An MSP Playbook for Best Practices in Disaster Recovery Planning, and Testing

Best Practices in Disaster Recovery Planning and Testing

Disaster Recovery plans are widely accepted as a way to ensure all critical data, IT systems and networks can be recovered in any event classed as an emergency. These plans also ensure that corporate business objectives can be achieved during the disruption. In short, it is a plan that keeps a business operational.

In a recent Disaster Recovery survey, we asked business owners if they currently had a Disaster Recovery Plan in place. While only 1% felt secure without one, the overwhelming majority didn't. More than 57% of those surveyed said they currently have a plan that needed a little work; 27% said they don't have a plan, but would like to develop one; and the remaining 15% have a plan that they felt was good to go.

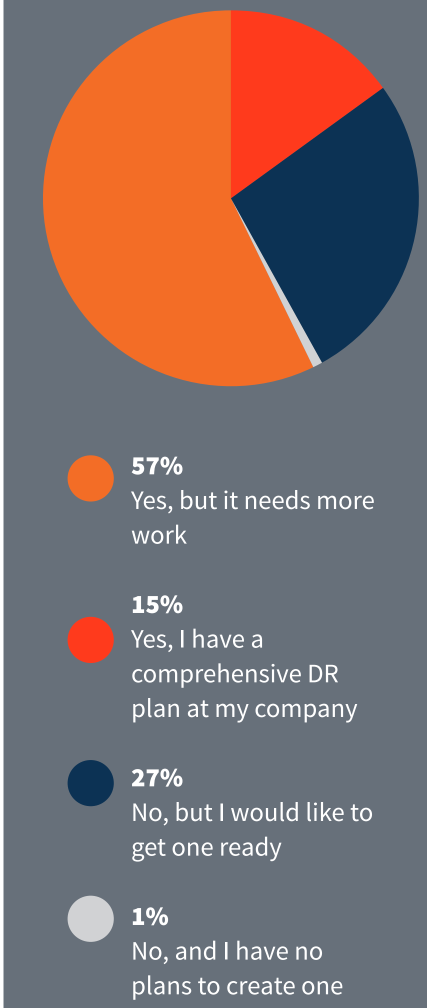
Your clients think of these plans as a documented strategy to save their business in the event of a major disaster like a flood or fire, and they wouldn't be alone. But the reality is that a Disaster Recovery plan is created to protect infrastructure against any event that could cause disruption, including technical glitches, system failures, human error, power outages and even cyber attacks or data theft. These disruptions cost companies thousands (and in some cases hundreds of thousands) in damage and an even bigger loss at the end: damage to the company's brand.

Devising Your Plan

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

- **Management Support:** Without the support of management, creating the plan is futile.
- **Approved Funding:** Ensuring business continuity during a disaster recovery requires foresight and investment. This budget should be proactively discussed and decided ahead of time.
- **Structured Plan Framework:** Discuss the steps and assign response activities to specific people. Plus, have a plan for communication if critical and preferred systems are down.
- **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 expert consultants. Document your DR solution vendors role in the disaster recovery.
- **Access to Relevant Information:** Research and/or conduct interviews to gather the information you need. Set a timeline to acquire tools and capabilities to keep business going, and to answer critical questions like "will you pay a ransom?".
- **Documentation and Testing:** Your plan has to be documented and tested regularly to ensure smooth execution in the event of an emergency.

DO YOU CURRENTLY HAVE A DISASTER RECOVERY PLAN?



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 you're 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 and country.

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. Axcient pulled together this digestible guide on the NIST Framework For Improving Critical Infrastructure Cybersecurity.

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.
In the next section we will explore the components that make up your plan.

COMMON STANDARDS USED IN THE DR INDUSTRY INCLUDE:

- **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

Plan Components

The previous information is there to help you structure your plan, but these components are what you need to run it. For a Disaster Recovery plan to actually work, there are certain elements that have to be included. These are all important to the plan's ease of execution and effectiveness and they begin with your company's own DR policy. 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.

Your DR plan should include the IT DR plan, the results of previous efforts for testing the plan, and supporting documents.

