



After the Disaster: Business Continuity

Heather R. Schimmelpfennig

Student

Columbia Southern University

Abstract

This paper discusses the updates and changes to standards that are intended to minimize business interruptions as the result of natural disasters, terrorism, and any other crisis that can affect both the private and public sectors. Specific standards are mentioned and discussed in the context of recent disasters that have occurred in the United States. Weaknesses of continuity plans are discussed, and examples of business interruptions and the effects on both the private and public sectors are included.

Introduction

The biggest hurricane of the 2012 season was Sandy. She barreled her way onto the shores of the East Coast leaving devastation and testing the existing emergency management systems put in place after 2005's Hurricane Katrina, which claimed 1,833 lives. Hurricane Sandy left 285 dead over the course of several days. What began as a declared tropical depression on October 22, 2012, ended as a category one hurricane that hit the Mid-Atlantic region seven days later. This disaster is just one of many recorded in U.S. history, and Sandy's story truly begins where Hurricane Katrina left off.

This paper briefly discusses the correlation of what is done after disasters like Hurricane Katrina and what emergency management systems are used based on the standards, their effectiveness, and how experience affected the response to Hurricane Sandy. Particularly addressed is the topic of business continuity and how adoption of certain standards was considered in light of prior disasters such as Hurricane Katrina and 9/11. The best time to plan for disaster recovery is before the disaster can occur again. "Disaster recovery is the process that takes place during and after an organizational crisis in order to minimize business interruption and to return the organization to a pre-disaster state as soon as possible" (Fuller & Vassie, 2004).

After Katrina

After Hurricane Katrina left its mark on the Gulf Coast, there was a recognized need to make updates to the current codes and standards in relation to response management and business continuity. “Widely held views of a bungled government response to the tragedy forced the U.S. federal government to take a close look at what went wrong” (Zellen, 2007). One change that came about as a result of Katrina was the publication of the revised NFPA 1600-2007, *Standard on Disaster/Emergency Management and Business Continuity Programs*, which was approved as an American National Standard (ANS) on December 20, 2006. In addition to guidelines for risk mitigation and prevention when disasters occur, the 2007 edition of the standard added a section on “incident prevention” intended to assist the organization – whether private or public – in developing a strategy to prevent an incident that threatens people, property, and the environment. The areas covered by NFPA 1600-2007 range from risk assessment and mitigation to disaster planning and incident management to communication, training, and corrective action implementation.

On June 21, 2010, the Federal Emergency Management Agency (FEMA) of the Department of Homeland Security (DHS) adopted NFPA 1600-2007, along with two other standards, ANSI/ASIS SPC.1-2009, *Organizational Resilience*, and BS 25999, *Business Continuity Management*. These adoptions resulted from a 9/11 Commission recommendation program, and were “intended to improve preparedness for disasters and emergencies in the private sector” (“DHS Adopts Standards for Private Sector Emergency Preparedness Program,” 2010). ANSI/ASIS SPC.1-2009, an American National Standard from the American Society for Industrial Security (ASIS), outlines a management framework to help businesses anticipate disruptive incidents and prepare and prevent the disasters from affecting their ability to recover quickly and continue with minimal interruption. Developed by the British Standards Institution (BSI), BS 25999 helps organizations maintain business continuity by implementing codes of practice to implement and develop disaster response plans and then develop specifications for monitoring, reviewing, and improving their management system.

The American National Standards Institute (ANSI) Homeland Defense and Security Standardization Collaborative (HDSSC) identifies standards needed to assist federal agencies in addressing homeland security and homeland defense priorities. The HDSSC seeks to aid in the building of cooperative partnerships to protect commerce by standardizing the requirements to protect the nation’s infrastructure when disaster strikes. It works with the DHS, the Department of Defense (DOD), and the National Institute for Occupational Safety and Health (NIOSH), and will collaborate with other agencies and organizations to identify standards needs.

Failures and Weaknesses

In spite of committee meetings and changes made to standards and their resulting adoption and national implementation strategies, Hurricane Sandy outwitted the experts in a number of ways. New Jersey residents were without electrical power for up to two weeks, and gas stations were unable to dispense gasoline due to the lack of energy to operate the pumps. Residents and businesses alike were

not equipped to react to the damages the storm inflicted. This disaster proves that we still have a lot to learn about continuity.

One gap in some current standards is the need for back-up generator requirements for coastal communities to address energy outages. “States prone to coastal or tropical storms should revisit back-up generator requirements for service stations (in a way that doesn’t put them out of business), and stations should be allowed alternatives for fuel deliveries (without waiting for a governor’s decision) should a refinery go offline” (Warren, 2013).

Another issue that affected business continuity after Hurricane Sandy was in the cable sector. Cable is not only used for residential entertainment, but also is the basis for most communication in the home and in the business sector. Compounding the problem of the lack of energy to make the cable systems work was the damage done to the system itself. As technology advances it seems that the grid used to support it becomes even more fragile. Infrastructure is dependent on common means of communications and inter-workings, and when the delicate balance is disturbed the interruption is widespread. “Although networks have been hardened to provide more robust services, Sandy proved yet again that there is still strategic planning necessary to ensure...customers have access to information and communication on TV and handheld devices, as well as instant messaging and social networking” (DiGiacomo, 2013). Compliance with existing standards for cable systems, such as the many American National Standards (ANS) developed by the Society of Cable Telecommunications Engineers (SCTE) and other standards developers, can help to ensure that there is protection.

