BEST PRACTICES IN DISASTER RECOVERY PLANNING AND TESTING

Apex
Technology Management, Inc.

Transforming Organizations and Lives Through Innovative Technology Solutions

apex.com · (800) 310-2739 · info@apex.com

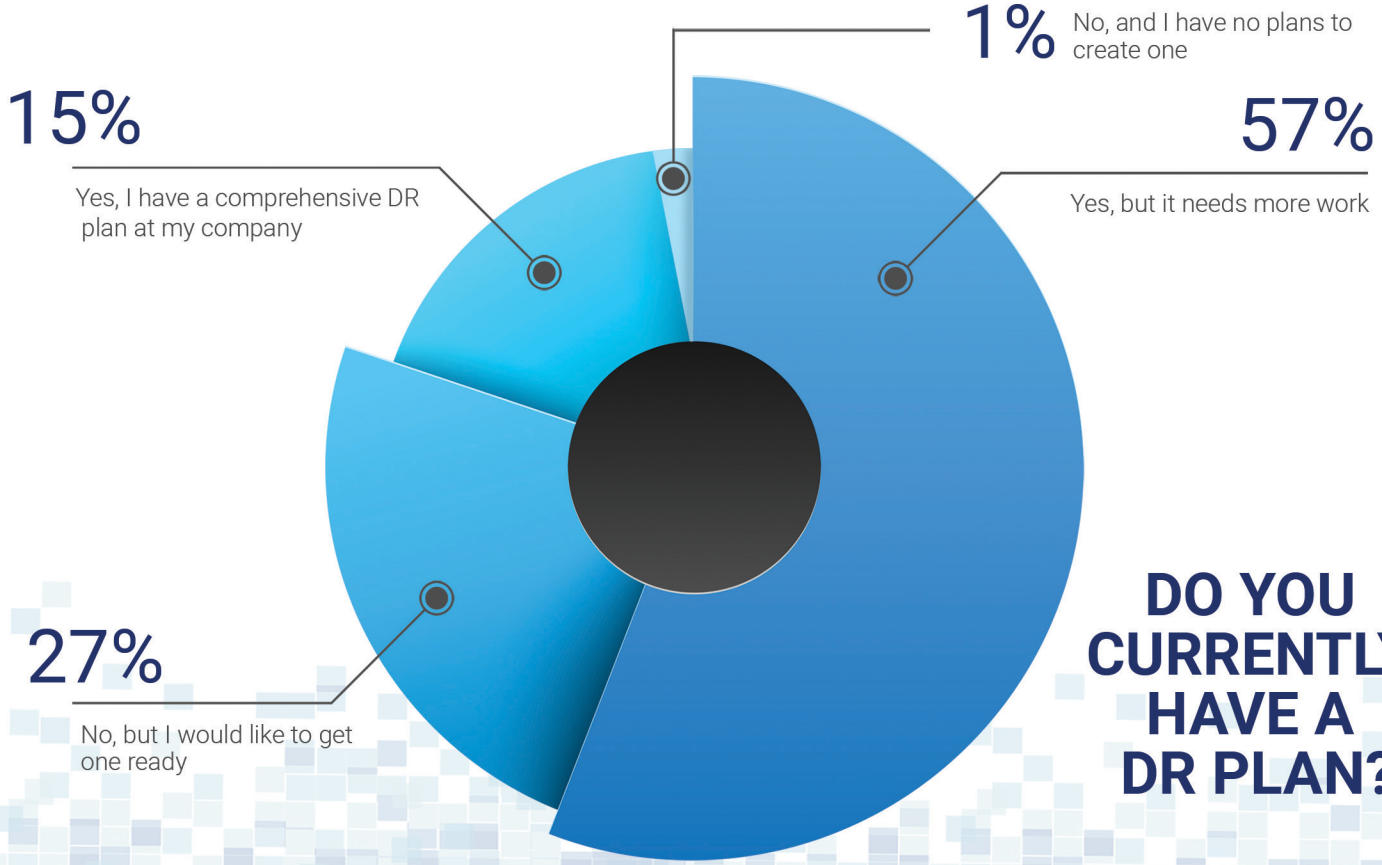
Apex Technology Management understands the importance of strategic and unique Disaster Recovery plans for all of our clients. DR plans are widely accepted as a way to ensure that critical data, IT systems and networks can be recovered in the event of an emergency. These plans are also a key component to ensure that your business objectives can be achieved during the disruption.

