Ten Years After

Reflections on 9/11

In America, everyone remembers where they were on 9/11. In that horror, we all recognized an unexpected and "**asymmetric**" attack by the few against a much larger, more powerful enemy. While we did not anticipate that a small band of guerillas could inflict so much damage within our borders, we have learned how to make sure those methods would never work that well again.

The tactics used on 9/11 did not even last through that day. As the passengers on the airplane over Pennsylvania demonstrated, our people can react to a new threat as fast as anyone can put it into practice. On the ground, people committed too many acts of heroism to count, from the small and technical to the ultimate and unforgettable. We will try to remember them, the fallen and the wounded and those who quietly kept the machinery of our lives going in the aftermath. It's hard. We don't like to focus on the price so many paid, or those big holes in our security we still need to address.

We've locked the doors, improved our screening procedures, and closed down the easy routes into positions of destructive power. It won't be so easy next time. But we can't pretend that we can close and lock every door, anticipate every attack or prevent anyone from inflicting damage on our shores.

It **will** happen again: it's the price we must pay for keeping our society open, for protecting the foundation of a republic based on the pursuit of life, liberty and the pursuit of happiness. The tenets of our nation are fundamentally incompatible with any attempt to seal our borders, or to create the type of police state that would minimize the threat. While our safety and security are important, they are not the only goals we must pursue. We have made the changes we can live with, and perhaps a few that we cannot live with: time will tell.

What else have we learned from that day? In the world of business, we learned that our plans for responding to attacks of the few against the many were not adequate. In some cases, the plans were abandoned in favor of an ad-hoc response that confronted the exigent circumstance. Those who created the plans failed to consider a scenario of this magnitude, one in which the financial markets would close down for a week, the loss of critical staff would cause players to suspend operations, and customers would lose some confidence in our ability to recover.

In the aftermath, the SEC defined new **rules** for all players in the market. To play the game in this new post-9/11 world, a business must create continuity plans that define how they will recover their mission critical systems, their data, and communications with customers and other players in the market. They must define how they will grant customers access to their funds and securities in the event they are no longer able to stay in business. Each company must also deliver a summary of their plans to customers without exposing details that an enemy could use to disable the company.

Asymmetric attacks change the rules of the game: there is no effective offensive plan short of total warfare. Instead, we must prepare for recovery from the random or chaotic shot from an unknown direction.

It's a significant challenge, and requires some creative thought. However, it's not without parallel: drafting plans for natural events is similar in some respects. We don't really know where or when a tornado may strike, or how much damage it may inflict. The residents of Joplin, Missouri found out how well they had planned for the unexpected. As did the managers of the Fukushima Daiichi Nuclear Power Plant after the tsunami hit. What they have in common is the scale of an event, the number of people who were affected, and the need for more effective communication.

Just as natural and "man-made" events can have common impacts, useful recovery and continuity plans are built from a set of best practices. These include the following:

Identify critical activities that support the market

Acknowledge interdependencies and market position

Determine appropriate resumption objectives

Major players should set a target of 4 hours

Maintain sufficient out-of-region resources

Maintain staff, equipment and data for high volume

Routinely use or test resumption arrangements

Test connectivity, functionality and volume capacity; test with partners

Other topics to consider include the following:

Out-of-region arrangements are critical: account for staff, training and travel.

Access to data is critical: plan to transmit data continuously, use multiple network resources and draw from one or more active backup sites.

Develop flexible plans: identify single site and wide-scale strategies. Include backup facilities, clearing and settlement organizations, and key service providers in testing efforts.

When drafting plans, it pays to remember that it's the **people** on a recovery team who will make them work. Take the time to assign authority, define roles, and give those we will count on the **charter to act** when an event occurs. Formally give them permission to exercise their wisdom, make decisions, and re-write the plans and protocols, on-the-fly if necessary, to meet the objective.

Whether it is saving lives, protecting our assets, bringing a business back up to serve its customers, or just letting the families know that everyone is accounted for, we are all invested in making our recovery plans **work**. They may be the best line of defense we have against the few who would attack the many.

For more information about business continuity and recovery planning, please use the resources listed below:

Intro to Business Continuity Planning (http://www.desolationpress.com)

This course supports corporate and government professionals, and other students who will participate in business continuity and recovery planning efforts as a subject matter expert, a recovery team member, or in a management role.

For advanced content and certification programs required to supervise planning efforts, contact the Business Continuity Institute (http://www.thebci.org/) or DRII, the Institute for Continuity Management (https://www.drii.org/index.php).

The Disaster Recovery Journal (http://www.drj.com/) is an excellent industry resource for those seeking resources, community interaction and ideas for starting or extending a recovery program in their organization.