Electrical companies worked tirelessly to repair the damage after Sandy, and some companies were able to assess and restore service more quickly than others. In spite of the prior mentioned adoption of continuity plans, not all companies displayed compliance. This brings to light a need for greater accountability by companies in the public and private sectors to demonstrate reliable implementation of effective business continuity plans. Once repairs were underway and service began to be restored to the area, the focus quickly became how utilities and service providers could be better prepared for similar disasters going forward. It was found that some companies were well prepared and able to address service concerns in a timely manner considering the circumstances, while others were found to have poor maintenance programs for existing equipment and defunct management systems. “New York’s Consolidated Edison generally got high marks for the response and recovery work. But in Long Island, [LIPA] is getting crucified in the press because of its slow response, poor maintenance of an aging above-ground distribution system, and general mismanagement” (Lucy, 2012).

It is not just electrical, telecommunications, and gas services that are affected by disaster. Medical care can be interrupted if the technologies used to manage records and treatment plans are affected. Financial institutions may face power, telecommunications, staffing, and other challenges. Transportation can be disrupted. Educational institutions, retailers, and workplaces may be closed. All of these foundational aspects of society rely on the same basic infrastructure, and any time that is interrupted the effects are far-reaching. Effective emergency management and continuity plans based on the expertise contained in standards have the power to reduce the strength and breadth of those effects.

Modern Contingency Planning

Businesses no longer think of contingency planning as an optional program to have just in case something bad may happen from a disaster of some sort. Having a plan in place presents a value in itself because the means and wherewithal to manage recovery are already in place when the disasters occur. The time saved in coming up with a quick and reactionary plan is just a small part of the savings involved in having completed a risk assessment and mitigation strategy.

Non-compliance to emergency preparedness standards can present unforeseen costs for a company. “Just as an organization is picking up the pieces of a shattered infrastructure, it may find itself in hot water with the relevant authorities for failing to plan” (Dimartini & McAnally, 1997). In addition, in today’s global market many companies will choose not to do business with other companies that have no business continuity plan to ensure that products, services, and expertise will be available after a disaster. Part of a company’s continuity plan may specify that its affiliates have a contingency plan in place that excludes companies who do not meet certain standards.

Conclusion

Standards are meant to protect commerce and society, and part of that protection must come from companies recognizing that having a business continuity plan is necessary not only for themselves but also for their customers and affiliates. Continuity plans must encompass all aspects of risk, whether it involves energy, emergency management, communications and information technology, recordkeeping, or interdependence with other suppliers and affiliates. The plan must address the crisis period, the emergency response period, and the recovery and restoration period, and it must be reviewed and tested for effectiveness.

It is not a matter of *if* the next disaster will occur, but rather a matter of *when*. The standards in place to assist companies with their business continuity plans are there to use as a guide to manage post-disaster management. And while these standards are often updated after major disasters in the United States, it is clear that the process is an ongoing need and should be addressed continually. Members of the private and public sectors must remain vigilant to identify the risks that exist within their management systems. As technology advances, we must continually identify and address the deficiencies and interdependencies related to our energy sources, infrastructure, and business practices.

References

- DHS Adopts Standards for Private Sector Emergency Preparedness Program. (2010, June 21). *ANSI News and Publications*. Retrieved from http://www.ansi.org/news_publications/news_story.aspx?menuid=7&articleid=2567 on April 13, 2013.
- DiGiacomo, D. (2013, January). Some lessons from Sandy. *CED Magazine*. Vol. 39 Issue 1, p13-13.1/2p. Retrieved from Business Source Complete on April 10, 2013.
- Dimartini, W. & McAnally, P. (1997, December). Regulating disaster recovery. *Internal Auditor*. Vol. 54 Issue 6, p42.7p.1 Chart. Retrieved from Business Source Complete on April 10, 2013.
- Fuller, C.W. & Vassie, L.H. (2004). *Health and Safety Management: Principles and Best Practice*. Prentice Hall, Upper Saddle River, New Jersey.
- Lucy, J. (2012, December 1). What We Learned from Superstorm Sandy. *Electrical Wholesaling Exclusive Insight*. P1-1, 1p. Retrieved from Business Source Complete on April 10, 2013.
- Warner, C. (2013, January). New Jersey's power and fuel infrastructure was no match for Sandy. *Electric Component News*. Vol. 57 Issue 1, p8-8. 1p. 1 Color Photograph. Retrieved from Business Source Complete on April 10, 2013.
- Zellen, B. (2007, February 2). After Katrina: Confronting the Business Continuity Challenge. *Technology Innovator*. Retrieved from <http://technologyinnovator.com/index.php?articleID=9871§ionID=238> on April 13, 2013.