Government of Canada | Gouvernement du Canada

Office of Critical Infrastructure Protection and Emergency Preparedness

Bureau de la protection des infrastructures essentielles et de la protection civile

INCIDENT ANALYSIS

Number: IA02-001
Date: 27 September 2002

The September 11, 2001 Terrorist Attacks - Critical Infrastructure Protection Lessons Learned

EXECUTIVE SUMMARY

- In the year following the September 11 terrorist attacks on the World Trade Center and the Pentagon, a number of documents have been compiled that analyze the impact, response and outcomes that stem from the attacks. This report has been compiled to assist Canadian critical infrastructure (CI) owners and operators with their business continuity planning and emergency management (EM) preparations by identifying critical infrastructure protection (CIP) and EM lessons that can be learned from these tragic events. The analysis is based on open source information and feedback provided by CIP and EM partners. A selected list of lessons learned reports regarding the September 11 attacks has been included at the end of the document.

- The September 11 terrorist attacks impacted CI directly through their physical effect, and indirectly by provoking CI users, regulators and owners to take actions which further impacted CI.

- Future terrorist attacks may provoke actions from CI decision-makers that impact society, government and the economy more substantially than the terrorist incident itself.

- Communications: Predetermined emergency phone lines that are given call priority and immediate service attention during a crisis will assist emergency response. Redundant mobile communications facilities will assist EM.

- Transportation: The ability of the transportation sector to sustain normal functions will be jeopardized if sufficient planning and resources are not dedicated to meeting the challenges of an assistance operation.

- Energy: The rapid restoration of power to critical sites will be more efficient if a predetermined list identifies and prioritizes sites which are particularly vulnerable to prolonged outages.

- Banking and Finance: Comprehensive business continuity plans that include electronic and physical backup arrangements will enable most organizations to relocate and re-establish operations following a disaster.

- Government: The ability of government to coordinate its response to CI threats will be improved by the development of a government-wide alert system that incorporates high levels of security and infrastructure redundancy.

TABLE OF CONTENTS

INTRODUCTION

In the year following the September 11 terrorist attacks on the World Trade Center and the Pentagon a number of documents have been compiled that analyze the impact, response and outcomes that stem from the attacks. This report has been compiled to assist Canadian critical infrastructure (CI) owners and operators with their business continuity planning and emergency management (EM) preparations by identifying critical infrastructure protection (CIP) and EM lessons that can be learned from these tragic events. The analysis is based on open source information and feedback provided by CIP and EM partners. A selected list of lessons learned reports regarding the September 11 attacks has been included at the end of the document.

This report will identify lessons learned from the attacks that could be applied to five sectors of critical infrastructure (CI): communications, transportation[1], energy, banking and finance, and government. Following a brief description of the attacks, each sector will be examined in turn for general CIP lessons that can be drawn from specific instances relating to the terrorist attacks. The lessons have not been ranked according to importance and readers are encouraged to peruse the document in its entirety as lessons cited for one sector can often assist with CIP/EM efforts in another sector.

INCIDENT DESCRIPTION

At 08:45, a hijacked aircraft crashed into the north tower of the World Trade Center (WTC) building in NYC. At 09:03, a second hijacked aircraft crashed into the south tower. Forty minutes later, a third hijacked plane crashed into the Pentagon, in Washington, DC. A fourth hijacked plane crashed at 10:00, 80 miles southeast of Pittsburgh. Thousands of individuals were trapped, including hundreds of rescue personnel, when the south and north towers collapsed at 10:05 and 10:28 respectively. The official number of people killed in the WTC and aboard the two aircraft was 2,823. A total of 189 people were killed in the Pentagon and aboard the aircraft which struck it. The Pennsylvania crash resulted in the deaths of 44 passengers and crew.[2]

INCIDENT IMPACT

The attacks had wide-ranging impacts on local infrastructure. In NYC, the local emergency services sector was dealt a serious blow when hundreds of responders were killed under the collapsing towers of the WTC.[3] Local communication was disrupted leading several wireless carriers to donate mobile phones and pagers to emergency personnel.[4] The attacks hindered local emergency transportation and taxed the resources of local health infrastructure.

The Office of Critical Infrastructure and Emergency Preparedness (OCIPEP) has analysed the September 11 attacks and concluded that the terrorist strikes impacted CI in two ways.

[1] Lessons relating to the airline industry will not be examined in this paper.
[2] Sara Kugler, "Silent tribute marks end of search for missing at ground zero in New York," Associated Press.
[3] Multiple sources.
[4] ComputerWorld.com, 12 September 2001.

First, CI facilities and operations were directly disrupted by the physical impact of the attacks. The WTC housed, and was surrounded by, a number of key businesses that support CI. The destruction of the WTC area caused the disruption of business operations vital to several CI sectors including banking and finance, transportation, and communications. While the immediate impact of the attacks on the latter CI sectors will be elaborated in the analysis which follows, it is not known what effect the destruction of other firms in the WTC area might have had on the legal, health, business and public sector communities. It is difficult to ascertain the impact the Pentagon attack had on government continuity because of the secrecy with which this national security issue has been dealt.

Second, the decisions of CI regulators, owners and users made in response to the attacks also impacted CI. The U.S. Government was responsible, through the Federal Aviation Authority (FAA), for issuing the first ever national grounding of commercial aircraft immediately following the attacks. Owners of infrastructure such as financial markets and market participants altered the financial and banking sector by deciding to temporarily close key markets as a safety precaution. Increased demand for telephone and Internet connections forced carriers to truncate their services to avoid crashing their networks.

The analysis will now examine five CI sectors for lessons that can be learned.

COMMUNICATIONS

Landline - Emergency Communications

Verizon Communications made extraordinary efforts to turn its telecommunications network to public use during the crisis in NYC. The carrier provided nearly 2,400 spare circuits to municipal government agencies, including police and fire departments; approximately 900 to the state government; and more than 2,600 to federal agencies and the military.[5] Verizon restored service to essential operations such as hospitals, doctors' offices and healthcare centres by formulating a priority list for their technicians to follow.[6] Verizon also reconfigured its 4,000 Manhattan payphones to provide free calls to anywhere in NYC and set them to accept incoming calls, something they ordinarily cannot do. In addition, Verizon Wireless made a half-million wireless handsets available.[7]

LESSON:

1. Predetermined emergency phone lines that are given call priority and immediate service attention during a crisis will assist emergency response. The conclusion of communications agreements between CI owners, local emergency services and federal emergency management agencies will help to guarantee that these dedicated lines exist.

[5] Lisa Guernsey, "An Unimaginable Emergency Put Communications to the Test," NYTimes.com.

[6] Eugene Grygo and Jennifer Jones, "U.S. recovery: Cost of rebuilding N.Y. IT infrastructures estimated at $3.2 billion," IDG.net

[7] Paul Coe Clark III, "Verizon Fights to Reconnect New York," The Net Economy.

Landline - Emergency Management

The Federal Emergency Management Agency (FEMA) was unable to set up a fully functional field office in NYC to coordinate recovery efforts because it lacked a telecommunications infrastructure. FEMA worked around the situation using mobile wireless technology and satellites, but a fully functioning joint operations centre with the city and the state was not up and running before September 26. NYC and state officials spearheaded most of the initial relief efforts.[8]

LESSON:

2. Lead emergency response agencies require appropriate telecommunications infrastructure in order to assist recovery coordination with first responders.

Landline - Telecommunications Priorities

During emergencies, local phone lines can quickly become congested by inbound calls seeking reassurance and information. On September 11, the Verizon telecommunications network in NYC became extremely congested. While many individuals outside NYC had difficulty reaching phone numbers in the city and assumed that the network had crashed, Verizon officials asserted that inbound calls to NYC were blocked by design rather than network failure. These blocking procedures kept the network from crashing and allowed it to carry a record number of calls.[9]

LESSON:

3. Communications CI will be protected, and emergency response efforts will be facilitated, by preventing disaster-affected networks from crashing. The allocation of sufficient network space to local emergency services will assist relief efforts. Attempting to accommodate all inbound communication will endanger network stability and bandwidth for the emergency response.

Landline - VOIP Technology

A Voice-over-IP (VOIP) owned by ITXC is located directly across the Hudson River from Manhattan. It has enormous user capacity and is leased to long-distance companies, which regularly re-route calls over the public Internet to reach overseas destinations or to level domestic spikes in call volume. Since Verizon Communications, like most regional telecommunications companies, has no interface with a VOIP provider, the VOIP capacity was not available to relieve the volume of usage on local exchanges.[10] The variable quality of service on many VOIP networks would not detract from their usefulness during a time of crisis. Corporations can achieve voice redundancy within their network by using dedicated IP circuits to build VOIP capability in routers or frame relay devices.

LESSON:

4. Telephone carriers will be better positioned to relieve network congestion during emergencies by drafting contingency plans that take into account the redundant capacity of local VOIP networks. Corporations using VOIP can achieve voice redundancy within their network when voice traffic has saturated other modes of communication.

[8] Matthew Weinstock, “FEMA unable to set up New York City field office,” GovExec.com
[9] Dana Coffield, “Phone Nets On Call,” Interactive Week.com.
[10] Rob Fixmer, “Burried Illusions,” Interactive Week.com.

Wireless – Emergency Communication

Police and fire wireless communications relied on a radio "repeater" located on top of the WTC. The destruction of this device resulted in the elimination of wireless communications and forced emergency communication to temporarily rely on the phone system. Communications was further complicated because the main and backup phone systems at the police headquarters were on the same grid, which had been damaged by falling debris from the WTC. The U.S. National Communications System has since proposed that in emergencies priority to the wireless networks used by cellular telephones should be given to police, fire and EM personnel.[11]

LESSON:

5. Emergency services that install redundant computer, electrical and communications systems on different grids from their main systems will help to secure the functionality of CI in the event of a disaster.

Wireless – Transportable Mobile Phone Infrastructure

Many wireless operators in NYC used transportable mobile phone infrastructure to allow calls to continue despite damage to their facilities near the WTC. Verizon and AT&T Wireless moved mobile phone antennas in New Jersey and Brooklyn toward lower Manhattan to improve wireless reception. In Washington, DC, Verizon and Cingular Wireless transported mobile phone infrastructure into the vicinity of the Pentagon and nearby Shenendoah National Park to ensure that rescue workers could rely on the network.

LESSON:

6. Following a significant disruption of wireless communications service, transportable mobile phone infrastructure will facilitate the coordination of an emergency response.

Wireless – Alternative Modes of Communication

The loss of landline and wireless sites in or around the WTC, coupled with selective call-blocking throughout the Northeast U.S., left many institutions and emergency responders seeking alternative ways to coordinate their recovery efforts. Some wireless users with data-capable phones found that they could send and receive Short Message Service (SMS) text, despite being unable to make voice calls. Other modes of communication such as BlackBerry wireless e-mail devices, wireless-enabled Personal Digital Assistants, two-way radios, satellite phones and pagers worked well and were of use for those who had them. Institutions in possession of pre-determined contact lists for these various modes of communication were able to rapidly communicate with concerned stakeholders. An Enhanced 911 (E911) system, which provides the precise location of 911 calls from wireless phones, could have enabled some victims to have been located more quickly.

LESSON:

7. Following a disaster, alternative modes of communications will assist with recovery and crisis management while freeing network space for the voice communications of emergency responders.

[11] Mike Fish, "Attacks in New York provide sobering lessons," CNN.com.

Internet/Information Technology – Internet Redundancy Planning

Many companies affected by the attacks had more than one line from their offices to high-speed Internet access points. In some cases, both regular and the redundant lines travelled through the same conduits to the same routing centres. When those conduits or routing centres were damaged, all cables, including those dedicated to emergency redundancy, were affected. The cost of rebuilding IT infrastructure on Wall Street was expected to be approximately US$3.2 billion, with the full restoration to take place over a period of 12 to 24 months. [12]

LESSON:

8. Institutions that insist on the need for geographic and technological redundancy from their networks and/or service providers will be better placed to implement contingency plans following a disaster.

Internet/Information Technology – Criticality of Financial Sector

The deputy manager of the U.S. National Communications System (NCS) stated that the destruction of 1.5 million circuits in the financial district was a threat to U.S. economic stability and constituted the most significant challenge that the NCS had ever encountered.[13] The White House ordered the NCS to make Wall Street connectivity the next priority after rescue efforts had been given the support they required. Federal and industry engineers worked together to restore the digital backbone as quickly as possible. In spite of this effort, diesel generators succumbed to fuel and maintenance problems, causing backup power to fade and restoration efforts to be delayed.

LESSON:

9. The restoration of financial sector digital connectivity will be a priority following large urban disasters but repair may be hindered by interdependencies from outside of the telecommunications sector.

Internet/Information Technology – Y2K Contingency Planning

Investment in Y2K preparations helped to expedite recovery of IT systems impacted by the attacks. The Y2K problem had focused management on the enumeration of infrastructure components, the prioritization of critical applications and the identification of interdependencies between systems and organizations. In addition, system configurations were standardized to assist with rapid recovery. These elements of Y2K planning allowed organizations to rapidly determine where recovery efforts should be focused and how to implement work-around solutions.

LESSON:

10. Maintenance of up-to-date, Y2K-based inventories, procedures and standards will greatly assist with IT disaster-recovery efforts and business continuity.

[12] Eugene Grygo and Jennifer Jones, "U.S. recovery: Cost of rebuilding N.Y. IT infrastructures estimated at $3.2 billion," IDG.net

[13] Dan Verton, "Digital Destruction Was Worst Imaginable," ComputerWorld.com.

Internet/Information Technology – Distributed Systems Backup

Y2K planning primarily focussed on the recovery of mainframe systems and data centres. The majority of the damage caused by the attacks, however, was sustained by distributed systems such as end-user data and applications. Recovery of these systems was further complicated when servers and backup tapes were situated in the same location as the disaster. Loss of these distributed systems, especially e-mail, impeded the communication and coordination that was necessary to sustain business continuity following the disaster.

LESSON:

11. Frequently testing distributed backup systems and increasing their prominence in business continuity planning will help to ensure that the restoration of critical business resumption applications requires less time and effort following a disaster.

Internet/Information Technology - Internet Messaging

Internet messaging (IM) platforms pose both opportunities and liabilities during a crisis. On September 11, one of the unintended benefits of IM tools was the "presence" notification they provided. When IM users went online after the event, their names were highlighted on the IM address lists of their friends.[14] This presence helped to account for missing persons and may have diverted communication from jammed telecommunications systems to more robust Internet networks. IM platforms, however, can also increase the vulnerability of firms to opportunistic computer hackers. Several computer security firms advised their clients to shut down all non-critical connections to the Internet, including IM platforms, which could provide intruders a back door to critical systems.

LESSON:

12. During periods of increased threat, shutting down vulnerable Internet Messaging platforms will help to protect network infrastructure.

