What would happen to your organization if one of your vendors could not fulfill their obligations due to a disaster? Can you trust that your vendors are prepared to continue operations if an unplanned disruptive event occurs?

For today’s nonprofits, the impact of an event that adversely impacts operations can be devastating. The impact is magnified exponentially if the vendor is responsible for the nonprofit organization’s response management services (including payment processing, contact center, and fulfillment) and is inadequately prepared to mitigate the risk associated with business disruptions. Whether the event is accidental, deliberately caused, or the result of a natural disaster — like a fire, flood, or hurricane — having an actionable plan to resume operations after a crisis is critical.

In order for nonprofits to effectively reduce the risks and consequences of service interruptions, they must require their vendors to have a well-defined business continuity and disaster recovery plan (BC/DR) in place. The plan must be comprehensive and cover all the necessary steps for rapid recovery, from identifying effective mitigation strategies, to defining a detailed action plan for resuming daily operations and functions, as well as how to communicate these processes to donors and other constituents.
Introduction

By definition, the purpose of a business continuity and disaster recovery plan is to help organizations resume business operations, including technology and support services, in a timely and organized manner after a disruptive event. In practice however, most response management vendors do not have an adequate or effective BC/DR strategy in place, if they have one at all. As a result, they cannot effectively continue or resume services in a timely manner, which may cause significant damage to the financial health and reputation of the organizations they serve.

According to Gartner, Inc., an information technology research and advisory firm, only 35 percent of small and medium enterprises (SMBs) have a comprehensive BC/DR plan in place. In many cases, if direct response processing vendors fail to implement a comprehensive backup and restore strategy for their information technology (IT) infrastructure, their BC/DR plans may be rendered ineffective. According to Gartner, Inc., an IT research and advisory firm, only 35 percent of small and medium enterprises (SMBs) have a comprehensive BC/DR plan in place. As more and more organizations and nonprofits continue to rely on outsourcing their response management solutions to run high-performance process controls and improve productivity, any downtime experienced by a vendor after a disruptive event can adversely impact the organization and its donors.

Many nonprofits outsource their donation processing and fulfillment operations and have limited staff resources for developing their own comprehensive disaster recovery plans. Therefore, nonprofits need to ensure that their donor response management partner and other key service providers involved in the revenue flow of an organization have a comprehensive BC/DR plan in place.

In order to be well prepared to select the right vendor, organizations need to have insight into the vendor’s BC/DR strategy, including their business impact analysis (BIA) and business continuity playbook. The BIA and business continuity playbook should be thorough in scope, and outline the necessary steps for resuming business operations, including physical, IT and human resources.

The BIA identifies which of the vendor’s systems and processes are most crucial, and then assigns each a specific priority. It also analyzes the effect an outage would have on the organization, and the recovery time objective for the entire IT and production infrastructure. The BIA will help a response management vendor set a restoration sequence by determining which parts of the organization should be restored first and how. For instance, vendors should prioritize the rapid recovery of systems that allow critical functions to continue within the nonprofit, such as the depositing of funds and capturing of donor data.

Ensuring that caging and data capture vendors have a strong DR/BC plan is especially critical for nonprofit organizations that receive a significant amount of revenue from direct mail fundraising. Based on a survey of our nonprofit clients, Merkle Response handles between 30 and 60 percent of the revenue received by those organizations, making the ability to continue making deposits and capturing data especially critical.

While the BIA presents foundational recovery and mitigation strategies, it is the business continuity playbook that provides the framework and checklists to manage and execute all facets of a BC/DR plan. A business continuity playbook provides a detailed action plan for resuming donor care operations and functions, as well as communications infrastructure and support operations quickly and effectively after a disaster event.
Regardless of its complexity, a robust playbook must include a detailed communications strategy for notifying the nonprofit and its donors after a disaster. It must include the appropriate responses planned for different disaster scenarios, best practices for securing the communications infrastructure and data backup, as well as a crisis communications plan with documented procedures for notifying customers, suppliers and employees of an incident, their response, and how to communicate necessary information to all constituents. For vendors, a smart, well thought out playbook can mean the difference between continuing to serve nonprofits and their donors, and passing on the disruption, disorganization, and obstacles of a catastrophe.

Make Sure Your Vendors Build their BC/DR Plans on These Four Fundamentals

All direct response processing companies should have an organization-specific BC/DR plan for responding to a disaster event. It should be an important requirement in the vendor selection process, just like ensuring that a vendor complies with the payment card industry (PCI) data security standards to address the security, integrity, and privacy of cardholder data. Although disaster preparedness is a smart precaution, it is not a requirement unless your organization insists that it be treated as one.

When considering vendors, look for those whose BC/DR plan contain these four essential components:

1. Communicating with Personnel
2. Establishing an Alternate Workspace/Facility
3. Protecting Data Files and Paper Documents
4. Managing Risk

1. Communicating with Personnel

Employee communication is key. The BC/DR plan should include a review of personnel files to be sure that all contact information is current and includes numbers for police, fire and other emergency responders. An employee phone tree, in the form of a printed card, can be created to identify designated employees who are responsible for calling other team members in the case of an emergency. It’s also important to test the numbers to make sure they actually work before a crisis hits. Using alternative means of contact, such as social media can be considered, but the cellular and other data networks these communications rely on for transmission are often unreliable during an emergency when the power grid is disabled.

2. Establishing an Alternate Workspace/Facility

What would your response management vendor do if its building or production facilities were inaccessible tomorrow? Would it continue to provide the products or services your nonprofit organization needs to deliver critical business functions from an alternate site? How long would it be before it could resume production, or restore IT services? If a response management vendor does not have an alternate BC/DR facility in a separate location, a physical or environmental disaster would make implementing its continuity plans impossible. Since a crisis may last anywhere from a few hours to a few weeks, or even months, it’s critical that any BC/DR plan designate an alternative facility. Ideally, it should be located far enough away so that it’s not affected by the disaster, but not so far away that employees have difficulty getting to it. The alternate site should be close enough to move to and start production with minimal downtime, but far enough away to pull power from a different grid not affected by the disaster. Additionally, it must have adequate capacity, integrated communications capabilities and be safe and secure. If a vendor claims to have a secondary facility, it’s also beneficial to request a site visit or pictures of a physical layout, as well as detailed information regarding how its personnel plan to operate at that location in an emergency.
3. Protecting Data Files and Paper Documents

Without access to files containing donor data, program details, and other information used on a daily basis, nonprofits would be immobilized. All desktop computers and server-based data must be backed up, preferably at the end of every business day. Migrating data to the Cloud offers nonprofits a cost-effective way to do this, as well as the ability to access the data from a remote location — eliminating the need for creating back-up files and storing them away from the central location. Using Cloud storage brings other risks, however, and cyber insurance may need to be obtained to cover the risks associated with storing data this way. Even with the popular push to move to paperless, most nonprofits still have a large number of paper files, contracts, insurance documents, donor information, correspondence, employee records, manuals, and more. These documents should, at a minimum, be stored in a safe, or other water/fire proof receptacle.

4. Managing Risk

Assess the level of risk by reviewing the physical office, establishing building safety procedures and putting processes in place to avoid risk. Once that’s done, an insurance audit should be performed to make sure there is adequate coverage. Are workers covered by worker’s compensation? Is the cost to repair or replace office equipment known? Is it insured to the full amount? Taking these precautions is an important part of the plan.

Maintain the Communication Ecosystem for Quick Recovery

At its heart, BC/DR planning is about continued communication. Customers need to know when and how a response management vendor will continue operations in the event of a disaster, and accurate information will help them understand the impact of service interruptions. As such, vendors with an effective BC/DR plan will not only address communications among employees, but also between the vendor and the nonprofit’s constituents.

