AN INFORMATION TECHNOLOGY DISASTER RECOVERY PLAN – WHY YOUR SERVICE ORGANIZATION NEEDS ONE

DiSanto Priest & Co.
Certified Public Accountants

Businesses increasingly rely on networks of subservice organizations to support key operations and to help them provide services to their customers. Unfortunately, the climate of today's cyberspace is volatile with cyberattacks creating headlines daily, therefore, an increased focus is placed on the need for comprehensive risk assessments and adequate subservice organization monitoring. According to the 2018 State of Cybersecurity in Small and Medium-Sized Businesses research report presented by the Ponemon Institute, 67% of respondents[1] reported that their company had experienced a cyber-attack in the past 12 months. Compared to the 2017 version of the same report, 2018 showed a 6% increase in cyber-attacks over the previous year.

Companies are taking proactive measures to combat this rise in cyber-attacks and minimize risks. As a result, more and more companies are obtaining System and Organization Controls (SOC) analyses to provide their clients with the assurance that there is a plan in place, that is tested regularly, to ensure that when disaster strikes, the subservice organization recovers in a manner that is timely and in line with their customer's needs and expectations.

Time is money and the cost of company downtime is significant, especially when dealing with a security risk. While customers will be sympathetic at first when disaster strikes, they will likely be unwilling to wait for long periods of time before beginning to look at how competitors could better meet their needs. Keeping company downtime to a minimum is key to running a successful service organization, which is why having a Disaster Recovery Plan (DRP) is so critical to business continuity.

When disaster strikes, a service organization needs to be able to respond quickly and get the business back up and running. Having a thorough, written plan that outlines, in detail, the steps that need to be taken to accomplish this will prove to be invaluable in times of crisis.

[1] 1,045 individuals from companies in the United States and the United Kingdom with headcounts ranging from less than 100 to 1,000

If you don't have a Disaster Recovery Plan drafted yet for your service organization, the time to begin developing one is now. There are many websites that provide Disaster Recovery Plan templates such as **disasterrecoveryplantemplate.org**. You should also consider utilizing an Information Technology (IT) consultant with experience in developing DRPs.

DRPs can be very basic, but they can also be quite comprehensive. There are many factors that determine how comprehensive the DRP will be, including company size, human resources available and budget. Service organizations should perform a cost-benefit analysis to determine how extensive their DRP needs to be to meet their business and their customers' needs.

To develop a DRP, it is important to have the support of upper management. The tone at the top will be important in stressing the importance of the DRP. To begin developing an effective DRP, a team of key employees (which should include members of senior management and IT staff) should collaborate, brainstorm, and perform a risk assessment to determine the types of risks and disasters that are most likely to occur and impact daily business continuity. A thorough DRP does not just cover one type of disaster that could occur, it should be all encompassing of the disaster scenarios with the highest probability to impact your service organization and it should outline a specific recovery plan for each of those scenarios. For example, responding to a hurricane disaster where the physical office could be impacted by flooding, wind damage and power failure would be very different than responding to a cyber-attack.

When a disaster occurs, the DRP should clearly identify the individual or individuals who have the authority to activate the DRP. The names and contact information of each critical individual or vendor that is responsible for executing the various aspects of the DRP should be included. In case someone cannot be reached in an emergency, a backup individual and their contact information should also be listed in the DRP. Since an emergency could occur at any time, and time is of the essence, it is very important to keep the contact information for key parties up-to-date at all times. Clear and consistent communication coupled with timely training of key employees who will be executing the DRP is also extremely important.

There is no one DRP that will work for all businesses. Each DRP is unique to a business and its their specific set of circumstances. Below is a list of some items that should be considered for inclusion when developing a DRP:

- Purpose and goals of the DRP.
- A diagram of the entire IT network.
- Updated inventory listing of all critical IT assets (hardware and software).
- A description of what measures are in place to prevent certain disasters from occurring, such as the use of generators and surge protectors.
- A description of the service organization's current efforts to detect possible issues before a disaster occurs such as antivirus technologies, network monitoring tools and regular employee training.
- Likely disaster scenarios and plans for an orderly recovery for each scenario.
- A defined recovery time objective or the maximum amount of time allowed between the disaster taking place and when normal operations and service levels are resumed. This will vary from business to business depending upon what each business (and its customers) is willing to accept.