The supporting documents for your DR plan are what stand between a successful recovery and a failed one. These documents include processes for data backup, information about off-site storage and processes, vendor and maintenance contracts, diagrams, and training plans.

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 (if necessary)

- 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
- Automated Notification Systems
- Conference bridges

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. Your plan should have a TOC (Table of Contents) and outline that lists each step of the plan in order of importance. (Emergency Response Actions should always come before anything else). Lastly, 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 and the BIA (Business Impact Analysis) will illustrate how these disruptions will impact it.

Things to Avoid When Creating the Disaster Recovery Plan

Although gathering the above information is a lengthy process, avoid skipping any of the steps or required sections. Some businesses make the mistake of utilizing generic DR plans or the plans of other businesses in their industry. This may seem like a time-saver at first, but you'll see during testing that it could prove disastrous. The other business (or the business that the generic plan is modeled after) could have more assets or finance than you or have fewer risks than you. So, if that plan only covered natural disasters and your business is the victim of data theft, it's pretty much useless. This makes research — and, more importantly, a BIA and RA — a must.

Other pitfalls you'll want to avoid:

- **Not defining a clear budget from the start**
- **Creating the plan without management's backing**
- **Summarizing procedures in the plan**
- **Assuming that all systems will be backed-up and running immediately**
- **Skipping testing and reviews**
- **Keeping all copies of the DR plan on-site**
- **Not training DR personnel**
- **Assuming all listed personnel will be available (including IT staff)**
- **Underestimating the time and cost for failback to original or new hardware after a recovery**

The last item is possibly the most important in this section. As your business grows or expands into other areas, your needs, risks, vendors and key personnel may change. This requires you to manually update the plan and recalculate any figures contained within it. Once you do, the new plan should be discussed and another exercise should take place.

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.

When we asked business owners what kind of technology they used for Disaster Recovery, the numbers were surprising. More than 69% said they still use local backup to a disk or tape. While local backup might seem like an attractive option at first, it leaves businesses susceptible to interruption in a variety of scenarios such as power outage, virus attack, or server crash. All three could have serious business implications.

Taking Advantage of Cloud Backup Technology for Remote Workforces

By backing up directly to the cloud, MSPs can enjoy excellent margins that allow them to offer fast disaster recovery and business continuity for all of their client types, without the cost and hassle of expensive appliances for more cost-sensitive customers.

Remote workers typically rely on less sophisticated security solutions that often don't include firewalls. Their data is more susceptible to loss because they may not be able to contact corporate networks for regular backups or can only do so through cumbersome VPNs.

Innovative hardware-free BDR backs up end-user desktops, laptops, client servers, and workstations with significantly less costs, limitations, and stress than appliance-based BDR solutions. Not only are your distributed workers protected with comprehensive backup, but features like Axcient AirGap, which separates requests to delete data from the mechanics of data deletion, provide a last line of defense against ransomware and various disasters.

With cloud-based backup, MSPs can rapidly recover a single file or a whole system in the blink of an eye. With a solution like Axcient's x360Recover Direct-to-Cloud, all volumes on each endpoint are protected automatically, offering an elegant solution to remote workforce business continuity, backup, and recovery.

Over 70% of MSPs use more than 1 backup vendor. MSPs know that having multiple vendors can increase the complexity and cost of DR and DR testing. As an Axcient partner, you can consolidate your local and cloud BCDR services with one reliable provider and reduce your vendor maintenance time and monetary costs while increasing your margins.

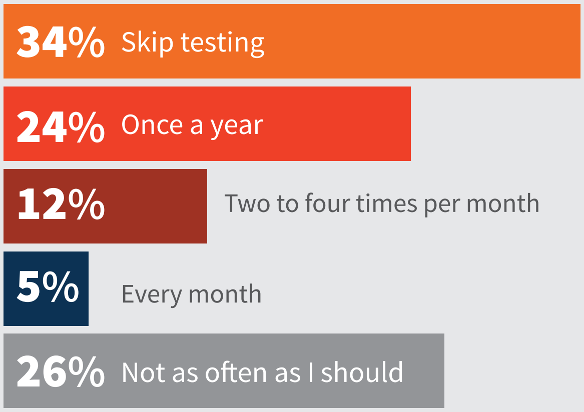
DIY DR

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 a 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**

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



How often you should test is determined by your risks and assets. Those who are at a greater risk like to test more frequently (say, every week), those who are at a moderate risk may test quarterly, and those who are at a very low risk may only test once a year. However, no matter what category your business is in, you should always test your DR plan.

