FIRESTORM®
PREDICT. PLAN. PERFORM.

CRITICAL DECISION SUPPORT:
PERSPECTIVES ON BUSINESS CONTINUITY AND CRISIS MANAGEMENT

Samuel D. Smith

DATE: 04.15.11

1000 Holcomb Woods Parkway | Suite 130 | Roswell, GA 30076 | 770-643-1114 | **Fax:** 1-800-418-9088

www.firestorm.com

Page Intentionally Left Blank

INTRODUCTION FROM FIRESTORM®

This white paper offers critical senior-level perspectives on business continuity and crisis management. Samuel Smith's perspectives were gained through more than ten years of experience leading this function as senior vice president at the Federal Reserve Bank of Cleveland, and as a banking consultant. This white paper provides an actionable approach to developing a business continuity and crisis management program. The white paper includes best practices and valuable lessons learned from his years of direct experience.

The task of building an actionable business continuity and crisis management plan can seem overwhelming. This white paper's intent is to simplify the topic and help senior leaders in banks and other organizations chart a path forward. The principles discussed are universally applicable. The views expressed are Samuel Smith's and are not those of the Federal Reserve System. Mr. Smith is a member of Firestorm's Expert Council™, and his insights align to the Firestorm **PREDICT. PLAN. PERFORM.®** process.

BACKGROUND

The Federal Reserve System is the central bank of the United States. It is composed of the Board of Governors in Washington, D.C., an independent government agency, and the twelve regional Federal Reserve Banks that it supervises. The Federal Reserve Bank of Cleveland is one of these twelve banks. The Reserve Banks have corporate structures with their own boards of directors and officers.

The Reserve Banks are the operational arm of the Federal Reserve, and they perform economic research, supervise and regulate banks, and operate the nation's payments system. Millions of financial transactions worth billions of dollars flow through the Reserve Banks each day. Therefore, it is imperative that the Reserve Banks are themselves resilient and have extensive business continuity and crisis management plans that are tested.

Reserve Bank plans cover all aspects of operations, support and policy functions. These have been forged through testing and actual business interruptions caused by floods and water, power and telecommunications outages, and through preparation for the year 2000 roll over. The experiences of 9/11 and Katrina led to further plan refinement.

AN APPROACH TO BUSINESS CONTINUITY AND CRISIS MANAGEMENT

Mr. Smith's approach is consistent with Firestorm Solutions, LLC's **PREDICT. PLAN. PERFORM.®** process. Assistance from an experienced firm can accelerate business continuity and crisis management program development and increase its quality and effectiveness at a lower development cost.

The approach below addresses:

- The foundations of strategy,
- Organization and culture,
- The phases of threat assessment and mitigation,
- Development of business recovery and crisis management plans, and
- Plan testing and refinement.

STRATEGY, ORGANIZATION, CULTURE, AND LEADERSHIP

Business continuity and crisis management should be one of an organization's key assets. Business continuity and crisis management should be an agenda topic during meetings of an organization's Risk Management Committee and board meetings.

There is no question that every organization needs a robust business continuity and crisis management program. The downside for the organization and its customers is otherwise too great. The results of a slow or ineffective recovery from a disaster are incalculable, as witnessed in the news.

Additionally, Federal banking regulations prescribe business continuity plans for banks and their outsourced data processing suppliers, which are audited as part of safety and soundness examinations. Recent legislation, PS Prep (Public Law 110-53, Section 534), directs the Department of Homeland Security to publish voluntary standards for business continuity plans for other private organizations. Organizations that wish to do business with the government will have to meet these standards over the next few years.

For these reasons, boards of directors have a keen interest in business continuity, as the board shoulders the ultimate responsibility corporately and personally. Leadership of program development rests with the CEO, assisted by senior officers and management staff. A best practice is to assign responsibility for business continuity to a senior officer. Also, it is helpful if this leader has responsibility for facilities, human resources, physical security and information security.

The business continuity program should be administered by a senior business continuity officer, or where no such position exists, by the officer responsible for the business continuity function. A best practice is to assign this duty to an individual who has direct experience, training, or has become certified in risk management/emergency management.

Management of each functional level is responsible for their component of the program, including threat mitigation and business recovery plan development. It is a best practice for each business function manager to assign a staff person to be a member of the business

continuity team. The team is charged with testing, updating plans and participating in program administration.

