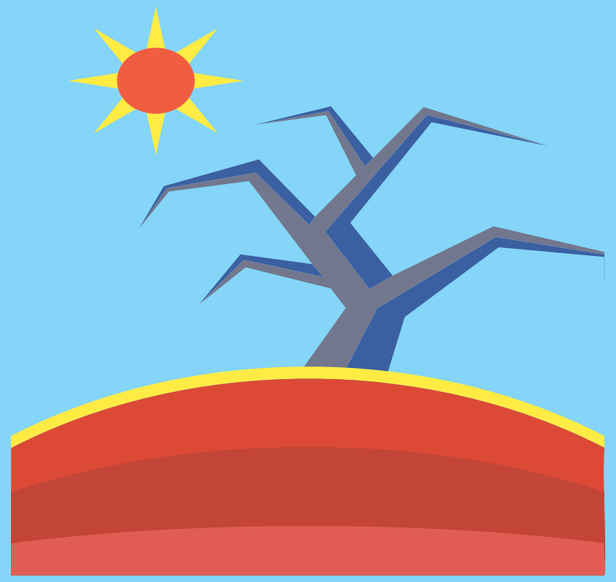

WHAT HAPPENS WHEN DISASTER STRIKES?

Disaster recovery plans have been put on the shelf to collect dust, given a cursory annual review, and are not put back up until an auditor or examiner asks to see it.

BY MARC RICCIO

Has your community been effected by a natural disaster? If not, it may only be a matter of time. When it happens, will your institution be ready?

This issue has always faced institutions but was made a regulatory issue for Y2K. Remember 1999 when we were all being told that computer systems all over the world were going to fail? We all worked diligently to insure that when (or more correctly, if) we had a massive computer meltdown, our institutions would all be able to operate and service our customers. January 1, 2000 came and went without so much as a burp in most computer systems and has gone down in history as one of the biggest non-events of all times. Conversely, the natural disasters of the past several weeks have recorded the highest levels of destruction in history.

Disaster recovery plans have been put on the shelf to collect dust, given a cursory annual review, and are not put back up until an auditor or examiner asks to see it. Does it meet the regulatory requirements? Probably. Does it protect your institution and customers in today's environments in the best possible way? Maybe that deserves another look.

During the 9/11 crisis, one of the largest areas of financial institutional markets was shut down for days and in some cases weeks. The New York Stock Exchange, the New York Federal Reserve, and the corporate offices of the biggest banks in the world were all affected. The disruption of these businesses could have had a devastating effect on not only the United States, but on world markets as well. The disaster recovery plans utilized by these institutions worked, but it also provided a real test that uncovered weaknesses and flaws.

Disaster recovery is an all-encompassing concept. To be effective it needs to be broken down into subsections:

>>Business continuity

>>Incident response

>>Notification alerts

Business continuity is an institution-wide plan that incorporates all critical elements of your business. A meaningful business continuity plan (BCP) incorporates all institutional resources, employees, locations, vendors and processes and addresses how each will react to a disaster. It is important to keep in mind that a critical vendor or process may not be occurring in your part of the country but may still affect your business. The interdependency of your institution with other businesses is a risk that needs to be assessed, analyzed, and considered. The collection and correlation of data and resources is an integral part of your BCP.

During the 9/11 crisis, one of the largest areas of financial institutional markets was **shut down for** days and in some cases weeks.

In order to have a coherent BCP the institution first needs to conduct a business impact analysis and a risk assessment. What is the consequence on your business if your core provider in unable to function as opposed to the impact of the Internet being down. Both are important functions in today's financial institutional environment but may impact your ability to service your customers differently. Next the institution must develop a strategy of what will happen if a disaster occurs. Is there a secondary provider? Can the institution function for a period of time without a specific service? The answers to these types of questions provides a solution strategy which will then need to be tested, accepted and disseminated throughout your institution. The last issue to be addressed is maintenance of the BCP. An annual review is mandatory, more frequent reviews are advisable, and reviews after an incident are a must. Tools are available to assist your organization in compiling this in-

It may be an impossible task to plan for every type of disaster but keep in mind that your institution's disaster recovery plan should **not be a stagnant document.**

formation, keeping it current, and making sure it is in a safe and accessible environment should your institution need it.

Incident response, as alluded to above, is how your institution reacts to a problem. An incident response plan allows your institution to systematically respond to problems. This type of plan ensures that all incidents are handled by appropriate personnel in a professional and consistent manner. It also provides your institution with ways to improve and prepare for future issues. We are all conscious of the potential financial or regulatory risks this type of plan may mitigate, but consider how this plan may reduce the huge impact on your institution's reputation if misinformation is made public. Knowing who is going to speak to law enforcement, the press and customers, and what is to be said, is just as important as protecting the financial assets of your organization. The aftermath of an incident should also be addressed. What went right and what went wrong. Documenting this information in a central location is imperative.

Lastly, consider how are you going to let your personnel know what is going on. The days of having a phone tree are obsolete as our organizations grow larger and people are more spread out. Maintaining a system that knows ahead of time who should be notified for particular incident message and knowing that the message is received, is not only efficient but may be life saving. Say a fire occurs in the early morning at one of your branches. The branch manager is alerted by the fire department of the alarm. The branch manager is able to send an immediate notification to his staff. One employee, that sometimes goes in early, does not reply. The manager is then able to advise the fire department that there is a chance someone may be inside. Or conversely, all reply and the fire department does not have to risk personnel conducting a search of a burning building.

This article started off with a list of natural disasters that have been in the news recently. Also consider the un-natural disasters. Security leaks, hacking, cybertheft to name a few. Our society has become enmeshed in the Internet, social media, and online banking. There was a danger to consider in 1999 when we started to contemplate a disaster recovery program, but the risk has escalated so dramatically since then that this is now one of our country's biggest threats. There are reports almost daily on large databases of information being compromised, yet the use of computer-aided programs to assist us in our daily lives continues to grow. It may be an impossible task to plan for every type of disaster but keep in mind that your institution's disaster recovery plan should not be a stagnant document. ❖

About The Author

Marc Riccio, President of Specialized Data Systems, Inc., has over thirty years of experience providing software solutions to the financial industry. Marc is known for his forward thinking and vision of introducing new and innovative technologies including "rules-based" Loan Origination software, COLD/Document Image Systems, Internet Security Services on Demand, Cloud Computing and now Operational Risk Management software.

Index of Advertisers