These results clearly show that bringing Disaster Recovery in-house is not the best choice for most companies. When looking at the different options available, businesses that have taken into consideration the Total Cost of Ownership (TCO) seem to have gotten a better bargain.

While an expanded discussion of TCO is outside the scope of this document, keep in mind that the effectiveness of a Disaster Recovery plan is also tied to the effectiveness of the underlying technology being used to recover from a disaster.

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

The Importance of a DR Plan to Protect Cloud Applications

Your Disaster Plan should include backup for Microsoft 365 and Google Workspace. You should back up client's G Suite and everything in their Microsoft 365 instance – including all licensed and unlicensed users' Exchange, OneDrive, SharePoint, and Teams – so you can always recover anything and everything the moment you need it most. – because Microsoft doesn't.

MSPs creating a cloud application DR plan should aim to minimize downtime while at the same time ensuring data security and compliance with regulatory requirements. If you're not educating clients about Microsoft's Service Agreement and providing a disaster recovery plan for disaster recovery cloud application protection, you could be putting your business at risk.

Axcient x360Cloud provides MSPs and their clients the most reliable and complete backup and restore for Microsoft 365 and Google G Suite. Did you know Microsoft does not guarantee against data loss? Data can still be lost in the cloud due to accidental deletion, a malicious employee, or ransomware – yes, even Microsoft 365 can be crypto-locked. x360Cloud backs up all Microsoft 365 services with unlimited storage and retention.

Considerations For DR Testing

All of the tips provided are designed to keep you and your staff abreast of any changes that could affect the plan or the execution of it. 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.

TIPS FOR DR TESTING

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 or alternates are present. You'll also need to notify your IT staff at least two weeks prior to testing.
- ✓ Document the step-by-step procedures of the test and hand them out to all selected personnel.
- ✓ Before administering the test, think about the area you need to test. It may not be (and almost never is) 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. Running a test might disrupt them and cause further disruptions to processes that need to keep running.
- ✓ 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.

Free DR Testing Tools in Our Solution

Axcient partners can take advantage of free DR testing tools in the x360 solution such as self-managed Virtual Office and Runbooks. Virtual Office is a cloud failover feature in x360Recover allows you to start virtual machines in the Axcient Cloud of one or more protected devices. You can then create a Virtual Office running within the Axcient data center, using matching existing server configurations.

Axcient x360Recover Virtual Office enables MSPs to quickly virtualize one or more systems in the Axcient Cloud to replace all impacted production infrastructure temporarily. The self-managed cloud disaster recovery technology provides MSPs with flexibility, optimization, and peace of mind that their clients' businesses will always be on.

Axcient's Virtual Office technology provides the ability to:

- Instantly recover production servers and workstations in the Axcient Cloud
- Perform regular full-office recovery tests to ensure backups are always recoverable
- Easily configure secure access to Virtual Office instance using VPN, Site-to-Site OpenVPN, and port forwarding
- Restore to the production server or desktop at the partner's convenience after business continuity
- Ensure compliance needs are met by encrypting data in transit, and at rest in our offsite SOC II Type II certified datacenters
- Self-manage Axcient Virtual Office using a secure, web-based application, which includes role-based authentication with required MFA

In addition, MSPs should consistently verify that the backup data on protected systems have good backups that are fully recoverable with free DR testing tools like Axcient's x360 is automated nightly BootVM checks and Autoverify.

Autoverify is a critical capability of x360Recover that intelligently tests your backup integrity and ensures backups are always recoverable via boot and deep volume checks. x360Recover has supported integration into popular PSA/RMM tools so that AutoVerify data and BootVM screenshots can be seamlessly captured. In addition, Axcient x360Recover supports alerting and escalation rules so that techs are notified only when absolutely required. As part of Axcient x360Recover by default, you know AutoVerify intelligently tests your backup integrity on a regular basis.