Experience confirms that a participative organizational culture is a prerequisite for success. Employees must be encouraged to raise concerns, make suggestions, take initiative and work collaboratively with each other. In addition, employees need to have disaster plans at home to allow them to focus on crises at work. Recovery of complex operations requires agility and teamwork on everyone's part. Maintenance of a healthy culture that supports process improvement is the responsibility of the CEO and the senior leadership team. Failure to lead will result in a failed program.

THREAT ASSESSMENT AND RISK MITIGATION

The threats that could affect an organization are myriad and include wind storms, fires, floods, power and telecommunication outages, earthquakes, interruption of water supplies, workplace violence, terrorism, nuclear, biological and chemical contamination, and pandemics to name a few. 9/11, Hurricane Katrina, the Gulf oil spill and the recent earthquake and tsunami in Japan, with damage to their nuclear plants, are prominent examples of unthinkable disasters that have occurred within the last ten years. If a threat can be imagined, it can happen. On a local level, disasters too can occur. Business continuity and crisis management plans can keep a small disruption from becoming a disaster.

It is useful to view threat assessment, mitigation and business recovery as related but separate endeavors. Threat assessment involves identifying internal and external threats, their probability of occurrence, their specific risks to the organization, as well as identifying existing gaps. Mitigation involves implementing measures to lessen these risks and close the gaps. Business recovery is the process of recovering the organization after being affected by a threat.

As mentioned, there are a seemingly endless number and variety of threats which have unique characteristics, and the assessment process can be easily managed by categorizing each threat as to its effect on supply chains, data processing and data integrity, buildings and people. Then, appropriate risk mitigation measures can be selected. Mitigation decision making is where cost benefit analysis is important. Threat risks and their potential costs are weighed against the cost of mitigation. Time to recovery objectives factors into these cost calculations. Not every function can be restored at the same time. The higher the confidence level, and the shorter the recovery time, the higher the cost.

A detailed business impact analysis empowers senior management to focus on critical decisions. Understanding recovery time objectives and departmental interdependencies are key to prioritizing actions.

IT Risk Mitigation

Software testing, automatic offsite backup of data, physical and information security measures, redundant computer systems, backup power generators, uninterruptable power supplies and geographically separate processing sites are common measures taken to reduce risks of data loss and computer outages. Experience has shown that sources of backup cooling water for computer equipment should be added to this list. Also, water for hydration, sanitation, and air conditioning is critical for building operations and employee sustainability. Power and water are the most important resources needed for the continuity of an enterprise other than its employees.

Loss of IT capabilities is damaging, but loss of the buildings housing them is a larger problem. Loss of employees for whatever reason is the worst case scenario. Measures to promote employee health and security are important mitigation steps.

Supply Chain Risk Mitigation

Supply chain failure is the most common failure in a disaster. As organizations have adopted just-in-time inventory methods and outsourced data processing centers, call centers, and other critical functions, they have become more dependent on their supply chains. Supply chain failure is the most common failure in a disaster. Due diligence is required to assure that outside suppliers have their own effective business continuity and recovery programs and are not themselves a threat to the company. A best practice is to include business continuity and recovery plan requirements in service agreements with the provision that they be audited. A quantitative assessment versus best practices is best.

Experience shows that electrical power, water, gas and telecommunications services should be viewed as important parts of the supply chain. Power generation facilities and the underground infrastructure are astonishingly old and fragile in many cities. Power outages, water main failures and subsequent floods are more frequent than most realize. Broken water mains often flood power and communications conduits under the street, resulting in power and telecommunications failures.

It is prudent and enlightening to visit power, gas, water and telecommunications facilities to assess their resilience and determine the routing of these services to one's buildings. Also, loss of electrical power in a city affects city water pumps, and few cities have backup generators to support their water operations, which leads to an interruption of water delivery.

Due to the fragility of underground utilities and the ever present "back hoe" problem, it is wise to consider diverse routing of power, gas, water and telecommunications into a building where that is possible. As mentioned, consideration should be given to installing backup water storage tanks for cooling and sanitation. Bottled water supplies should be readily accessible for

employee hydration, and arrangements should be made with sanitation vendors to provide portable toilets in a water or sewer emergency. Similar agreements should be reached with diesel generator fuel suppliers to obtain priority during an extended power outage.

