

Hello. It looks like you're using an ad blocker that may prevent our website from working properly. To receive the best experience possible, please make sure any blockers are switched off and refresh the page.

If you have any questions or need help you can email us

From the Sept. 2007 Issue

Firms rely on information technology to manage every part of their practice, making them more effective and efficient. Unfortunately, many firms take their technology and business systems for granted and don't really appreciate how much they rely on them until something breaks or services become unavailable. The incidences that can impact firm productivity range from a corrupted or accidentally overwritten file to the loss of an entire office due to fire, flood or other weather damage. How you respond to these types of situations determines your firm's survivability and should be an integral part of your firm's overall strategic planning, which should be reviewed and updated annually. To more easily frame the discussion that all firm owners should have on incidence response, we discuss four scenarios to consider: Basic Restoration, Immediate Response, Disaster Recovery, and Business Continuity.

Basic Restoration

This aspect deals with the ability for your firm to quickly restore a file that has been lost or damaged or to restore services to keep your individuals working. This is usually handled by a member of the IT team or an administrative individual assigned to oversee the role. At the simplest level, it is having documented instructions so that any person in your firm who has authorization can easily search and restore a file from an archival solution. While most firms have a tape backup system, the instructions to restore files can sometimes be confusing, so IT support is required, which can delay the response. Firms are finding that by backing the entire server contents to a network attached storage device, they can not only keep full daily backups available in the same network directories that their people are used to working with, but that they can run their tape backups from these storage drives to minimize the impact of network backups on the rest of the firm during this time. The

cost of these drives has come down significantly, so some firms are keeping multiple

Hello. It looks like you're using an ad blocker that may prevent our website from working properly. To receive the best experience possible, please make sure any blockers are switched off and refresh the page.

If you have any questions or need help you can email us

equipment on the shelf and ready to go is minimal.

Immediate Response

The second level of response is when an incident escalates to the point where there is risk of loss to personnel or to the firm's information resources. We've seen many stories in the news about weather damage, fires and theft of equipment, but there is also the issue of building inaccessibility due to gas leaks or other unexpected activities. Rather than to try to develop a detailed plan that will respond to every possible event, we feel that firms are better served by having an immediate response document that assembles the appropriate personnel, evaluates the situation and determines the firm's immediate response. The immediate response document should be written by your IT team, which should consist of an owner, IT support personnel and representatives of each department. It should designate a primary and secondary person with responsibility and how to notify them when a situation occurs. These people are responsible for assessing the situation, determining a course of action, securing firm resources and initiating Disaster Recovery if necessary. The immediate response document should also include the process to initiate firm communications and account for all personnel if necessary. This would include each employee's contact information and a location to meet in the event that the firm's office is inaccessible. This document would also include contact information for your external IT support services and emergency services. Prior to developing the firm's disaster recovery plan, we recommend that they have an immediate response document created, copied and stored offsite, and that personnel are educated on the reasons for the document and the expected response.

Disaster Recovery

With the immediate response document in place, we feel that firms should then begin the process of developing a disaster recovery plan that would outline the firm

response in the event of a loss of the firm's network infrastructure. A number of

Hello. It looks like you're using an ad blocker that may prevent our website from working properly. To receive the best experience possible, please make sure any blockers are switched off and refresh the page.

If you have any questions or need help you can email us

Business Continuity

While the Disaster Recovery document discusses how to rebuild your information systems, the business continuity plan outlines how your firm will function during and after a disaster. This will detail information on the firm's insurance policies for recovery and include life, disability and benefits, such as how employees will be paid and receive benefits during this time. This portion can be developed in conjunction with your insurance company and should also include information resources from the Internet such as the American Red Cross, which has information on family preparedness.

Firm owners should meet at least annually to discuss the four types of incidence response with their personnel and update their documents. While there is no way to account for every situation, having a planned response will give confidence to your firm and ensure its survival.

Technology

CPA Practice Advisor 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.

© 2024 Firmworks, LLC. All rights reserved