Internet/Information Technology - Emergency Information Management

Emergency services increasingly employ information technology to better coordinate their relief efforts. It took nine days, however, for NYC to establish a computerized clearinghouse to help families locate loved ones or to file missing persons reports. Many telephone lines were either destroyed or disrupted, leaving concerned individuals with little choice but to walk between rescue stations, city offices and hospitals in search of information. Following the attacks, a U.S. Senator suggested that the nation form a cyber-National Guard to furnish necessary information systems in the event of a disaster and to quickly repair damage to the nation’s CI.[15]

LESSON:

13. During a crisis, a standing, rapidly deployable emergency information management capacity will be of great assistance to first responders and victims. It will also help mitigate the strain on government and health infrastructure following a disaster.

[14] Randy Barrett, “Safety Net,” Interactive Week.com

[15] Lisa Hoffman, “Lawmaker proposes creation of cyber-National Guard,” Scripps Howard News Service.

TRANSPORTATION

Emergency Partnerships

The U.S. response to the attacks impacted the Canadian transportation system in several ways: vehicle and train border crossings were temporarily suspended, air traffic was redirected from the U.S. to Canada, increased security measures were stipulated by the FAA for Canadian airports, and tightened controls at re-opened border controls slowed the flow of traffic. Transport Canada (TC) worked to mitigate the impact of these developments on the Canadian transportation system by coordinating all branches of the Department (particularly Security and Emergency Preparedness, and Civil Aviation) and by working with NAV CANADA, Royal Canadian Mounted Police, Department of National Defence and many other key agencies, provincial governments and airports. These efforts helped TC to manage the diversion of 224 U.S. bound planes to Canadian airports, the care and security of passengers, the increased demand for non-air travel, the subsequent re-opening of airspace, and other related issues. As events unfolded, however, links to some external organizations and international partners had to be improvised since pre-existing relationships were non-existent or out of date.

LESSON:

14. Well-maintained partnerships and established common emergency protocols will provide a foundation for proactive measures during an urgent situation and creative responses during a crisis.

Emergency Assistance

Following the closure of airspace in the U.S., the Canadian Government gave permission for the FAA to redirect U.S. bound flights to the nearest airport in Canada. In total, 224 re-routed aircraft landed in Canada. Many of the airliners were directed to small or remote airports such as Gander, Newfoundland, which had limited human and material resources. Several of these airports could not meet the fuelling and maintenance needs of the diverted aircraft. Additional resources and personnel had to be deployed to assist with airport operations and the security screening of passengers and baggage. In spite of these efforts, the subsequent departure of re-routed aircraft was delayed even after the ban on general aviation to the U.S. had been lifted. The critical functions of Canada’s transportation infrastructure were not compromised by the challenges of the assistance operation. Supplementary planning and resources, however, were not sufficient to prevent overtaxing of the transportation infrastructure in certain localities.

Lesson:

15. The ability of the transport sector to sustain normal functions will be jeopardized if sufficient planning and resources are not dedicated to meeting the challenges of an assistance operation.

Alternative Modes of Transportation

The interruption of air transportation directly and immediately impacted all aspects of public and private activities that normally relied on this mode of transportation. The transportation of critical employees and time-sensitive materials, such as materials for data centres, was impacted. The inability of critical employees to travel by air hindered recovery operations and prompted widespread use of alternative means of transportation. Securities settlement and clearing in the U.S. markets were adversely affected because trades could not be matched within the time required. Land-based couriers were relied upon as alternative means of shipping. In Canada, materials within provinces were delayed for up to a day, resulting in a significant increase in financial holdovers for banks. Items travelling to adjacent provinces were delayed for up to five days, and items travelling across Canada were delayed for up to seven days. Stricter customs examinations delayed trans-national shipments to the U.S.

LESSON:

16. The interruption of air transportation will result in mass usage and delays of alternative modes of transportation and will hinder operations involving critical employees or time-sensitive materials.

ENERGY

Emergency Power Production in NYC

Emergency power production and recovery efforts were threatened by diesel generator vulnerabilities. Most critical network hubs in lower Manhattan switched over to diesel generators during the power outage from September 11 to 19 inclusive. The ban on the delivery of diesel fuel in NYC threatened to further deteriorate Internet access and some telephone communications until it was lifted. In addition to these concerns, maintenance issues assumed critical importance after a week of emergency power generation. Backup diesel generators were particularly susceptible to malfunction because of dust and soot in the air.[16]

LESSON:

17. Operators of network exchanges will benefit from a sustainable energy contingency plan that addresses the potential of a medium- to long-term power disruption. Communications and business continuity will further deteriorate after the initial impact of a disaster if backup power generation facilities are not provided with guaranteed access to fuel and maintenance.

Restoration of Power to NYC

Power companies must negotiate between a number of different interests and priorities when restoring power after a blackout. The disruption of electrical power to lower Manhattan posed a question about how remaining and restored power should be allocated. Consolidated Edison Inc. (ConEd), the primary supplier of electricity in NYC, restored power to streetlights and small businesses first. Larger businesses were then connected to the electric grid, as it could handle the loads.[17] ConEd completed the restoration of power on September 19 to all areas affected by the WTC attacks, although customers were requested to limit their energy consumption.