Other Considerations

If a crime is committed on the organization's property, the area can be cordoned off as a crime scene for several days. The crime scene process can be extremely disruptive to an organization and pose a public information challenge. In essence, crime scene restrictions can be a threat in themselves, and organizations should take steps to mitigate them.

A final suggestion regarding disaster due diligence is to develop a close relationship with fire and law enforcement agencies, sharing plans with them and hosting building familiarity sessions. It is beneficial to be on a first name basis with possible first responders. An emergency should not be the first time fire or law enforcement personnel tour the building, other than the fire inspector. It is important to remember that the fire chief assumes command of the building in a fire, and it is best that he or she is familiar with the building and owner concerns prior to a fire occurring.

BUSINESS RECOVERY PLANS

Business recovery plans specify those steps to be taken at both the organizational and functional levels to recover the organization after a disruption. Plans should cover loss of supply chains, systems, buildings, employees or a combination of these. It is more manageable to focus plans on the worst case scenarios, loss of buildings and loss of employees, which subsume lesser contingencies. By their unique nature, pandemic recovery plans are generally separate plans.

These plans are developed from the ground up by each function, and they are detailed by nature. The organizational level plans focus on evacuation, relocation, and crisis management, including crisis communications. A best practice is to set targets for time to recover from a disruption, which is a regulatory requirement for banks.

Where an organization does not have an offsite command center already set up, arrangements should be made ahead of time with a local hotel, or other suitable facility, in the event of a building evacuation. It is helpful to test building evacuation and these offsite command centers at the same time. It is a best practice to equip "cold" relocation sites with IT and other necessary equipment and make contingency transportation arrangements.

Recovery of the New York financial markets within a week in the aftermath of 9/11 was miraculous, and it was a prime example of the importance of business recovery and crisis management plans and the geographical diversity and multiplicity of backup processing sites.

Many of the market participants' processing sites were outside of the city, which sped recovery. However, it was reported that a primary clearing bank had its backup site located in the World Trade Center, forcing it to go to a tertiary site. The lesson learned is that primary backup sites should have sufficient geographical separation from the day-today operational location.

While airplanes were grounded on 9/11 and the days following, the Reserve Banks continued accepting check deposits, absorbing the float until the checks could be presented to paying banks. This assistance prompted Bank of America to send packages of "Lifesavers" to all Federal Reserve Banks and their branches to show its appreciation for mitigating the total disruption of the air transportation supply chain.

CRISIS MANAGEMENT

It is important that crisis management steps be initiated immediately upon the occurrence of a crisis, which begins by determining the extent of the problem and notifying management and key employees. Afterhours calling trees have traditionally been used for this contact. Automated methods similar to reverse 911 and broadcast emails are in favor to expedite this process.

A best practice after hours is to ask crisis team contacts on the calling tree to dial into an always available conference call line for the initial crisis management session. The crisis management team should include the CEO, senior officers, and key personnel representing operations, security, marketing, human resources and public information. The senior business continuity officer and his staff facilitate the crisis management discussion and decision making.

Depending on the severity of the crisis, a command center is set up including PC's, white boards, and phone lines. As status information flows into the command center, it is useful to record it on the white board for the crisis team to see at a glance.

Human Resources is charged with updating employee information phone recordings and web site with status and instructions. The security officer should communicate with fire and law enforcement, if necessary. Marketing should develop customer communications, and public information should craft carefully worded statements for the media. It is imperative that media inquiries be referred to an experienced, designated spokesperson. The secretary to the board or CEO should inform directors, when appropriate. The command center is staffed around the clock, and team members are rotated until the crisis passes and full recovery is completed.

Time is of the essence in crisis management, and it deserves its own plan specifying participant responsibilities. A measure of success is that the dimensions of the crisis are known and recovery activities are begun within the first few hours. In the absence of a tested crisis management plan, the crisis management process can be a turbulent and reactive instead of a calm and productive experience.