Organizations should verify that they have agreements in place stipulating the notification of the impact a vendor disruption will have on their business. The agreements should address how the vendor will alert an organization of a disruption, and communicate the necessary measures for resuming caging, data capture, contact management and fulfillment operations. Whichever methods are used during an unplanned disruptive event, whether they be e-mails, individual calls, or even social media, it’s important that nonprofit clients clearly communicate their contact preference and employees adhere to the agreed upon protocols. Disaster communication should be both flexible and effective enough to reach across the entire system of organizations, people and activities critical to operations.

IT systems aside, the most unpredictable elements in any contingency planning exercise are people. A response management vendor’s ability to restore operations is dependent on its workforce, so crisis communication plans must have options in place that address the relocation of employees after an event. Specifically, a plan should include the following:

• Transportation to and from the secondary facility;
• Information on lodging; and
• Roles and responsibilities for donor engagement
Practice Makes Perfect. Has Your Vendor Tested Its BC/DR Plan?

Best Practices of Documenting a BC/DR Plan

The old adage, 'practice makes perfect' is truer than ever. Often, organizations write strong strategic plans but fail to put them into practice effectively. **Having a BC/DR plan in place does not guarantee that the plan can be executed,** or that downtime will be minimized in the event of a disaster. The key is to test the plan repeatedly by setting up and prioritizing a series of exercises that address the entire spectrum of operational activities and the complexity of navigating a disaster environment. An effective BC/DR plan should be tested at least every six months.

A well-tested BC/DR plan shows that the vendor is keeping a plan that's up-to-date and is aware of how well the plan can be executed during an event, setting a high bar for the delivery of services. For an organization, these walkthroughs result in fewer flaws in a vendor’s BC/DR plan, even under the most unpredictable conditions — enabling them to maintain the professionalism, stability and transparency of their operational plans if the worst should happen.

Conclusion

Disasters and disruptions can be defining moments. Even if your nonprofit was not directly affected by an event like Hurricane Katrina, Super Storm Sandy, or September 11th, the fear and chaos that ensue are excellent reminders that we live in an unpredictable world, and that anything can happen at any time. Recognizing this, it is foolhardy and even dangerous to assume that a vendor will be able to fulfill its obligations during an unplanned disruptive event without a game plan. Thus, it’s essential to make sure each vendor has a comprehensive BC/DR strategy and plan in place, and it’s equally crucial that the strategy be communicated to the organization, tested frequently, and updated regularly.

Determine whether or not your vendor has evaluated their disaster readiness by asking these questions:

- How frequently are their BC/DR plans tested?
- When was the last time the BC/DR was tested?
- Who was involved in the BC/DR plan test?
- What constitutes a successful test?
- Are test results documented and available for review?
About Merkle Response Management Group

For Merkle Response, supporting your mission is our mission, and we measure our success by how well we help you achieve yours. Merkle Response Management Group is one of the nation’s largest full-service direct response processing and fulfillment companies. Merkle has served the response management needs of nonprofit, government and for-profit organizations since 1983, and has earned its reputation for excellence by combining experience in customer verticals with rigorous quality and security controls, the latest technology, extensive business continuity and disaster recovery planning, and a passion for delivering superior customer service. This “High-tech, High-touch” approach helps us custom-fit our solutions to your specific needs, because every mission is different, every stakeholder matters, and every budget is limited.

---

1 Gartner, Inc.  http://iosafe.com/industry-stats
2 Disaster Planning and Business Continuity for Nonprofit Organizations: Preparing for Disruption, Ron Matan, CPA, and Bridget Hartnett, CPA, 2010

Join in the Conversation

linkedin.com/Merkle Response Management Group
facebook.com/Merkle Response Management
@MerkleRMG

Merkle Response Management Group
100 Jamison Court
Hagerstown, MD 21740
301-790-3100
www.merkleresponse.com