Key benefits of AutoVerify:

- Offers MSPs confidence in the integrity and recoverability of their backup system
- Reduces the time spent manually fixing issues that might occur during a recovery fail over
- Lowers the total cost of ownership (TCO) by automatically detecting, alerting, and fixing backup consistency issues
- Allows for faster identification if there are any potential backup issues
- Alerts from AutoVerify can sync directly with PSA and RMM technology tools, such as ConnectWise

> "I'm glad we moved to Axcient x360Recover because now I can tell clients, 'don't worry, we did an automated test restore yesterday, and your data was good.' Some clients have access to their Axcient portal so they can actually see the backups themselves and don't need us to confirm anything."
>
> – Roddy Bergeron, CISO at Enterprise Data Concepts

Additional Resources

For more information about best practices in disaster recovery planning and related topics, we encourage you to check out the following resources:

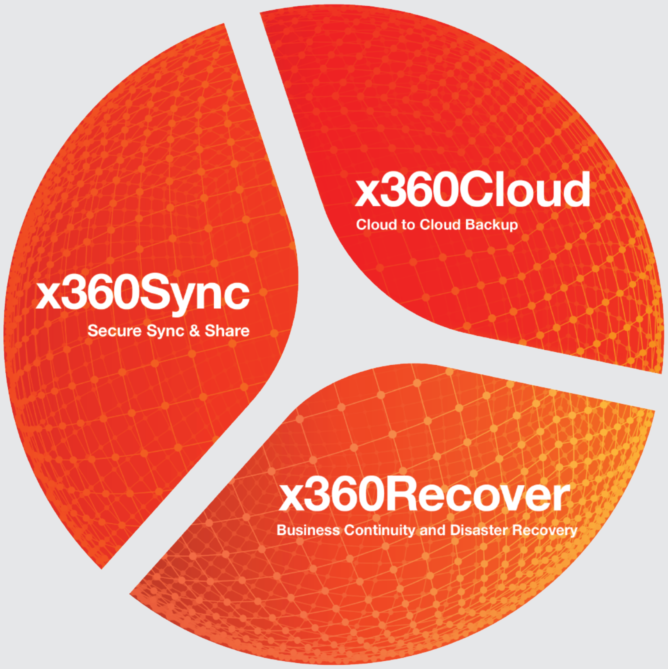
How to Talk RPO and RTO With Your Clients
https://axcient.com/blog/rpo-and-rto-the-conceptual-vise-grips-of-bdr-sales/

Why You Should Care How Your Backups Work
https://axcient.com/blog/why-should-you-care-how-your-backups-work/

Is Microsoft 365 the Big Hole in Your Business Continuity Plans?
https://axcient.com/blog/importance-of-business-continuity-planning-microsoft-365/

Seamlessly Virtualize Azure VMs with x360Recover Direct-to-Cloud for Microsoft Azure
https://axcient.com/blog/seamlessly-virtualize-azure-vms-with-x360recover-direct-to-cloud-for-microsoft-azure/

Local Cache for Fast Recovery Without the Pricey Hardware
https://axcient.com/blog/local-cache-for-fast-recovery-without-the-pricey-hardware/



Axcient x360 Platform

The Axcient x360 Platform is the proven business continuity and disaster recovery solution for MSPs. Axcient's powerful business continuity, backup, and disaster recovery solutions protect your clients and enable you to standardize on reliable, affordable technology. Axcient is 100% focused on helping MSP partners build their businesses.

See the Axcient x360 solution for yourself at Axcient.com

ABOUT AXCIENT:
Axcient is an award-winning leader in business continuity and disaster recovery for Managed Service Providers (MSPs). Axcient x360 provides one platform for MSPs to Protect Everything™, and includes BCDR, Microsoft 365 and Google Workspace backup, and secure sync and share. Trusted by more than 3,000 MSP partners worldwide, Axcient protects business data and continuity in the event of security breaches, human error, and natural disasters.

CONTACT:
Axcient, 707 17th Street, Suite 3900, Denver, CO, 80202
Tel: 720-204-4500 | axcient.com

FOLLOW US: