Business Continuity and Disaster Recovery Planning

By Lisa Traina, Partner

Disaster recovery, particularly the backup of financial systems and data, has been an area addressed in IT controls in financial audits for many years. Recent hurricanes with historic flooding have been a reminder of the critical need for appropriate planning to allow for access to systems during natural disasters. Social threats and the ever-increasing number of cyber breaches, attacks, and vulnerabilities should have equal consideration as a reinforcing concern. One ransomware attack on an NFP that does not have appropriate backups and an incident response plan can cripple the organization's ability to produce reliable financial statements.

There are many areas pertaining to disaster recovery that should be addressed, and the list of considerations is much broader than whether the organization has a current backup and whether backups are taken offsite. The following discussion of comprehensive business continuity and disaster recovery planning should help NFPs and their auditors familiarize themselves with the planning process and the content of sufficient plans. In-depth reviews of disaster plans by IT professionals often identify weaknesses in many of the areas mentioned. Although auditors may try to limit their perspective to the financial data only, a broader perspective is helpful and relevant in understanding the entity's ability to continue operations and fulfil its mission. The accounting system is often intertwined with many systems, so the entity-wide process should be understood.

The Planning Process and Business Impact Analysis

Business continuity and disaster recovery planning are no longer the focus of the IT department alone. As more functions shift to the cloud and other electronic storage mediums, it is becoming ever more crucial for organizations to consider and regularly test plans to access this information during an unplanned outage.

Developing a formal business continuity and disaster recovery plan is an important first step in contingency planning. A strong plan stems from a thorough business impact analysis (BIA). A BIA identifies and evaluates the possible effects of an interruption or complete outage to critical operations as the result of a disaster, accident, or emergency. From there, the NFP can begin to gather and document the information and resources needed to recover from the identified events.

Although predicting and planning for every possible scenario isn't feasible, there are high-risk, high-probability topics that make good starting points. These can include loss of internet (including cloud computing), primary servers, or connection with key service providers; an extended outage of key service providers; and power issues. Plans should document formal steps to be followed during natural disasters specific to the geographical area, such as hurricanes, tornadoes, earthquakes, floods, fires, and so on. Man-made scenarios also should be considered, including pandemics and terror events. Plans should document concise, easy-to-follow steps and procedures in the event of each considered outage or event.

Business Continuity and Disaster Plan Components

Once planning for foreseeable general risks has been completed, the next step is to establish more specific procedures for all functional areas. Each functional area should include responsibilities, the responsible party, and procedures to be followed both during and after an emergency.

Examples of functional areas beyond the primary operation and mission of the NFP include accounting and finance, human resources, facilities, IT, administration, and remote operations. Interim processing and recovery procedures for all locations, critical functional areas, and IT systems and infrastructure should be documented as

Business continuity and disaster recovery planning are no longer the focus of the IT department alone.

part of the plan. These procedures may include restoration for virtual and physical servers (including server-specific applications), alternate internet service providers and firewall and intrusion detection systems, primary network infrastructure, and external data transfers. Data transfers are often key components of financial reporting; for example, donor systems may provide an import file for the accounting system.

Other key elements of a comprehensive plan include an employee contact list, accurate and current assignment of action to be taken in an emergency, procedures for document storage, procedures for accessing an area that has been declared a disaster zone, and storage of the plan in multiple locations in case the primary location becomes inaccessible.

Data Backups

A current and comprehensive plan is a key element of contingency preparedness, but without a detailed back-up configuration, operations can come to a standstill during a disaster event. The back-up process should be sufficient to preserve data in the event of a disaster. This requires a comprehensive inventory of the systems to be backed up, including both onsite and cloud systems.

Cloud vendors perform their own backups, but organizations should consider maintaining their own backup of information stored in the cloud. Although it may not be possible to create a "full backup" for a cloud system (for example, QuickBooks Online) that could be restored in the traditional sense, periodic exports or reports should be generated to ensure there is a complete record of all data. The frequency of server backups or cloud reports and exports should be determined based on the critical nature of the system.

Back-up media should be encrypted and stored off-site. Storing back-up media at the same location or in proximity to live systems increases the risk of losing data in the event the primary location is destroyed or physical access is temporarily restricted. For this reason, backups should be farther away than a building next door or a few blocks down the street.

Adequate retention and rotation policies and procedures should also be considered. Retaining periodic backups, whether online or on offline media, is an essential step to ensure all data are available. It is common practice to retain backups at month-end and year-end. This is needed in addition to daily backups to ensure the data can be restored in the event of a dormant virus or similar issue.

Replication is another great control to ensure the immediate availability of data; however, one common issue is that replicated data is only retained off-site for 24 hours and it is overwritten. Organizations should have additional copies of replicated data to protect against corrupted replication. For example, if ransomware infects a system, it could be replicated to the online backup. A good rule of thumb is the "Rule of Three," which says data should always be in three places at once:

1. With the vendor or on an onsite system
2. At the vendor's hot site, a replicated backup or copy onsite
3. At an additional location (that is, the organization maintains a copy or keeps a backup at another location)

In the case of a cloud vendor, the third copy may be in the form of exports.

Plan Testing

Adequate and frequent plan testing and employee training are critical components of disaster planning. Employees should receive annual training to ensure they are familiar with their responsibilities and the procedures to follow in the event of an emergency or disaster. Training should cover all key areas, such as succession plans, alternate locations, expectations for employee reporting in an emergency, details regarding employee communication options and availability of contact information, re-entry requirements, critical functional areas, and emergency team assignments. The size of the NFP will dictate the level of training that may be needed. As a best practice, thorough plan testing should be performed annually, at a minimum.

Many organizations are surprised to find they don't have reliable backups when the situation requires a data restore. This is becoming more frequent as the occurrences of ransomware attacks increase. It is vital to test the ability to restore not just a single file, but entire systems. In addition to back-up restoration, all plan procedures should be tested at least in a table-top manner (for example, processing payroll without access to the primary system or communicating with key stakeholders, as may be necessary in an emergency).

Summary

The business continuity and disaster recovery environment is changing every day and new considerations arise frequently. It is critical for NFPs to establish baseline plans, back-up configurations, and training and testing processes to ensure ongoing operations. Auditors who understand the importance of comprehensive planning; the changing environment with new cyber, social, and environmental threats; and the intricacies involved will be more successful at identifying areas of risk.

This document originally appeared in the AICPA's *Not-for-Profit Entities Industry Developments—2018*

About the Author

Lisa Traina, Partner
CapinTech
ltraina@capincrouse.com
o 505.50.CAPIN ext. 2000

Lisa uses her more than 30 years of experience to assist organizations in implementing measures to secure data and manage risks efficiently and effectively. She is a nationally recognized speaker and author, and serves on the AICPA Cybersecurity Task Force. Lisa founded Traina & Associates in 1999 to provide IS security services to a broad range of industries. Traina & Associates joined CapinCrouse in January 2017 and is now CapinTech.

About CapinTech

CapinTech, a CapinCrouse company, provides information security services, including cybersecurity assessments, consulting, and training services, to nonprofit organizations, financial institutions, medical entities, professional services firms, and other organizations. Each year the firm performs hundreds of assessments, consulting, and speaking engagements with a team of experienced professionals retaining numerous certifications, including CPA, CISSP, CISM, CISA, CITP, CGMA, and CTGA. Each engagement is tailored to fit the unique needs of the organization, and information and reports are presented in a clear, concise manner intended for an audience with varying information systems (IS) knowledge. More information is available at capintech.com.

About CapinCrouse

As a national full-service CPA and consulting firm devoted to serving nonprofit organizations, CapinCrouse provides professional solutions to organizations whose outcomes are measured in lives changed. Since 1972, the firm has served domestic and international outreach organizations, universities and seminaries, foundations, media ministries, rescue missions, relief and development organizations, churches and denominations, and many others by providing support in the key areas of financial integrity and security. With a network of offices across the nation, CapinCrouse has the resources of a large firm and the personal touch of a local firm. Learn more at capincrouse.com.

CapinCrouse is an independent member of the BDO Alliance USA.