergency response organizations have come to understand how this satellite-based technology helps them deal with the age old problem of knowing where their equipment and staff are located at any point in time, as well as where they are needed and what routes they might take to get there. Unmanned mobile technology also played a part. Robotic surveying equipment was deployed at Ground Zero to collect data about the stability and condition of the debris pile in areas that were too dangerous for humans to enter.

Remote sensing was judged to be extremely useful but was not advanced enough to be employed in as many ways or places as were needed. For example, the extremely valuable remote imaging that resulted from the fly overs had to be processed on the ground in Albany and then driven by car to the City each day by the State Police. Several respondents described how much more useful it would have been to have technologies in place that would not only collect the data but also send it directly to analysts and users. Given its great potential, remote sensing research has increased in visibility and funding in academic, government, and commercial venues since 9/11.

### Retrofitting and adapting existing technology

*"We had been working on a project to automate inventory tracking of evidence in the forensics lab . . . and the light bulb came on that maybe they could use it down there in the medical examiners' office."*

Flexible and adaptive use of existing or emerging applications allowed quick response to unexpected situations. For example, a severe weather advisory application for use on the Internet had recently been completed by the City's Department of Information Technology and Telecommunications (DOITT). Designed to give residents directions to shelters and other safe locations, it was quickly modified to notify City residents of changes in transportation systems and availability of housing, water, and electricity. A recently built New York State Police application for keeping track of forensic evidence and DNA samples was immediately installed and adapted for use by the NYC Medical Examiner for the arduous process of identifying victims.

Some technologies were quickly implemented that had never been used in the City before. For example, identification of human remains was a grim task that began as a cumbersome, error-prone manual process in which descriptions and location of body parts was written down by hand and later transcribed and entered into a data base. After a few days, NYC officials searched for and adopted a wireless, hand-held technology that used global positioning and pocket PCs with scanners that could withstand extreme environmental conditions. This allowed data to be collected once, in electronic form, for use in a variety of applications including maps and forensics. Another example is E-team, a collaborative software system for emergency management, that uses the Internet to transmit information collected in a variety of places by different responders and supporting staff. The information is analyzed and integrated and then made available for access by these same workers, giving them a more comprehensive picture of changing conditions and available resources. NYC OEM had already contracted to purchase E-team but the contract had not been completed by September 11. The event prompted immediate deployment with expert assistance from the vendor and experienced users from Florida and other states.

### "Hidden" technologies

*". . . at the moment when a [military] technology could be of maximum benefit for a civilian population . . . please don't be bashful about showing up and telling us how you could be of benefit."*

Surprisingly, helpful and available resources unknown to the responders were not always offered by those who had them. While many organizations in New York, the nation, and the world spontaneously offered technical and humanitarian assistance, some tools that would have been extremely useful remained unknown to the emergency response teams. These tools for working in hazardous areas, such as technologies that could produce clear images despite thick smoke and haze, had been developed for the US military but were simply unknown to the civilian government agencies dealing with the crisis. Formal emergency response protocols rest on a series of official requests to activate various forms of assistance. Eventually, these resources were discovered because, while touring the EOC weeks after the attack, those who had them asked why they had never been requested. Respondents pointed out the consequent need for a readily activated assistance connection across civilian and military lines that would not depend on knowledge of specific resources as the trigger mechanism for communication.

### Technology expertise

*"Nothing we did . . . over the whole duration of the recovery was entirely new to us."*

The expertise and capacity of IT professionals were diverse, widely available, and readily deployable. Both government and businesses were able quickly to supply this expertise along with equipment and software. Staff of the City's HRA built the internal networks on Pier 92 (the EOC) and Pier 94 (the Family Assistance Center) in two to three days, drawing on the expertise and products of its long-time suppliers and its own finely-honed experiences of dealing frequently with smaller technology crises in its many far-flung service locations. The Pier



92 and 94 experiences showed that it does not matter where the IT capacity exists as long as it can be identified, mobilized, and deployed. Thus, as mentioned above, OEM had software and data but needed hardware and networks; HRA provided that equipment and the expertise to install it. Other organizations, like the IT unit of the State Police, were similarly well prepared to act, discovering that the demands made on them were the same ones they routinely encounter in their regular mission, although much larger in scope and duration.

