CPA
Practice Advisor

BACKUP & SECURITY

A 12-point Checklist for Disaster Recovery Planning

Scott Cytron • Aug. 15, 2011

By the time you read this, I will have delivered a new presentation, "Crisis Communications: What Would You Do if BP Happened to You?" for the Kansas Society of CPAs. I was fortunate to be invited to speak during the KSCPA's Business & Industry Expo in August to an audience of tax and accounting professionals who work in business and industry.

While this is a departure from my usual presentations to public practitioners, I thought the topic was definitely applicable to both audiences. So here are my observations *any* tax and accounting professional can apply, whether working in public practice, business or industry, as well as with a firm's small business clients.

What is your role when a crisis occurs?

Many practitioners feel they are immune to being involved in crisis and disaster planning, but think again. Tax and accounting professionals have the right mix of competencies and skills that would be very helpful in case a disaster occurs – from the way they analyze numbers and plan for the future to their extensive knowledge of the company's history, goals, technology and systems. When clients are going through a crisis, they *should* turn to their accountant for help. In fact, I have found that many accountants readily offer their clients proactive business continuity and disaster planning services, which, of course, is much more useful than having to put the pieces together after disaster has struck.

A crisis can occur anytime, anywhere, and it can strike in a variety of ways. This includes natural disasters such as hurricanes, floods or tornadoes; man-made disasters such as arson; intentional disasters (terrorism); and vital mistakes made by a CEO or senior leadership. Disasters also include white collar crimes. In fact, according to the Institute for Crisis Management's 2010 ACM Crisis Report, white collar crime made up 20% of the overall total for crises that occurred last year. That's a huge number, but it's even more encompassing when you think that when hackers steal private data, a company could, literally, be forced to shut down overnight.

Here is a 12-point checklist you can use to help clients, customers and companies with the disaster planning function. Although I didn't invent this list (source: cgsolutions.biz), I did add and update some items based on my experience, including some of the more modern technologies we have at our fingertips.

1. **Define mission-critical company functions and establish a hierarchy of operational importance.** As a tax and accounting professional, you can prepare the company to implement the orderly re-establishment of critical operations that

will help reduce the impact of business interruption on cash flow. This affects virtually all areas: CEO, MIS, accounting, production, marketing and sales.

2. **List mission-critical personnel and their job functions.** You can guide managers and department heads to determine which personnel function must be re-established immediately, which ones could be phased in over time, and which ones could be excluded in a crisis.
3. **List equipment needs of critical personnel.** This is where you document a complete inventory of computers and accessories, telecom equipment, office equipment and furniture. Keep in mind that it may be necessary to acquire this information from the company's vendors or other providers.
4. **Determine a site relocation for contingency.** You need to determine the amount of space required for emergency relocation, and identify a means of securing short-term space for emergency relocation. You may have to enlist the resources of commercial real estate companies.
5. **Establish a recovery event task list.** This is where you would create a chronological task recovery list, where each recovery step would be assigned to specific company personnel.
6. **Document current computer data backup methods and frequencies.** Of course, you should always be advising your clients to have backup procedures in place. For example, if a disaster occurred today, the client should be prepared to rely on a redundant backup. In this step, you would also identify any data loss vulnerabilities, including intermittent backup procedures, lack of off-site backup (including cloud-based storage), and failure to test and restore the backup.
7. **Identify hard copy documents vital to the company that cannot currently be re-created electronically.** While just about everything can be electronic or paperless, we all must live with *some* paper. In a company, this includes files, contracts and financial data. You can also develop corrective procedures to eliminate potential loss of documents, and, of course, consider paperless solutions, including scanning and cloud-based storage.
8. **Identify mission-critical items vital to company operations that would be required in the event of a disaster emergency.** This is where you create a reference list of appropriate items for off-site storage, including copies of insurance policies, contracts, letterhead, business checks, employee emergency contact numbers, and client and provider lists.
9. **Form an internal emergency response or crisis committee with employees assigned to specific crisis functions.** Members assist in creating the disaster recovery plan and are responsible for specific functions. The size of the committee is up to the company and its needs.

10. **Create a crisis management media kit.** You'll want to be prepared for any media or press coverage, providing samples of communications to be sent in an emergency. You would include spokesperson info, news releases, and letters to employees, clients and providers.
11. **Create a systematic schedule for updating the plan; an outdated plan is worthless!** The disaster recovery plan should be reviewed and updated semi-annually.
12. **Measure and evaluate — test the plan!** My clients probably get tired of hearing me talk about this, but you must measure and evaluate what you're doing in order to improve. If a disaster were to occur, you should create an evaluation checklist, asking, "How did we do?" You can also stage a mock disaster and evaluate how the company did.

If you think you're too busy to actually go through these steps in your own firm, then you're doing yourself a real injustice. Not only will you not be prepared should something happen; you are short-changing your co-workers and affecting the fate of your company.

You can make this task a little easier on yourself by delegating some of the responsibility or actions, and even doing a bit at a time. Naturally, fate might get in the way. If something happens, let's hope you're prepared for the worst scenario possible.

Backup & Security • Disaster Recovery • Product & Service Guide • Technology • Article

CPAPA is registered with the National Association of State Boards of Accountancy (NASBA) as a sponsor of continuing professional education on the National Registry of CPE Sponsors.