LESSON:

18. The rapid restoration of power to critical sites will be more efficient if a predetermined list identifies and prioritizes sites which are particularly vulnerable to prolonged outages. This list will help contend with the wide range of interests expressed by business, government and public facilities during an urban emergency.

[16] Max Smetannikov, “Diesel Shortage Could Cripple Net Access,” Interactive Week.com

[17] FEMA, “Congressional and Intergovernmental Advisory #20: State of New York,” Federal Emergency Management Agency.

Airborne Monitoring of Infrastructure

Following the attacks, both the U.S. and Canada closed their airspace to all flights except military and humanitarian operations. Concurrent to this action, CI owners were advised to take appropriate measures to ensure the security of their assets. Oil and gas industry preparedness measures often include airborne patrols of critical pipelines and facilities.[18] The ban on air traffic during this period of heightened alert made such patrols impossible, impairing industry security and government relationships with the private sector.

LESSON:

19. During a ban on general aviation traffic, provisions that allow members of the private sector to conduct airborne monitoring of distant CI will further CIP objectives.

BANKING AND FINANCE

Corporate and Geographic Concentrations

The operational impact of September 11 was intensified by the fact that the financial sector is concentrated both geographically and corporately. The September 11 incidents severely impacted the financial sector because of the high geographic concentration of financial institutions in the NYC area. The impact of the terrorist incidents was also magnified because of the high degree of market concentration in certain key parts of the sector. For example, the sector relies on a small number of institutions to carry out the settlement of funds, securities and financial contracts. The disruption of these entities following September 11 hindered the operations of third parties through interdependent relationships.

LESSON:

20. Financial institutions that recognize the effects of concentration and interdependence of the sector will be better placed to manage the operational implications of disasters in other parts of their sector.

Business Continuity Planning

As a result of the 1993 bombing of the WTC, many companies in the Center established business continuity plans that included evacuation plans and backup arrangements for electronic and physical assets. With a few exceptions, these organizations were able to safely and quickly relocate and re-establish their operations after the September 11 attacks. No significant cyber losses were reported in the media. Prearranged response activities with local food services, hotels, law enforcement agencies, fuel providers and utilities, as well as extensive contact information for public and private organizations, helped expedite business resumption. In spite of this preparedness, the total cost of the WTC attacks has been estimated at US$40 billion.[19]

The preparedness of businesses in the WTC area is not mirrored in the rest of the U.S. One data backup service estimated that 82 percent of U.S. companies did not have adequate disaster recovery plans in place. On the physical side, one business recovery

[18] "Crisis Management Center – DOT Status and Overview #33," U.S. Department of Transporation.
[19] Deepti Hajela, "Cost of New York attacks almost $40 billion, officials say," AP Online.

service noted that only 7 of its 3,000 U.S. clients had contracted for standby offices.[20] A Gartner report cites insufficient testing as the most frequent shortfall of business continuity plans around the world.[21]

LESSON:

21. Comprehensive business continuity plans that include evacuation and backup arrangements for electronic and physical assets will enable most organizations to relocate and re-establish operations following a disaster.

Critical Staffing Shortages

In spite of the extensive business continuity planning that had been invested in Y2K, many institutions did not account for disasters involving significant shortages of critical staff. Most disaster-recovery plans were premised on the assumption that key personnel could be relocated or drawn upon to assist with recovery. September 11 graphically illustrated that such an assumption cannot be relied upon. The challenge of accounting for all personnel was formidable, especially in the case of contract employees, and in instances when evacuation plans did not include predetermined assembly points away from the site. Casualties and psychological trauma further impacted the ability of local corporate personnel to resume business operations. In addition, federally-imposed flight restrictions hampered out-of-area employees from assisting with recovery plans.

LESSON:

22. The business continuity planning of financial institutions will be improved by accounting for disaster scenarios that involve consequences that could harm or render inaccessible critical employees.

Crisis Managing Employees

Nasdaq resumed trading six days after the attacks and credits both technical and personal management solutions with the rapid recovery. Nasdaq established a 24/7 “crisis line” teleconference call to establish its core internal decision-making communications and to establish the ranking of executives for decision-making and escalation. Site-specific hotlines were regularly updated to inform employees about site closures, redirections, and status. Separate daily conference calls enabled staff to coordinate recovery efforts with Nasdaq, industry and technical stakeholders. Phone-out groups were established to help push information to relevant constituencies, including the families of employees. The basic needs of employees were addressed by providing food, water, heat, shelter and psychological counselling.

LESSON:

23. Institutions that address the information, communication and personal needs of employees during a crisis will further the efficiency of their business resumption plans.

[20] Max Smetannikov, “Safeguarding Data,” Interactive Week.com
[21] Chuck Tucker and Richard Hunter, “September 11: Business Continuity Lessons,” Gartner, May 2002.