The private sector response in terms of IT products and expertise was enormous and immediate. Many IT equipment, services, and consulting firms assisted affected organizations in all three sectors – public, private, and nonprofit. This response included equipment, software, systems design and programming, loaned facilities, temporary office space, and project management. Among the most important were the case management system in the Family Assistance Center, imaging applications used by the Medical Examiner, and an umbrella data services organization to serve nonprofit service organizations.

### Role and effect of existing plans, programs, and relationships

The emergency called into action a wide variety of existing plans, programs, procedures, and relationships. In some cases, these served the effort quite well. In others, they revealed historical problems that had been taken for granted, or showed how some long-established ways of working needed to be revised for better performance.

#### Preparedness plans and practice

*"We do a lot more drills. We invite a lot more people to our drills.... And also during those drills every aspect of the response is drilled, which really wasn't the case in the past."*

There was universal agreement among the interviewees that emergency response plans are important, but they do not guide specific action in a specific event. Planning provided participants with the opportunity to identify likely threats, think through their capabilities, identify key resources, explore contingencies, and develop action scenarios. This thinking process prepared them with a general framework for action, rather than a blueprint for specific actions.

Most responders have neither the time nor the inclination to pull out "The Plan" when disaster strikes. Rather, they rely on what one respondent called "muscle memory" to know what to do in an emergency. This "muscle memory" is built through practice and drills that involve multiple organizations, and at least one respondent noted that active involvement of related organizations was a key feature of post-9/11 planning for his organization. Most respondents emphasized that practice for emergencies was by far the most important form of preparedness. Whether through drills or actual experience in smaller events, the organizations that had practiced response and recovery activities were better equipped to act decisively and effectively. For some, like the NYPD and FDNY or the State Police and National Guard, this meant carrying out their regular missions on a larger scale. For others, such as the NYC HRA, Consolidated Edison, the City's huge electrical utility, and Verizon, the largest telecom provider, frequent "mini-emergencies" associated with keeping complex operations operational had given their staff the knowledge and experience to act quickly and decisively. NYC OEM is responsible for organizing drills for dealing with possible risks. As a consequence of one of these planned exercises, Pier 92 was empty and available to become the substitute EOC because it had been reserved by OEM for a bio-terrorism drill on September 12.

The response to the September 11 attacks showed that the City of New York did not have in place a coordinated incident command system (ICS) as this concept is generally understood in the emergency management community. Its absence became manifest in the immediate response to the attacks on September 11, when the FDNY and the NYPD established separate command posts and were unable to effectively communicate with each other. As a consequence emergency response organizations that were well-trained and able to act individually are now concentrating on better coordination with other responders.

#### Succession plans

*"When the people who are in command aren't there, are we prepared to handle that?...Continuity that includes a succession planning process is vital. And we never had needed to do that before...where organizations were gone or people who made the decisions in organizations were gone, on the private side as well as the public side."*

One outcome of the loss of the WTC was the stark realization that succession planning is important to any organization at risk of losing a substantial number of its top managers. For example, the executive director and

several top level staff of the Port Authority of New York and New Jersey (PA)—the developer and owner of the WTC and a key agency in the regional economy—were lost in the collapse, as were key personnel in many of the businesses housed there. Many government officials we interviewed mentioned new efforts to build succession into their contingency plans and business continuity strategies.

The death of the top executives of the PA was clearly a loss of strategic leadership, which remained a void for several months. However, the PA also provides an example of a resilient organization that was able to carry out its normal functions despite the loss of its top headquarters staff. A key feature of the PA is its remarkably decentralized structure, both organizationally and geographically. The PA runs four airports, port facilities, office and telecom facilities, a rail transit line, and other facilities in the New York-New Jersey metro area, and thus facilities leadership was in place to manage and secure those places not immediately struck in the attack. The PA has long been known as an agency that promotes from within, so this combination of managerial talent and decentralization provided a pool of expertise from which to draw as it recovered from its losses. This decentralization mirrors large firms that have staff in multiple locations, which can create redundancy and resilience in the face of disaster. Smaller organizations or those operating in a single location regardless of size, such as many of those housed in the WTC, did not have decentralized data and work locations. Organizations like these need to carefully consider succession planning and the delegation of authority to manage and lead the firm in a crisis.

### Professional networks

*"The team started forming with people from the GIS community in New York City, from the private sector, . . . City employees and volunteers as well. We all just showed up; nobody waited to be called; everybody brought what they had."*

Some of the most successful activities rested on years of relationship and trust building among key individuals. Familiarity and trust in the competence of people who had worked together for many years helped the work move smoothly and quickly in the absence of formal procedures. In the GIS effort, a community of practice, called GISMO, had already existed for many years. Its members were immediately mobilized as a volunteer data analysis team that worked for weeks on Pier 92, gathering and managing data, conducting analyses, and producing and refining maps for every organization involved in the EOC.

Key private sector executives had spent substantial parts of their careers in City government. Starting in the earliest hours of the crisis, these individuals volunteered or were tapped by the City staff who knew them. These professionals not only knew their current business capabilities, they understood how the City government worked and could therefore direct and deploy the resources of their companies in ways that were immediately and lastingly useful. There are many examples of this kind of relationship, but one of the most visible and significant was the rapid and sensitive work by Accenture (with no initial contract) to lead the design and implementation of the Family Assistance Center on Pier 94.

Because these professional networks existed, consultants were able to offer their services to the City, and the City was able to tap these services in very short order, without lengthy negotiations. In many cases, consultants and vendors, particularly in information technology and telecommunications, were willing to aid the City with free or reduced-price goods and services, and, in the short term, City staff were able to shortcut the usually cumbersome procurement and contracting systems.

### Formal and informal relationships and structures

*"There were hundreds and hundreds of partnerships. . . starting the second or third day of the operation. People who could help, people who wanted to do different things, community organizations, governmental units, private businesses."*

Formal organizational structures and procedures are inherent in large organizations of all kinds and these formed a backdrop of stability and predictability throughout the response and recovery period. For the most part, organizations played their expected roles according to their formal missions. Yet, respondents described a remarkable willingness by all parties—government at all levels, the private sector, and nonprofits—to abandon or circumvent needless hierarchy or the routine chain of command and do the job as they perceived it. This was not true in all cases—and in some, maintaining the chain of command was essential—but where routine "bureaucracy" would have prevented quick action, key officials at various levels were often able to make use of their experience, network of contacts, and the willingness of both organizational and individual volunteers to obtain information, equipment, supplies, and other resources.

Nevertheless, the notorious "stovepipe" programs and funding streams of government were very much in evidence. Many of the success stories had to do with efforts to overcome or work around them, at least temporarily. Some of the more difficult situations were a direct result of this traditional structure. For instance, the traditional separation of public safety agencies meant no single communication mechanism connected them during the response period. Different radio, telephone, and e-mail systems kept them from sharing early information about the situation and from working in coordination, especially during the immediate response. Since that time, several local, state, and national efforts to build integrated emergency communications systems have begun.

In human services, nearly every service organization, whether public or nonprofit, is organized and funded to carry out specific, stand-alone programs. Their organizational structures, policies, processes, and incentives all reinforce this way of working. Existing procedures and their natural reluctance to share confidential information further emphasized barriers to collaboration. Ironically, interviewees from service organizations involved in the WTC recovery process often recognized that their structures and incentives were working against their goals to serve people quickly and compassionately. A number of them described the frustration of having to ask grieving families to supply information and documentation that had already been provided to at least one other organization. On the positive side, human service organizations clearly recognized how sharing client information could help them deliver better, faster, more compassionate service. As a result they have begun a longer term effort to build an information sharing mechanism that supports both service quality and client confidentiality.

