NATIONAL ASSOCIATION OF
ELECTRICAL DISTRIBUTORS

Executive Guide # 8:

IT Disaster Recovery Planning

Developed by the NAED Strategic Technology Taskforce

Published April 2013

IT Disaster Recovery (DR) is a subset of business continuity planning, focused on the technology systems supporting business functions—*including phones, email, websites, servers, ERP systems, etc.* It outlines the steps IT personnel must take to resume Information Technology operations in order of priority in the event of an IT service interruption.[1]

Possible Disaster Scenarios

Natural and man-made disasters can occur anytime, anywhere, cutting businesses of all sizes off from their usual IT services. While some geographical locations are more susceptible to certain natural disasters than others, no business is immune from severe weather. Regardless of the disaster scenario, IT disruptions and telecom outages are likely to occur. Furthermore, a business is impacted twice by a disaster—*during the event itself and in the chaos that usually follows.*

Natural Disasters

Adverse Weather
- Blizzards
- Dust & Wind Storms
- Hurricanes
- Ice Storms
- Tornadoes

Avalanches

Earthquakes

Floods

Landslides

Tsunamis

Volcano Eruptions

Wildfires

Man-Made Disasters

Blackouts

Civil Disturbance & Riots

Cyber Attacks & Security Incidents

Electronic Incursions & Data Breaches

Equipment Failure
- Hard Drives & Servers
- Burst Pipes & Plumbing/Sewage Backup
- Sprinkler System

Fire

Hostage Situations & Random Acts of Violence

Industrial Accidents & HazMat Situations

Plane Crashes

Roof Leaks

Sabotage, Terrorism, Vandalism & War

Utility Infrastructure Failures & Outages
- Electricity, Gas, Water
- Internet & VPN Connectivity
- Telephone Service (cell, land, VOIP)

Electrical distributors are more likely to experience flooding as a result of burst pipes, clogged toilets, sewage back-ups, sprinkler system failures, or even water damage from a nearby fire rather than an overflowing river. Branch offices may have to be evacuated due to accidental releases of hazardous materials, bomb threats, fires, hostage situations, random acts of violence, or terrorist attacks. Data loss from electronic intrusions, security incidents, and IT equipment failure—*including hard drives and servers*—is almost guaranteed.

Is your information technology department prepared for the inevitable?

[1] For information on business continuity planning, visit www.naed.org/disasterplan/

Why IT Disaster Recovery Planning is Important to Electrical Distribution

Developing an IT disaster recovery plan is the first step in ensuring business continuity. In the era of Internet dependent services, IT disaster recovery planning can enhance your company's competitiveness in the marketplace, improve business processes, standardize the use of technology company-wide, increase "uptime" for critical IT equipment, and develop new technical expertise within your organization.

What will you do if your information technology systems stop working? Consider these statistics:

1. The survival rate of companies without an IT disaster recovery plan is less than 10%.
2. 97% of data loss is not caused by a natural disaster.
3. Every week 140,000 hard drives crash in the United States.
4. The average cost of company downtime due to data loss is $84,000 - $90,000 per hour.
5. Only 6% of companies suffering from a catastrophic data loss survive, 43% never reopen, and 51% close within two years.

Things to Consider When Developing Your IT Disaster Plan

Communicating information is central to every electrical distributor's operations. Your IT disaster recovery plan must spell out the actions to be taken to protect your business, communicate with employees, and continue to service customers.

1. **Most Likely Disaster Scenarios.**
   The first step in creating your IT disaster recovery plan is to create a list of disastrous events that are most likely to interfere with your company's operations. Think through potential problems in advance. Prepare for the unexpected. Address catastrophes that could happen because by the time disaster strikes, it is often too late.

   Visit http://www.disastersafety.org/zip-code-risk-search-results/ to discover the natural disasters your company might face.

2. **IT Hardware, Processes, Software, and Systems Currently in Use.**
   In order to restore your information technology services, you must know what hardware, processes, software, and systems are currently in use. If the equipment or software is an asset, your accounting department most likely maintains a listing of makes, models, and serial numbers. However, the inventory required for IT disaster recovery must be much more detailed.

   Itemize hardware, network services, resources, and security configurations. Itemize equipment and system-level components, including operating system documents, licensing, access management, etc. Document IT processes, such as back-up procedures, cloud computing, mobile computing, and server virtualization. Likewise, business applications and software must also be inventoried—including make, version, patches and fixes, configurations, users and roles, interfaces, customizations, client systems, network considerations, etc.

Download sample computer equipment and software inventory forms and voice/data communication forms by visiting http://www.disastersafety.org/open-for-business/ofb-basic/

3. **How Quickly Each IT Service Should Be Restored.**
   It is critical to prioritize the restoration of IT services before disaster strikes. Therefore, determine the maximum time your company can survive without each IT service—*telephones, Internet connectivity, email, access to your Virtual Private Network (VPN), website, order entry capability, inventory status, shipping and invoicing capabilities, etc.*

   Set objectives for the amount of time each IT service can be unavailable without unacceptable consequences while the IT department works to get the service back up and running in order to avoid unacceptable consequences. This is known as the Recovery Time Objective (RTO).