Business Resumption Plans and Hotsite Models

Several firms in lower Manhattan had not created business resumption plans or hotsite models that could contend with a large-scale disaster affecting several critical sites within the same area, city or region. The destruction of the WTC destroyed 30,000 securities positions (trading, sales, research and operations) in the building and damaged 15,000 to 20,000 positions in adjacent structures.[22] Some firms had located their private hotsite facilities in neighbouring buildings for convenience and efficiency, but were unable to use them following the attacks because the facilities had been destroyed, damaged or cordoned off for security purposes. Still other firms found themselves unable to access their commercially-contracted hotsites because the demand in the NYC area following the attacks exceeded supply and space was allocated on a first-come, first-served basis. Some disaster-recovery firms offered hotsites that were not readily accessible due to air transportation restrictions. Some firms are now integrating in-house, hotsite capabilities into geographically separate, primary operational sites that can absorb some or all of the work of another primary site in event of a disaster.

LESSON:

24. Business resumption plans and hotsite models that take into consideration disasters involving broad geographic areas (such as a district, city or region) will be better equipped to cope with the impact of such disasters on business recovery efforts.

Crisis Management Communications

Frequent communications with stakeholders is essential to managing a crisis situation. Securities and settlement institutions reported that information-sharing regarding the status of operations, problems and work-around plans was integral to allow their customers to manage their operations. It was difficult for institutions, however, to establish communications with the right people in the right places when they were unfamiliar with their partners' recovery plans or contact details at backup locations.

LESSON:

25. CIP & EM stakeholders that share recovery plans and contact information with one another will be better able to establish crisis management communication in the event of a disaster.

Critical Infrastructure Interdependencies

The banking sector drew attention to the way in which CI interdependencies posed challenges to their recovery efforts. The disruption of communications carrier services was cited as a significant problem, and telecommunications suppliers are being encouraged to establish diverse routing, but not through the same geographical area. Some suppliers of other products and services did not have adequate business continuity plans and this impacted the ability of some institutions to fully implement their proprietary plans. The banking sector is encouraging a dialogue between CI sectors to be able to establish priorities needed to recover from future disasters.

LESSON:

26. Advanced planning and communication between CI sectors will help to minimize the impact of interdependencies on business continuity plans.

[22] Eugene Grygo and Jennifer Jones, "U.S. recovery: Cost of rebuilding N.Y. IT infrastructures estimated at $3.2 billion," IDG.net

GOVERNMENT

Evacuation Procedures

Most government offices have a standard alerting system and evacuation procedure to cope with bombs threats, fires, etc. No system existed in the U.S., however, to issue a government-wide alert on September 11. As military officials at NORAD ordered fighter jets from Langley Air Force Base to intercept one of the hijacked aircraft, neither the FAA, NORAD, nor any other federal government organization issued evacuation orders to the buildings presumed targeted in Washington, DC. Officials at the Pentagon said that no mechanism existed within the U.S. Government to notify various departments and agencies under such circumstances.[23]

LESSON:

27. The ability of government to coordinate its response to CI threats will be improved by the development of a government-wide alert system that incorporates high levels of security and infrastructure redundancy.

Standardization and Interoperability of Emergency Equipment

The annual meeting of the International Association of Emergency Managers (IAEM) expressed concern following September 11 about the lack of uniform standards for EM equipment.[24] No standards had been set, for example, as to which types of gas masks or suits would protect responders against specific chemical or biological agents that could have been at the scene. The interoperable equipment between jurisdictions also impacted the effectiveness of first responders. NYC fire fighters found that they were unable to exchange their depleted oxygen tanks for those offered by the New Jersey fire department because the breathing apparatus attachment nozzles were of different sizes.

LESSON:

28. The standardization of emergency equipment will help to safeguard first responders. Interoperable equipment will further the efficiency of emergency operations.

Internet Communications

In times of crisis, citizens look to the government as a trusted source of information, assurance and advice. The government, in turn, can use the Internet as an effective way to communicate with its citizens. In the hours following the attacks, however, FirstGov (www.firstgov.gov), the U.S. federal government's only official portal, remained a list of links to other federal sites and did not mention the crisis.[25] FirstGov users had to navigate through the portal before finding the web site for the Federal Emergency Management Agency, which was posting relevant information about the tragedy. In contrast, the NYC.GOV web site proved to be an enormously important and efficient means of communicating with the general public. A record number of individuals used the Internet to find information during the crisis.

LESSON:

29. Web portals that consolidate clear and timely emergency response information will assist governments to convey important information to citizens during times of crisis.

[23] "Officials: Government failed to react to FAA warnings," CNN.com
[24] Mike Fish, "Cities ponder where terrorists may strike," CNN.com.
[25] Doug Brown, "Government Overlooks Web's Potential," Interactive Week.com.

Public Communications

The Canadian public was rapidly and significantly affected by the events of September 11. The close relationship between the U.S. and Canada led many Canadians to experience feelings of apprehension and sympathy in the aftermath of the attacks. Many citizens looked to the federal government and media for information about the tragedy, its implications for Canada and the potential for more attacks. Citizens also expressed a strong desire for information pertaining to public safety, personal preparedness and means to assist with recovery efforts in the U.S. Media sources that were not given access to substantial or regular briefings frequently produced reports that criticized the government and alarmed the public with speculation.