Emergency contracting and procurement mechanisms appeared to be used to great advantage throughout the response period, using established State and City purchasing vehicles where they existed and informal arrangements when they did not. The State Ethics Commission issued an opinion, requested by the State Office for Technology, that under the circumstances the ethics provisions of the Public Officers Law would not be violated if state agencies solicited or accepted gifts from the private sector. Knowing that an eventual accounting would be needed, agencies made some attempt to document the equipment and services they acquired. The state government also established a database for tracking the more than 50,000 offers received from citizens and businesses. This tracking system was operational by September 13. This was easier in Albany, removed from the event itself, than in New York City where the outpouring of assistance was difficult to comprehend, much less manage. One City official described this as "one of our biggest challenges" and noted "initially we realized we were going to need to [account for] this, we tried to set things up with sign out sheets . . . towards the end, looking back, trying to figure out what did we buy, what was donated . . . that was a huge task. . . . Having the ability to put an emergency inventory system in place is really critical." However, from a consultant's point of view the City's willingness to forgo routine processes was essential: "it didn't require that you follow the normal procurement process, which would have crippled everything. It caught up to the process. . . down the road [by] monitoring what was going on." While this relaxation of rules was hailed by nearly everyone we talked to, they all agreed that the whole weight of the former process moved back into place within a few months.

Some unexpected needs, such as the need to fly over Ground Zero to capture remote sensing and visual data, were so unusual that no existing legal procedures or routine relationships could be immediately invoked. The process of securing permission and resources to carry out this effort was invented as it unfolded, with frustrating gaps in understanding and overlaps of authority among people and organizations that had never met or worked together before. Because the fly overs involved civilian, military, local, state, and federal authorities, delays and misunderstandings added to the confusion. One person recalled that it took days to get the effort up and running. "I think everyone now recognizes that we'd like to set up contracts in advance, and specs, and have a company ready to go, so that when something happens, [you] lift up the phone, fly, no questions, everyone knows [what's happening], and they're up in the air and we're getting that intelligence back to us." This interviewee and others recommended that sample contracts and specifications be set up in advance so in an emergency this kind of work can begin immediately.

In a related situation, long-standing traditional tensions between government and the media prevented collaboration for gathering needed data. Almost immediately after the attack, a news organization offered the City a helicopter with a stabilized camera platform for aerial photography but the unprecedented offer was bounced from one organization to another and eventually refused because the aircraft was not a government-controlled asset.

Tensions also surrounded the need to serve immigrants and undocumented aliens in a situation that was considered a crime perpetrated by foreign nationals. Nonprofit organizations, especially, voiced concern that the threat of law enforcement prevented people from seeking the help they needed. In response, the Red Cross set up a large tent in a park across the street from the official Family Assistance Center on Pier 94. No law enforcement personnel provided security services in the tent, so assistance and translation services for people

speaking more than 50 languages could be provided in a less threatening environment.

### Information policy issues

*"How should we now balance a trio of public values—security, privacy, and responsible public access to information?"*

Policies about information sharing, records management, and information security influenced the ability of organizations to use information as an asset in both traditional operations and in emergency response.

### Confidentiality of personal information

*"We need to have a methodology so we can share verifications, we can share basic client information, so that we can really work better with clients."*

Confidential treatment of personal information was a major issue for both public and nonprofit agencies engaged in serving the families of victims. Nonprofit organizations quickly recognized both the value and the difficulty of sharing information about the people they were serving. While they could clearly see that services could be more streamlined and less stressful for clients, strong professional values and organizational restrictions about confidentiality prevented them from sharing information about individuals, which led to frustration for the people being served. In addition, for the first time, many people seeking assistance were middle- and upper-income families who had never encountered the fragmented social service system before. They had never before revealed intimate details of their lives, been subjected to multiple requests for the same information, or needed to verify the truth of their statements, as the welfare system requires.