- Where backups can be found.
- Comprehensive off-site data backup procedures including the procedures for the testing of backups.
- The frequency at which backups are performed. Data should be backed up with enough frequency that any potential data loss is not deemed unacceptable to the service organization and its customers. If no more than 4 hours of data loss is acceptable for a particular application, then backups should be done for that application at least every 4 hours.
- A clear list of the recovery priorities (most critical business continuity systems that need to be up and running first).
- A list of software and systems that will be used to recover from the disaster and any useful/helpful information related to each.
- Name and contact information for those who will be tasked with implementing and executing the DRP. Be specific in terms of who is responsible for each identified task. Backup personnel should also be clearly identified just in case the individual in the first position to respond is unable to do so.
- A list of any vendors that will be used in the disaster recovery efforts and how to get in contact with them.
- Contact information for law enforcement, first responders, property managers and other critical parties should be included.
- A description of how communication with employees will occur.
- A description of how communication with customers will occur.
- Possible relocation site if work cannot be conducted in the normal business location and directions on how to get to the relocation site. Careful consideration should be given to the location of the alternate site because selecting a location that would also be impacted by the disaster would not be favorable.

- Document history including dates of the DRP revision, what was revised and by whom.

While having a DRP is a great first step, putting it to the test in a simulated environment is even more important. A company should ensure that its DRP will work as intended when needed. Having a test fail is not a bad thing because it reveals issues that can be corrected ahead of a real disaster. Testing is also beneficial to those who will be tasked with implementing and executing the DRP. The more comfortable they are with executing the DRP, the smoother things will go in an actual emergency. The frequency of testing will vary based on the needs of the service organization but should occur at least twice per year.

Once developed, written and tested, the DRP itself should be reviewed and approved by key members of upper management. Any feedback from upper management should be incorporated into the DRP as deemed necessary.

A DRP is a living document. It can't just be developed and filed away. Having an outdated DRP can be as detrimental as not having one at all. The world is constantly changing, therefore, the DRP needs to be updated by key employees within a service organization at least annually. Risk assessments should take place at least annually to consider new vulnerabilities that could impact a service organization. Perhaps there are new IT tools that can be used to further reduce downtime or make the service organization less vulnerable to disasters. These and other factors should be considered when updating a DRP. When changes are made to the DRP, they should be tested, then staff should be notified of the changes and training materials should be updated.

All employees should know where to locate the DRP and have a copy available to them at all times. In the event of a disaster, employees need to clearly understand their roles and responsibilities and they need to know who needs to be contacted so that incident response can begin. A copy of the DRP should be kept in a location off-site in case it needs to be accessed in the event of a disaster. It is recommended that key employees who will play a role in the execution of the DRP in the event of a disaster be given a hard copy of the most recent DRP as well as an electronic copy to be filed away in their homes or some other off-site location.

In a competitive business environment, your service organization simply can't afford significant downtime and data loss which can cause loss of revenue, loss of customers and significant expense to your organization. If you have an updated and tested DRP in place, you will be better prepared for the unexpected. While all disasters can't be avoided, their impacts can be minimized with a proper DRP.

About Disanto, Priest & Co.
Disanto, Priest & Co. is a full service public accounting firm headquartered in Warwick, Rhode Island with expertise in assisting companies in evaluating their current and planned third party assurance needs, like those described above. Give us a call if you need assistance as we would be glad to talk with you about your needs.

Headquarters
117 Metro Center Boulevard
Suite 3000
Warwick, Rhode Island 02886
Telephone 401.921.2000
Facsimile 401.921.2010
www.disantopriest.com