



# THE AUDITOR'S REPORT

NEWSLETTER

A Publication of Nearman & Associates, CPAs, P.A.

## DISASTER RECOVERY

### Staying Afloat With Disaster Recovery Planning

*"When one asks me how I can best describe my experience in nearly forty years at sea, I merely say, uneventful. Of course there have been winter gales, and storms and fog and the like. But in all my experience, I have never been in any accident ... or any sort worth speaking about. I have seen but one vessel in distress in all my years at sea. I never saw a wreck and never have been wrecked nor was I ever in any predicament that threatened to end in disaster of any sort."*

~Captain E.J. Smith, prior to sailing the Titanic<sup>1</sup>

Captain Smith is credited with this quote in 1907, five years later Captain Smith went down with the Titanic on what was to be his last voyage before retirement. You may be asking what does this have to do with me? I'm not the captain of a ship. Or, in a way, are you? Captain Smith was responsible for the lives of his passengers and crew; his decisions literally meant their life or death. You are responsible not for the lives of your members, but for something just as important, the confidentiality and security of their financial assets and personal information.

On just about any evening we can turn on the television and see destruction somewhere; some natural, some man-made. We can see reports coming from the northeast about snowstorms, we see reports from the southeast of hurricanes, reports from the west coast about fires and landslides, and the midwest brings us tornados. Obviously these natural disasters are not unique to any one area. A complete

disaster or business continuity plan will address these issues but will also address areas we may not consider a disaster but can have a profound effect on service delivery. If an electrical substation in your area should fail, how do you handle an extended power outage? Our internal systems, computers and hard drives are mechanical devices and will fail. It's just a matter of when. When did you last do a full tape *restore* of your data systems? Do you have procedures in place to address the theft of member information by an employee? From natural disasters to internal fraud, all are real threats; all can and should be addressed in your corporate business continuity plan.

**“Are you prepared? Will your members remain loyal if you are not prepared but a financial institution down the road is?”**

Are you prepared? Will your members remain loyal if you are not prepared but a financial institution down the road is?

The Disaster Recovery or Business Continuity Plans of many credit unions I have reviewed are inadequate. *Many were designed for Y2K events.* Since that time, they have not been updated, tested, or even given a cursory glance.

Right now you are thinking this doesn't pertain to me. We review our Business Continuity Plan annually. We have an independent third party on site as we test the plan, a thorough review is done,

and the plan is updated with any findings. Congratulations, you will probably survive a disaster when your peers will not.

If this isn't you, you may be thinking what do I need to do? The NCUA has given guidelines in NCUA Letter 97-CU-3 Corporate Business Resumption and Contingency Planning and NCUA Letter 01-CU-21 Disaster Recovery and Business Resumption Contingency Plans. First and foremost you need to know what critical pieces are required to continue to offer service to your members. If you lost one or all pieces, how would you regain services? What resources are available and what resources are lacking? Most of all, where do you start?

There are five primary phases for business continuity planning. First, establish the **Organizational Planning Guidelines**. Set up the work groups that will drive this program and identify the critical systems and services. Second, perform a **Business Impact Analysis**. In this phase determine for each critical system or service the types of failures that could occur and their likelihood. Define your minimum acceptable level of service. The third phase begins the process of the actual **development and writing of the plan**. But will it work? The fourth phase seeks to **validate the plan**. These tests can be disaster simulations, table-top tests, walk throughs, or any other various means to validate the plan. This phase also reviews the entire process to identify if anything has been missed. The final phase should be the easiest but is usually the one that is most overlooked.

*Continued on page 2*

<sup>1</sup> <http://www.geocities.com/southbeach/lounge/8816/quotes.htm>

The fifth phase is the development of the **communication plan**. In a time of crisis, too often we fail to notify those that need to know (regulators, members, media, etc.) and thus fail to control the information, leaving everything to the imagination.

Most credit unions I have seen have some form of a Disaster Recovery Plan. My advice is to review it. If a plan is not up to date, it won't work. Not too long ago we recommended keeping a roll of quarters in many Disaster Recovery kits. Why? The phone company had long held that part of its Disaster Plan was to get pay phones up and running first. This gave it the widest coverage with the least amount of effort. Have you tried to find a pay phone lately? Most of the phone companies have removed them for lack of use. If I was relying on the availability of pay phone service as part of my communication plan, that piece is now obsolete and I need something else. Little things like this are caught in the annual review process but so are the big things.

What about the fact that the server's tape drive went bad and was replaced. Of course, with newer and faster technology available you went with the upgrade. Now your old tapes don't work. A review of your Disaster Plan showed that the hot site only has the old tape drive available. Now what?

There are credit unions that don't have a plan or, using an on-line system, are relying on the Service Provider's Disaster Plan. If you don't have a plan at all, in addition to not complying with regulatory agencies, you are placing your members' assets at risk. Oh, but my Service Provider has a Disaster Plan. Check your contract with them as well as their third-party review (SAS70). You may be surprised to find that you are obligated to maintain a plan as well!

No one has ever said developing a Disaster or Business Continuity Plan is easy. *Your plan should be a living document; you can't do it once and forget about it.*

The development of a Business Continuity Plan obviously takes a lot of time and resources. Time and resources you might not be able to expend. The involvement of a qualified third party gives an objective view. Nearman & Associates has years of experience working with credit unions and the development of Disaster / Business Continuity Plans. Various levels of involvement are available. We will work with you and your staff in developing a **customized and workable plan**. If you already have a plan, we can review it and make recommendations as necessary. There is an inherent risk in not having a workable plan. Take the steps now to lessen that risk.◆

*Jay Simonton, CNA, CNE, MCP  
Information Technology Manager*