Nonprofit organizations began to deal with the confidentiality issue with the assistance of IBM, which helped develop applications for social and income assistance to victims. They began to compare the details of their individual confidentiality policies in order to collectively understand how their various policies worked and whether they could be depended on to protect confidentiality if personal information was shared. Eventually, many nonprofits jointly supported the creation of a data management and sharing consortium, the United Services Group, which would help them communicate and coordinate information and services in the future. A number of respondents suggested that a standard emergency confidentiality agreement could help to remove unnecessary barriers to citizen services while preserving essential principles of confidentiality of personal information.

### Information and system security

*"We didn't know what information was in there [NYC.gov] that could be used against us, so we put up just a generic page with emergency information."*

Shortly after the attacks, public officials recognized that the wealth of information on government Web sites could create new security problems. The City's Web site, NYC.gov, was quickly examined for these risks, but the need to be online immediately prompted City officials to simply replace the regular site with one that solely addressed the emergency until time was available to review and bring the full site back into operation. Similarly, some federal agency Web sites were taken off line and later restored with some information removed. At the state level, all agencies were directed to review their Web sites for information that could risk national, state, or community safety. The State's GIS clearinghouse was closed to the public for several weeks for a thorough examination and was restored to the Internet after a small number of data sets and references were removed.

New agencies were created to deal specifically with these newly recognized security threats. At the state level, the Office of Public Security was created as an immediate response to the State's security needs. The new US Department of Homeland Security has significant information security programs and a broad portfolio of activities that depend on new sources and uses of information to identify terrorists and terrorist activity, which are themselves raising important policy questions associated with personal privacy and civil liberties.

Across the whole spectrum of organizations, and despite well-known barriers, new information sharing and integration goals have emerged, raising some new perspectives on information security. One private sector executive described them in this way: "[This experience] changed to some degree the perception that you can have a physically secure facility and that would be adequate. What you really need is [attention to] the people and their intelligence and their information wherever they may be and they may need to be. . . You think now of that command and control as being a network of communications."

### Public Communication

A primary concern for public managers in emergencies is to communicate important information to citizens, particularly if that information is intended to influence public behavior. The nature, methods, and frequency of public communication were all discussed in our interviews.

#### Communicating hazard information

*"We talked about the need for internal-external data coordination. One of the most telling aspects of this is that we are in a new world with the Web. People have much higher expectations from the government as to what information they can get and the speed that they can get it."*

The concepts of hazard and risk are very difficult to communicate to the general public. The WTC situation illustrates this vividly. The attack itself, the subsequent anthrax incidents, and the lingering effects of the Towers' collapse engendered fear and uncertainty that leaders needed to address. However, information regarding health and environmental risks was inadequate and caused considerable negative public reaction. Conflicts among the environmental and health agencies at the local and federal levels resulted in a dearth of information to the public about the possible short- and long-term health risks associated with the event. Federal policy makers directed expert staff to withhold or supply information in various formats without sufficient understanding of the science involved or of effective ways to communicate hazard information to a lay audience. As a consequence, little was communicated and public reaction turned to conspiracy theories and homegrown opinions about the health hazards. Beyond information associated with the WTC event, our interviews indicate that information to prepare the public for future emergency situations continues to be inadequate in content, specificity, and accessibility.