PLAN TESTING AND REFINEMENT

As it is said in the sports vernacular, a team plays like it practices. Therefore, it is imperative that plans be regularly tested. There are several types of exercises, tests, and table top exercises, involving individual functions, and broader, multi-function exercises which may involve large portions of the enterprise for a full day. Table top exercises should be done at least annually by each function. More frequent tests establish effective working teams. Moving from annual testing to semi-annually or quarterly will improve predictability of response. Tests involving multiple functions, individual offices or the whole enterprise should be done at least annually. Regular exercises developed by an independent third party can provide insights into potential gaps. In many cases, the individual who wrote the plan will design an exercise that focuses on the existing plan execution and not emerging vulnerabilities.

During the multi-function tests, teams are presented with a realistic, surprise crisis scenario affecting the organization over several days. They must recover operations during the exercise in a compressed time frame over several hours. The exercise is facilitated and includes the crisis management team. Reports are made at various intervals as would be done in a real crisis. At the end of the exercise, lessons learned are presented and recorded, and plans are subsequently modified.

It is amazing how realistic these exercises feel, how enthusiastic the participants embrace the exercise, and how much is learned. They are an excellent way for crisis management leadership and functions to practice working cross-functionally as a team to recover from a disaster. A consistent realization during these exercises is how important employee, customer, media and board of directors' communications are during a crisis. The value of these exercises, in revealing unforeseen vulnerabilities, cannot be overstated.

Real crises experiences provide the best information. Lessons learned from them should be discussed after every disruption, and plans should be updated where gaps are identified.

CONCLUSION

The suggested approach to business continuity and crisis management presented in this paper is consistent with Firestorm Solutions, LLC's **PREDICT. PLAN. PERFORM.®** process. The subject is strategic to any organization, especially to financial institutions. The Dodd-Frank Wall Street Reform and Consumer Protection Act, FFEIC Guidelines, standards, and Public Law 110-53, Title IX add new risk requirements.

A successful business continuity program depends on having a sound program organization, a healthy, participative corporate culture, and senior management leadership. It begins with the assessment and mitigation of threats, development of business recovery and crisis management plans, and ends with testing these plans to validate their effectiveness and

training the participants in the graceful recovery from a crisis. Business recovery and crisis management plans should be updated as conditions and operations change with master copies kept in an accessible, secure location.

To understand the strengths and weaknesses in your current business continuity plan relative to best practices, conduct a high level self-assessment of your current plans versus best practices.

THE FIRESTORM® BUSINESS CONTINUITY SELF-ASSESSMENT

Firestorm encourages private sector entities to use the PS Prep certification framework as a means of measuring the preparedness of their organizations, as well as that of their key suppliers/vendors. Firestorm's Business Continuity Self-Assessment provides insight to an organization's current level of preparedness, and provides a roadmap for the development of an up-to-date business continuity program that will empower organizations to mitigate threats and vulnerabilities.

Firestorm's Business Continuity Self-Assessment process specifically addresses a high-level review of business continuity program alignment to industry standards and best practices. While not the primary driver in many companies, Firestorm's Business Continuity Self-Assessment also addresses emerging PS Prep guidelines for private sector business continuity and preparedness planning. The self-assessment is focused on fifty-five data points. The results of the assessment will be a Findings Report that will measure the preparedness level of your company's overall program, based on industry standards and best practices.

FIRESTORM'S PREDICT. PLAN. PERFORM.® PROCESS

As experts in vulnerability analysis, risk mitigation, planning, and crisis management, Firestorm offers organizations of every size immediate access to its expertise and guidance in planning and preparing for any type of emergency along with plan enhancement/development, including business continuity, crisis communications, crisis management, security, workplace violence, and communicable illnesses. Firestorm's guidance allows its clients to complete plans, address emerging issues, and have resources available as needed. The client directs the project plan, timing, and resource level required. Firestorm manages the process and produces the deliverables. Firestorm will complete the work necessary to bring planning to the level of best practices.

Proper disaster planning requires that companies **PREDICT** the vulnerability, **PLAN** the response, and **PERFORM** when the event occurs. The **PREDICT** phase classifies the critical vulnerabilities, identifies key emergency personnel, ascertains critical decision processes, analyzes gaps, identifies infrastructure and supply chain needs, and defines communications requirements. The **PLAN** phase develops the strategy, constructs the plan, and involves the appropriate

personnel to assure their buy-in and commitment. The **PERFORM** phase establishes protocols for implementation, community involvement, communications, test exercises, audits, reviews, updates, and compliance.