P.J. Longstreth, CFO

Disaster Recovery
(and then some)

Disasters come in all shapes and sizes. Whether it's a hurricane (or hurricanes) in Florida, a fire in California, a flood in Indiana or a plague of locusts in Washington, you will not be able to completely avoid disaster. The real question lies in how you are prepared to respond to a disaster. Said another way: you cannot prevent, but you can prepare.

The first step in preparing for disaster is to identify the things that are critical to your business – a phone line, powers, information about the bonds you have already executed. If something happened to your office, how long would it take you to be 'up and running'? Hours? Days? Weeks? Do you know what you would do?

Once you've identified the critical components, you just need to put together a quick plan.

- Do you have a planned site where business would continue (even if it is at your own home)? Do your employees or sub-agents know where this site would be?

- Do you know how to forward your phone line to an alternate location?

- Do you have a small stash of off-site powers and checks in the event something happens to the office?

- Is your computer information backed up and stored off-site (having a backup that is stored at the office only helps when the office is still in tact)? How much information do you know about your existing cases without the physical file from the office? (Shameless plug for BARS Network – see advertisement on p. 12)

If you can answer these questions (and the answers aren't "NO"), you are well on your way to being prepared for the worst. Well, almost…

There is also a different kind of disaster that is becoming more and more common – employee theft. An act of betrayal may feel significantly worse than a fire or flood. Someone in whom you placed your trust has taken advantage of that confidence. Here are a few quick things to do in order to protect yourself:

- SEGREGATION OF DUTIES – the people who receive checks/cash and prepare checks should UNDER NO CIRCUMSTANCES be the same people who reconcile your monthly bank statement. If these two duties are separated, it would take those two individuals working together to pull one over on you. If based on your staffing levels this is not an option, have two individuals count and initial the daily deposit slips. Accountability deters wrongdoing.

- Audit your sub-agents. If you need an audit program – call our office, we'll be happy to provide one for you.

- Periodically do some "back of the napkin" math (metrics) on the business that you've written for a period of time and validate the resulting premium calculation against your total deposits for the same period (taking into account your receivables).

- Take advantage of the resources that are available to you. Know the typical schemes that are perpetrated against small business owners. You can get information from the Small Business Administration (SBA), National Federation of Independent Business (NFIB) and any number of other organizations.

Here are links to a few good articles on preventing employee theft and fraud.

www.allbusiness.com/articles/EmploymentHR/3935-33-1817.html
www.sba.gov/gopher/Business-Developement/Success-Series/Vol6/theft.txt
www.nfib.com/object/3511306.html

Remember, while this is a real risk, you cannot run your business with a paranoid fear of the unlikely. There is no substitute for appropriate supervision and surrounding yourself with trustworthy people.

Take these steps to avoid all types of disasters and remember, you can always delegate tasks, but you cannot delegate responsibility. Take responsibility for the success of your business.