#### Call centers

*"The City didn't have a central hot line that was well publicized during that time. It now has a whole variety of help lines and its 311 strategy will consolidate them . . . it will be a new channel, the voice channel, the help line channel for citizens to use."*

Call centers were used by several organizations to help meet the public need for information. Through them, callers could volunteer or donate to the recovery, ask questions, receive referrals to service programs, and generally get information without going physically to a remote or congested site. A little known example of this kind of service, converted from routine to emergency operation, was the role played by the New York State Department of Taxation and Finance. The Department normally operates a busy taxpayer assistance hot line in Albany during tax season. The hot line was activated immediately after 9/11 and more than 100 operators, already experienced in dealing with the public, were quickly trained and continually re-trained to eventually handle over 180,000 calls for information and assistance. Emergency information lines were also activated in New York City by various service organizations. As with the Tax Department call center in Albany, the Red Cross created a large call center to handle triage and client assistance a long distance away from the disaster site, in Virginia. This location provided a site that could be staffed quickly in an area unaffected by the immediate aftermath of the event. Since September 11, the City of New York has established a "311" help line as part of the Mayor's efforts to improve public service and information dissemination. Such a facility can quickly be reoriented to provide timely emergency information.

#### Web sites

*"I know a lot of people were tracking progress by how much green was filtering down toward the red area and I think it was a real morale builder. On a daily basis we could change the map, shrink the red zone, put areas into operation and post this kind of map to the Web."*

The "red zone" represented the quarantined area of the City where no one was allowed to enter except public safety and emergency workers. In the weeks following September 11, shrinking the perimeter of the red zone became a daily goal at the EOC because it represented an increasing level of recovery. Regularly updated maps and citizen-oriented status information about the diminishing size of the red zone and surrounding areas were posted on NYC.gov signaling the slow return to normalcy for City residents and businesses.

In contrast to the clarity and focus of information on NYC.gov, US EPA's Web site presented an overwhelming volume of technical information about air quality presented in long tables, without context or interpretation that

would help the public understand or act on it. Other organizations posted information of varying format, content, and utility for public consumption. The array of different Web sites presented a challenge in itself. Several respondents noted that there was (and still is) no universal Web site for current disaster information in the United States or in a particular locality. Citizens could not turn to one well-known, authoritative site as a comprehensive information source. To be sure, there was a great deal of information to be found on the Web, but the almost universal ease with which information is posted to the Web makes it exceedingly difficult for users to identify the most accurate, timely, or authoritative sources.

Some interviewees discussed the limitations of the Web as a passive form of communication that "pushes" information without necessarily knowing what the public wants to "pull" in the way of crisis information. When used thoughtfully, the Web can be an excellent medium for disseminating information. However, maximizing the potential of this medium requires careful planning before a crisis. According to one federal official, agencies should have "templates for what you would put on a Web site or in fact sheets or hard copy reports . . . done well in advance. And when you have the data, you have to have some good visualization of data and data trends set up in advance." In this way, much of the energy that was diverted to questions of subject matter and format could be applied instead to data management and analysis.

### Relations with the print and broadcast media

*"[CBS] became the pool or the center point of distributing photographic and aerial data to all networks and to all broadcast and print and electronic media for the City ... during the first two weeks or so, [City officials] were focused on other issues and it was easy for us to obtain the images from them and transmit those to the people we knew to take the pressure of the press off them."*

During the WTC crisis, people turned first to television and then to the print media for news. While a great deal of independent news gathering and reporting took place, much of the information provided by TV networks, newspapers, and magazines came from government sources. The demand for news and updated information from the EOC was enormous. If left unmanaged, this demand would have interfered with the work there. At the same time, government officials recognized how important it was to have accurate, consistent information streaming to the public through all usual communication channels. Consequently, an unusual alliance among the media and the EOC allowed authoritative information about the recovery and restoration of public services to be pooled and released through a variety of outlets. CBS News acted as a press pool for mapping information, allowing the emergency operations teams on Pier 92 to concentrate on data analysis and quality without the need to constantly brief multiple media outlets. Through the CBS pool, authoritative, accurate information was regularly released to the print and broadcast media for public advisories and all outlets carried the same information each day, avoiding confusion over which source of information was most current or accurate. Participants in this arrangement who were interviewed agreed that it contributed to efficiency, accuracy, and openness, and it could be a useful model for similar situations in the future.