# Effects Of 9/11 Attacks On Organizations Risk Management Processes

Posted on May 7, 2020

The aftermath of the 9/11 attacks in the United States of America led to the implementation of various disaster recovery plans and the inception of technology to counter such risks in the future. This attack on U.S soil brought about concepts dealing with risk management best suited to different organizations. I.T. was embraced in many organizations, thus integrating it into the enterprises" risk management capabilities. After this disaster, the Federal government placed hundreds of millions into upgrading the internal systems of control with the intent of complying with the Patriot Act (Khosrow-Pour, 2013). Conversely, this law had in it that all the financial companies ought to beef up their capabilities to flagging transactions seemingly suspicious from customers. Some firms went back and analyzed what they missed, thus resulting in an ambush unknowingly. An example of these firms is Merrill Lynch, which was at ground Zero and lost all its primary data for one month and two weeks. From their analysis, they found out that the regular gap analysis serves as the core component of preparedness in times of disaster. Human contingency was the key to evading such incidents of big disasters.

## Use Of Social Media And Other Methods Of Communication In Disaster Management

Social media is the current way of getting information quickly with some using it in responding to emergencies. Government and non-government agencies have also embraced the use of technology in countering disasters. An example is the Red Cross has integrated web 2.0 technologies to various regions in the world and thus can link with them in disaster times (Poole, 2016). The first indicator of disaster on the globe was published on Twitter, thus enabling a large population to get the information in real-time. This first post was in the year 2013 and thus posted the Boston Marathon bombing and the Westgate Mall attack that was in Kenya.

Additionally, there is also the use of email and even video chatting, whereby, in case of disaster, an individual can record a video or place it in real time and show it to the world. After relaying the video to the world, then the government and other disaster-organized groups can intervene to salvage the situation. A social media call can include calling a toll-free number to a specific organization, thus getting a quick response (Wai-chi Fang, 2010). However, despite the use of social media in relaying quick emergencies, there might be misrepresentation on these social media channels. In such incidents, this misrepresentation can be corrected immediately since social media has self-regulation, as other users can verify the misrepresentation and correct it.

# Distanced Geographical Locations For Backup Operations And Its Implications To RPO And RTO

While in preparations for a backup, Organizations ought to consider the distance since there is no rule of thumb I regard to the appropriate distance between the data centers and the recovery sites. From an American based Disaster recovery journal, some businesses state that good recovery site should be far away a thousand miles. Lamentably, between 2007 and 2010, the average distance was shrinking between the primary center for data and the farthest backup center (Khosrow-Pour, 2013). From various I.T surveys, the best and most comfortable distance is less than 100 miles, with 21 percent of the respondents stating that 25 miles was the best fit. The consequences of distance in the recovery of information in disastrous period befall RTO and RPO. These two help in determining the processes and information most important to the business, thus calling for the shortest recovery time and work back from the information center (Wai-chi Fang, 2010). After the 9/11 attack, the Federal Reserve was advised to integrate appropriate levels of diversity in the geographical distances between the backup sites and the primary center for the back office operations.

The benefits of having a close site are allowing a tighter synchronization between the secondary and the primary sites and leveraging the current employees together with the offsite backup service. Despite the distance, a geographical disaster inclusive of a tornado and hurricane could take both recovery and primary sites. Conversely, placement of the DR site far away can lead to the creation of a replication issue to some systems at times calling for a complementary workforce that could result in enormous costs.

# Evaluations Of The Use Of Cloud Services In Data Recovery Options

Cloud computing services, mostly based on virtualization, take a distinct approach to the disaster recovery process. Through cloud services, the server, inclusive of the operating systems, patches, applications, and data, is encapsulated in a single bundle (software) (Wai-chi Fang, 2010). This server can be copied or even backed up to an external data center and later spun in minutes to a virtual host. With cloud services, the recovery of the warm site is a much cost cost-effective option whereby the backups of the critical servers are spun in a few minutes on private cloud's host platforms (Wai-chi Fang, 2010). A continuous backup is being created whereby platforms, hardware, and networks will be virtualized.

The following are ways through which cloud services increase effectiveness in an Organization's dealings:

- The inception of cloud services has brought the conservation of resources, thus evading

expenses involved with setting up a duplicate data center;
- There is a faster response in case of disaster with instances of minutes to counter a disaster in an organization;
- Organizations with cloud serving as disaster recovery do not need to choose a location for a recovery facility since cloud services can be moved to different parts of the world.

# Is Cloud Services An Ideal Recovery Option?

Cloud-based backup services are the way to go for all businesses, irrespective of their sizes. According to a 451 Research Marketing Monitor survey, the business market has expectations of 21 percent growth over the coming three years, with 70 percent of the surveyed companies that did not have cloud-based disaster recovery expecting to embrace it in the next one to two years (Poole, 2016). Given the lack of resources to adequately replicate their data centers, both small and large enterprises have intent to deploy cloud-based disaster recovery options (Wai-chi Fang, 2010). Cloud services for disaster recovery are the key to many data-related disasters in various Organizations; thus need to deploy these continuous and synchronous replicating services for the best data storage performances.

# References

Khosrow-Pour, M. (2013). Interdisciplinary Advances in Information Technology Research. *Computers*, 357.

Poole, J. (2016, February 29). *Disaster Recovery in the Clouds Equals Business Continuity for All.* Retrieved from blog.equinix.com: https://blog.equinix.com/blog/2016/02/29/disaster-recovery-in-the-clouds-equals-business-continuity-for-all/

Wai-chi Fang, M. K.-j. (2010). Security Technology, Disaster Recovery and Business Continuity: International Conferences, SecTech and DRBC 2010, Held as Parts of the Future Generation Information Technology Conference, FGIT 2010, Jeju Island, Korea, December 13-15, 2010. Proceedings. *Information Technology*, 300.

https://www.computerworld.com/s/article/9219867/9_11_Top_lessons_learned_for_disaster_recovery