LESSON:

30. In times of crisis, clear and rapid emergency communications will assist in dealing with the situation.

Evidence Collection in Urban Disasters

The simultaneous efforts of law enforcement and disaster management professionals are often required when terrorist incidents take place in an urban setting. The need to quickly search for survivors or clear debris may not always compliment the need to methodically collect evidence. In the case of the WTC attacks, the affected 16-acre area constituted the largest crime scene in history. The estimated 1.75 million tons of rubble that needed to be cleared from the centre of NYC made the collection of evidence more complicated. The problem was resolved by taking rubble by dump truck to Staten Island, where it was spread out in a field. Teams of FBI agents and NYC detectives sorted through the debris by hand to locate anything that might add to the file of criminal evidence.

LESSON:

31. When a criminal investigation is conducted alongside a major urban disaster, it will be important for rescue services and law enforcement to reach early agreement on how to manage the rescue of survivors and restoration of normal city functioning while preserving evidence for criminal investigations.

SUMMARY OF LESSONS LEARNED

COMMUNICATIONS

1. Predetermined emergency phone lines that are given call priority and immediate service attention during a crisis will assist emergency response. The conclusion of communications agreements between CI owners, local emergency services and federal emergency management agencies will help to guarantee that these dedicated lines exist.

2. Lead emergency response agencies require appropriate telecommunications infrastructure in order to assist recovery coordination with first responders.

3. Communications CI will be protected, and emergency response efforts will be facilitated, by preventing disaster-affected networks from crashing. The allocation of sufficient network space to local emergency services will assist relief efforts. Attempting to accommodate all inbound communication will endanger network stability and bandwidth for the emergency response.

4. Telephone carriers will be better positioned to relieve network congestion during emergencies by drafting contingency plans that take into account the redundant capacity of local VOIP networks. Corporations using VOIP can achieve voice redundancy within their network when voice traffic has saturated other modes of communication.

5. Emergency services that install redundant computer, electrical and communications systems on different grids from their main systems will help to secure the functionality of CI in the event of a disaster.

6. Following a significant disruption of wireless communications service, transportable mobile phone infrastructure will facilitate the coordination of an emergency response.

7. Following a disaster, alternative modes of communications will assist with recovery and crisis management while freeing network space for the voice communications of emergency responders.

8. Institutions that insist on the need for geographic and technological redundancy from their networks and/or service providers will be better placed to implement contingency plans following a disaster.

9. The restoration of financial sector digital connectivity will be a priority following large urban disasters but repair may be hindered by interdependencies from outside of the telecommunications sector.

10. Maintenance of up-to-date, Y2K-based inventories, procedures and standards will greatly assist with IT disaster-recovery efforts and business continuity.

11. Frequently testing distributed backup systems and increasing their prominence in business continuity planning will help to ensure that the restoration of critical business resumption applications requires less time and effort following a disaster.

12. During periods of increased threat, shutting down vulnerable Internet Messaging platforms will help to protect network infrastructure.

13. During a crisis, a standing, rapidly deployable emergency information management capacity will be of great assistance to first responders and victims. It will also help mitigate the strain on government and health infrastructure following a disaster.

TRANSPORTATION

14. Well-maintained partnerships and established common emergency protocols will provide a foundation for proactive measures during an urgent situation and creative responses during a crisis.

15. The ability of the transport sector to sustain normal functions will be jeopardized if sufficient planning and resources are not dedicated to meeting the challenges of an assistance operation.

16. The interruption of air transportation will result in mass usage and delays of alternative modes of transportation and will hinder operations involving critical employees or time-sensitive materials.

ENERGY

17. Operators of network exchanges will benefit from a sustainable energy contingency plan that addresses the potential of a medium- to long-term power disruption. Communications and business continuity will further deteriorate after the initial impact of a disaster if backup power generation facilities are not provided with guaranteed access to fuel and maintenance.

18. The rapid restoration of power to critical sites will be more efficient if a predetermined list identifies and prioritizes sites which are particularly vulnerable to prolonged outages. This list will help contend with the wide range of interests expressed by business, government, and public facilities during an urban emergency.

19. During a ban on general aviation traffic, provisions that allow members of the private sector to conduct airborne monitoring of distant CI will further CIP objectives.

BANKING AND FINANCE

20. Financial institutions that recognize the effects of concentration and interdependence in the sector will be better placed to manage the operational implications of disasters in other parts of their sector.

21. Comprehensive business continuity plans that include evacuation, electronic and physical backup arrangements will enable most organizations to relocate and re-establish operations following a disaster.

22. The business continuity planning of financial institutions will be improved by accounting for disaster scenarios that involve consequences that could harm or render inaccessible critical employees.

23. Institutions that address the information, communication and personal needs of employees during a crisis will further the efficiency of their business resumption plans.

24. Business resumption plans and hotsite models that take into consideration disasters involving broad geographic areas (such as a district, city or region) will be better equipped to cope with the impact of such disasters on business recovery efforts.

25. CIP & EM stakeholders that share recovery plans and contact information with one another will be better able to establish crisis management communication in the event of a disaster.

26. Advanced planning and communication between CI sectors will help to minimize the impact of interdependencies on business continuity plans.