You may think of these plans as just a documented strategy to save your business in the event of a major disaster like a flood or fire – and you wouldn't be alone. But the reality is that a Disaster Recovery plan is created to protect your infrastructure against any event that could cause disruption, including:

- **Technical glitches**
- **System failures**
- **Power outages**
- **Cyber attacks**
- **Data theft**

These disruptions can cost companies thousands (and in some cases hundreds of thousands) in damage and an even bigger loss at the end of it all: reputational damage to the company's brand.

DO YOU CURRENTLY HAVE A DR PLAN?



Your Plan

There are a few key elements necessary for your DR plan to run efficiently:

Management Support: Without the support of management, creating an effective plan will be nearly impossible.

Approved Funding: Keeping your company running takes additional resources and these resources cost money that management may be reluctant to spend.

Structured Plan Framework: This ensures that everyone is on the same page.

Access to Qualified Staff: Don't assume that everyone in your IT team is qualified to put together or execute this plan. This may require additional training or knowledgeable consultant resources.

Access to Relevant Information: Research and/or conduct interviews to gather the information you need.

Documentation and Testing: Your plan has to be documented and tested regularly to ensure smooth execution in the event of an emergency.

All of these elements combine to form the goal of the DR plan, which is to build a plan and associated documentation based on a structured framework that is consistent with good practices and standards.

The good practices and standards ensure that your team is not only following the guidelines of what's best for your business and industry, but that you are also compliant with any regulations that surround recovery and planning in your industry.

Standards:
NFPA 1600:2010; ISO 27031:2011; ISO 22301:2012; NIST 800-34

Regulations:
FINRA 4370

Good Practice:
BCI Good Practice Guidelines, FFIEC Handbook

Corporate DR Policies:
Existing corporate policies that should apply to your DR plan

Sample Policies and Standards

For a comprehensive list of existing legislation and regulations worldwide related to Disaster Recovery and Business Continuity, refer to the Business Continuity Institute publication BCM Legislations, Regulations & Standards.

- The National Commission on Terrorist Attacks Upon the United States (the 9/11 Commission), recognized NFPA 1600 as the National Preparedness Standard. Created by the National Fire Protection Association, the NFPA 1600 **"Standard on Disaster/Emergency Management and Business Continuity Programs"** contains provisions related to the development, implementation, assessment and maintenance of programs for prevention, mitigation, preparedness, response, continuity, and recovery

- The **ISO/IEC 27031:2011** describes the concepts and principles of information and communication technology (ICT) readiness for business continuity, and provides a framework of methods and processes to identify and specify all aspects (such as performance criteria, design, and implementation) for improving an organization's ICT readiness to ensure business continuity. The **ISO 22301:2012** specifies requirements to plan, establish, implement, operate, monitor, review, maintain and continually improve a documented management system to protect against, reduce the likelihood of occurrence, prepare for, respond to, and recover from disruptive incidents when they arise.

- NIST **Special Publication 800-34, Contingency Planning Guide for Information Technology (IT) Systems** provides instructions, recommendations, and considerations for government IT contingency planning.

- **Rule 4370 of the Financial Industry Regulatory Authority** requires firms to create and maintain business continuity plans (BCPs) appropriate to the scale and scope of their businesses, and to provide FINRA with emergency contact information.

- The **Business Continuity Institute Good Practice Guidelines (GPG)** are the independent body of knowledge for good Business Continuity practice worldwide.

Gathering the above information will take a little time, but it's worth it to keep your business going through any situation. When gathering this information, it's important to also identify anything that could cause a glitch in your plan; the objectives you have for your system, network and IT asset recovery; and anything your company can do to mitigate your risks.

Plan Components

From experience, Apex Technology Management knows that for a Disaster Recovery plan to actually work, there are certain components that should to be included. These are all important to the plan's ease of execution and effectiveness.

Define

- Plan scope, purpose and authority
- Policy statement
- Management approval and funding
- Staff roles and responsibilities
- Authorized person to declare disaster
- Step-by-step procedures for recovery of all physical, mechanical and virtual items (this includes premise security, records and wireless technology)
- Step-by-step procedures for alerting key people (includes members of staff, family members, media, vendors and alternate vendors, clients, stakeholders and first responders)
- Process for training

Identify

- IT resources
- Risks and impact on IT assets
- Process for equipment replacement
- Process for obtaining spare parts
- Designated spokesperson

Determine

- Recovery Time Objectives (RTO)
- Recovery Point Objectives (RPO)
- Preventative controls
- Response and recovery strategies
- Event notification procedures (could be an automated feature or an outsourced call center)
- Recovery failover procedures
- System restart/ failback procedures
- Resumption of business procedures

Use

- Hot/Cold Sites (Hot sites have most of what you need to keep your business running, including hardware, software, servers and computers. Cold sites provide the power, environment and workspace, but no equipment.)
- Help desk support
- Call trees
- Conference bridges

Since both management and non-management staff are involved in Disaster Recovery, everyone should be aware of these policies. A meeting or the distribution of the policy will be necessary as soon as the key members of the plan are identified.

Next, everything should be compiled into a document. All aspects of your plan (including the information gathered from the previous page) should be made available to all DR personnel.

Lastly, it's crucial to include a Business Impact Analysis Report and Risk Assessment Report — this is vital.

- The RA (Risk Assessment) will outline events that could disrupt your business.
- The BIA (Business Impact Analysis) will illustrate how these disruptions will impact your business.

Technology Options for Disaster Recovery

A good Disaster Recovery plan will also discuss the technology behind your DR efforts. What kind of technology you use depends on your risks, how much data you have to store, the number of people needed to access that data, and the sensitivity of the data.

Due to budgetary constraints, some companies build their own DR architecture, assembling different products or building some infrastructure in-house. We have seen, for example, companies using local backup products in combination with automated scripts developed by their engineers to off-site data to public cloud storage like Amazon. Other companies mix different flavors of server replication to accommodate for their heterogeneous environment.

While interesting at first, the "do- it-yourself" approach to Disaster Recovery leads to a number of issues. As explored by Forrester Research in its report on the risks related to DIY DR, companies report a number of challenges when it comes to their in- house DR infrastructures, namely:

- Lack of focus on DR relative to other IT projects
- Not enough DR testing
- Lack of funding to keep DR infrastructure up to date
- Lack of skills in-house
- Not confident in ability to respond to a real disaster

These results clearly show that bringing Disaster Recovery in-house is not the best choice for most companies. That's why Apex Technology Management is eager to provide strategy and support that ensure your DR plan is aligned uniquely with the risks facing your operations.

TOTAL COST OF OWNERSHIP

Total cost for owning a disaster recovery solution takes into consideration factors such as:

Capital Expenditures:
Cost of purchasing software, hardware, and implementing the solution

Operational Expenses:
Cost for maintaining the solution, including time spent reviewing backup logs, ensuring successful completion of backup jobs, troubleshooting error messages, testing restores and running full DR tests

Downtime:
The time that it takes to bring files, applications, full servers and a full site back into production after an outage and related costs associated for loss of productivity and revenue

CONSIDERATIONS FOR DR TESTING

Businesses responded with surprising answers when asked, "How often do you test your DR plan and/or the ability to recover from a disaster?"

TIPS FOR TESTING

Ready to test your Disaster Recovery plan? Here are a few tips to follow:

- ☐ — Make sure the test is set for a date that isn't critical for your business and a date where all participants and alternates are present.
- ☐ — Ensure everything is properly documented.
- ☐ — Before administering the test, think about the area you need to test. It may not be possible to test all aspects of the plan at one time, so test section by section. You also need to keep in mind how much strain this test will have on your systems.
- ☐ — Find an environment to test in, preferably in a non-production area. Most businesses use conference rooms or empty offices for this.
- ☐ — Gather all personnel listed in the DR plan and have them play out their roles in the test.
- ☐ — Include a timekeeper.
- ☐ — Keep note of what did and didn't work in a report, and update the report based on the results.
- ☐ — Do a dry run first.

To make the most of your Disaster Recovery Plan, document it. You may not be present when an event occurs, so multiple copies should be available to selected staff members. Finally, run your DR plan by management each time a change is made to ensure financial backing and approval. By following this guide, you'll not only safeguard your business, but you'll also save yourself from hidden risks that would have otherwise gone unnoticed.

Get in touch with Apex Technology Management to discuss the most effective Disaster Recovery strategies for your needs. Our team of experts are eager to ensure that your operations are able to continue functioning no matter what type of disaster hits – reach out to us at info@apex.com or (800) 310-2739 to gain the peace of mind you need.