   Recovery Time Objectives vary by company. However, typical IT services that must be resumed in real time to prevent serious business impact include telephone service, text messaging, email, and voicemail. Your website, ordering, and inventory systems may need to be restored in two hours; invoicing systems restored within 24 hours; and accounts receivable, accounts payable, and payroll within 48 hours; and business intelligence systems within 72 hours.

4. **How Much Data You Can Afford to Lose.**
   Another aspect of IT Disaster Recovery Planning is the maximum amount of data that you can afford to lose during an outage. This is known as the Recovery Point Objective (RPO).

   Fortunately, there are many preventative measures available to electrical distributors of all sizes to prevent, or at least minimize, the loss of data. Examples include spreading IT equipment across multiple sites, offsite tape backup for servers, data centers, and laptops; offsite disk mirror and storage; offsite data replication; Storage Area Network (SAN) storage; remote backup servers; outsourced services; cloud computing; co-location sites, etc.

5. **Develop Recovery Strategies.**
   Key to restoring IT services quickly is having qualified individuals available to take the necessary actions. Rotate back-up operations so multiple people in your organization know how to back up and restore equipment. Make sure several people in different locations are thoroughly cross-trained on the most critical tasks.

   Create basic documentation for each application including tech support contacts, log-ins, admin passwords, how to troubleshoot and restore, etc. Keep electronic and paper copies of this information both on-site and off-site.

Compile a listing of key personnel contact information---home and cell phone numbers, as well as personal email addresses. Develop a notification calling tree and subscribe to a broadcast voicemail service to notify employees and keep customers up-to-date on the disaster, as well as your recovery efforts.

NOTE: Broadcast services, such as www.simpleblast.com, allow you to reach employees and customers through various personal accounts, home phones, and cell phones until normal phone and email systems are restored

6. **Continually Communicate Your IT Disaster Recovery Plan.**
   Anticipating problems and developing an IT Disaster Recovery Plan to address IT service outages does not in itself guarantee success. Implementation of the plan is what will help your business recover from a disaster. To ensure readiness, continually communicate your plan to employees. Provide training so everyone knows what IT services will be available when; how to communicate with customers and each other; and what to expect...before disaster strikes.

7. **Regularly Test Your Data Disaster Recovery Plan.**
   Build confidence in your IT Disaster Recovery Plan by testing it at least once a year (some companies even test their IT Disaster Recovery Plans quarterly). The primary reason for testing is to identify deficiencies in your plan. Testing will also make sure your plan is sound, make sure recovery processes work according to plan, and determine if your hierarchy for service recovery is correct. For example, your plan may have the computer system as the top service to restore; however, testing may prove that another service is more vital and should be moved up in the hierarchy.

   After testing your IT Disaster Recovery Plan, evaluate your company's performance because any plan that does not uncover any issues should be considered suspect. A successful test will uncover issues and gaps. Corrective action should be taken within 2 weeks of the test, followed up on within 2 months, and verified during the next annual test.

   There are three ways to test your Data Disaster Recovery Plan:

   - **Checklist Testing:** The plan is reviewed for any inconsistencies or missing elements individually by team members.
   - **Walkthrough Testing:** Team members discuss each step of the plan to identify inconsistencies, missing elements, and confirm that they know and understand their duties in the event of an emergency.
   - **Simulation Testing:** Tests all IT infrastructure concurrently using all of the business continuity resources such as recovery sites, backup and restore solutions, and any other specialized services. Simulation testing verifies if time estimates for recovery are realistic, identifies new business conditions that require changes in the plan, and tests the most unpredictable element in the plan—*people*.

8. **Continually Update Your IT Disaster Recovery Plan.**
   IT Disaster Recovery Planning is not a one-time event. Your IT Disaster Recovery Plan must be continually updated to reflect the IT hardware, processes, software, and systems actually in use. Since an IT disaster can occur at any time, develop internal processes to ensure new equipment purchases, upgrades, and process changes are included in your IT Disaster Recovery Plan in a timely fashion.

9. **Set Recovery and Investment Priorities.**
   Identify your information technology vulnerabilities by comparing the Recovery Time Objective and the Recovery Point Objective for each IT service. Prioritize issues in order of the potential impact of a particular IT service on your company. Make adjustments RPOs and RTOs as necessary.

   While smaller companies may have more options than larger companies, few businesses can justify the expense of upgrading every IT service at once. Tackle the most critical IT services first, spread IT disaster recovery investments over several years, and include IT disaster recovery in your annual budget.

Recommended Resources

Article: ***Business Continuity and Disaster Recovery: The Basics***
http://www.cio.com/article/204450/Business_Continuity_and_Disaster_Recovery_Planning_The_Basics

Data Protection: ***A Vital Part of Business Protection***
http://www.disastersafety.org/commercial_maintenance/data-protection-a-vital-part-of-business-protection/

IT Disaster Recovery Planning for Dummies by Peter Gregory

Disaster Recovery Journal
http://www.drj.com/

Sample IT Disaster Recovery Template
http://searchdisasterrecovery.techtarget.com/feature/IT-disaster-recovery-DR-plan-template-A-free-download-and-guide