<u>GOVERNMENT</u>

27. The ability of government to coordinate its response to CI threats will be improved by the development of a government-wide alert system that incorporates high levels of security and infrastructure redundancy.

28. The standardization of emergency equipment will help to safeguard first responders. Interoperable equipment will further the efficiency of emergency operations.

29. Web portals that consolidate clear and timely emergency response information will assist governments to convey important information to citizens during times of crisis.

30. In times of crisis, clear and rapid emergency communications will assist in dealing with the situation.

31. When a criminal investigation is conducted alongside a major urban disaster, it will be important for rescue services and law enforcement to reach early

agreement on how to manage the rescue of survivors and restoration of normal city functioning while preserving evidence for criminal investigations.

SELECTED LESSONS LEARNED REPORTS REGARDING THE SEPTEMBER 11 ATTACKS

Bailar, Gregor. "Nasdaq Lessons Learned from Sept. 11." *CIO.com*. 24 October 2001.

Computer Sciences Corporation. *Staying in Business: Recovery Lessons From September 11*. 25 October 2001.

Deloitte & Touche. *September 11: Continuity Lessons Learned Panel*. 7 November 2001.

Disaster Recovery Information Exchange. "Special Edition." *DRIE Digest*. November 2001.

Disaster Recovery Journal. *Disaster Recovery Issues in this Time of Crisis*. 20 November 2001.

Federal Emergency Management Agency. *World Trade Center Building Performance Study*. May 2002.

Gartner. *After the Fall: Lessons from Sept. 11*. 18 March 2002.

Gartner. *September 11: Business Continuity Lessons*. May 2002.

Institute for Security Technology Studies. *The First Line of Defense: Tools and Technology Needs of America's First Responders in the Aftermath of September 11, 2001*. 28 May 2002.

Jackson, Carl. "CSI Checklist: How the Sept. 11 Attack Should Impact Your Continuity Planning." *Computer Security Journal*. Vol.XVIII, No.1. 2002.

Junnakar, Sandeep. "Lessons: Keeping Networks Alive in New York," *CNET News.com*. 28 August 2002.

McKinsey & Company. *Increasing FDNY's Preparedness*. 2002.

Michaels, Sarah. "Digital Disaster Assistance: How and Why Selected Information Technology Firms Contributed to Recovery Immediately After the September 11, 2001, Terrorist Attacks," University of Chicago Natural Hazards Research and Applications Information Center. 2001.

Orfinger, Becky. "Lessons Learned from the World Trade Center Attack," *DisasterRelief.org*. 16 November 2001.

Port Authority of NY & NJ. *When Bad Things Happen to Good People: Lessons Learned from the WTC Attack*. Presentation by Michael Frank to the Society for Information Management, NJ Chapter Meeting. 11 April 2002.

Public Safety Wireless Network Program. *Answering the Call: Communications Lessons Learned from the Pentagon Attack*. January 2002.

Public Safety Wireless Network Program. *LI NYC Emergency Management Conference—Lessons Learned From The World Trade Center Attack*. June 2002.

RAND. *Protecting Emergency Responders - Lessons Learned from Terrorist Attacks*. 2002.

Rubin, Claire B. and Irmak Renda-Tanali. "The Terrorist Attacks on September 11, 2001: Immediate Impacts and Their Ramifications for Federal Emergency Management," *University of Chicago Natural Hazards Research and Applications Information Center*. 2001.

Security Industries Association. "Lessons Learned - A Collection of Observations and Experiences From Those Involved in Ensuring Business Continuity." *SIA Report*. 1 May 2002.

Security Industries Association. "Restoring Industry Functionality after 9/11: Lessons in Disaster Recovering and the Value of Contingency Planning." *Research Report*. Vol.II, No.9. 2 November 2001.

The Federal Reserve Board. *A Supervisory Perspective on Disaster Recovery and Business Continuity*. Remarks by Vice Chairman Roger W. Ferguson, Jr. before the Institute of International Bankers, Washington, D.C. 4 March 2002.

The Gilmour Commission. *Third Annual Report to the President and the Congress of the Advisory Panel to Assess Domestic Response*. 15 December 2001.

The Institute of Internal Auditors. *DRP Lessons Learned After September 11, 2001*. 15 November 2001.

THE YANKEE GROUP. *September 11, 2001: Infrastructure Impacts, Implications, and Recommendations*. September 2001.

Thomas, Deborah S. K., Susan L. Cutter, Michael Hodgson, Mike Gutekunst and Steven Jones. "Use of Spatial Data and Geographic Technologies in Response to the September 11 Terrorist Attack," *University of Chicago Natural Hazards Research and Applications Information Center*. 2002.

U.S. Securities and Exchange Commission. *Summary of "Lessons Learned" from Events of September 11 and Implications for Business Continuity*. 13 February 2002.

Weber, Richard T., David A. McEntire and Robie J. Robinson. "Public/Private Collaboration in Disaster: Implications from the World Trade Center Terrorist Attacks," *University of Chicago Natural Hazards Research and Applications Information Center*. 2002.

Wheatley, Malcolm. "Living with Terror." *CIO Magazine*. 15 February 2002.