Project Success Plan: Business Continuity & Disaster Recovery

Everything you need to know about business continuity and disaster recovery, planning and prevention.

In this guide

In this e-guide:

Because planning for business continuity and disaster recovery can be a real challenge, we have pulled together this Project Success Plan to make things a bit easier for you. Included is everything you need to know about planning for, or recovering from a disaster/unexpected event, to ensure you can resume operations quickly without too much disruption.

What are your options when designing a disaster recovery plan? What tools are available? What challenges will you run into? Where do you even begin? This comprehensive guide will walk you through the entire process of designing a DR plan that fits your needs all the way through to the testing your plan will require once implemented.

In this guide

What is Disaster Recovery

http://searchstorage.techtarget.com/definition/Business-Continuity-and-Disaster-Recovery-BCDR

Business Continuity and Disaster Recovery (BCDR or BC/DR) are closely related practices that describe an organization's preparation for unforeseen risks to continued operations. The trend of combining business continuity and disaster recovery into a single term has resulted from a growing recognition that both business executives and technology executives need to be collaborating closely instead of developing plans in isolation.

In general, disaster recovery refers to specific steps taken to resume operations in the aftermath of a catastrophic natural disaster or national emergency. In information technology, such steps may include restoring servers or mainframes with backups, re-establishing private branch exchanges (PBX) or provisioning local area networks (LANs) to meet immediate business needs.

Business continuity describes the processes and procedures an organization must put in place to ensure that mission-critical functions can continue during and after a disaster. In this sense, the concept is interchangeable with disaster recovery plan (DRP). Business continuity, however, also addresses more comprehensive planning that focuses on long term or chronic challenges to

In this guide

organizational success. Potential business continuity problems may include the illness or departure of key team members, supply chain breakdowns, catastrophic failures or critical malware infections.

Next article

In this guide

Why Consider a Disaster Recovery Project

http://searchcompliance.techtarget.com/news/2240160705/QA-Developing-your-business-continuity-and-disaster-recovery-plan

In this Q&A, consultant and auditor Paul Kirvan discusses what you need to consider when developing a business continuity and disaster recovery plan.

Business continuity and disaster recovery plans are the first line of defense in the aftermath of a disruptive event. After an unexpected catastrophe, these plans -- especially ones that are properly documented and regularly exercised -- help organizations greatly increase their chances of resuming normal business operations quickly and with minimal interruption.

Business continuity and disaster recovery plans can provide a competitive advantage, especially as major organizations increasingly require them as part of vendor selection and contracting processes. Without the plans, organizations risk sanctions, fines, loss of customers, lawsuits and even going out of business following an unexpected event.

In a Q&A with independent consultant and auditor Paul Kirvan he discusses the traits of a solid business continuity and disaster recovery plan, where

In this guide

organizations should start when developing their plans, and how to use cloud-based services for your disaster recovery and business continuity needs

Q: What are some common characteristics of a successful business continuity and disaster recovery plan?

Paul Kirvan: Among the key characteristics -- and these are not necessarily in a specific order of importance -- are:

1. Up-to-date contact lists -- both internal and external -- so plan activation can proceed quickly and smoothly.
2. Documented and easy-to-understand procedures on how to respond to specific situations -- examples can include evacuation plans with assembly points, recovery of servers and recovery of voice and data communications.
3. Regular exercises to validate plan procedures will work as designed.
4. Trained and motivated emergency response team members who know their roles and responsibilities in an emergency.
5. Advance arrangements with third-party organizations to provide emergency support services, such as work areas for temporarily displaced employees and rapid replacement of damaged equipment and furniture.

In this guide

6. Advance arrangements for obtaining cash and other financial instruments to maintain payroll and other key business activities.

7. Awareness and understanding of the business continuity and disaster recovery plans by local first-responder organizations.

8. Administrative and budgetary support from senior management for a business continuity and disaster recovery program.

Q: What business areas and processes do companies have to take into consideration when developing a disaster recovery and business continuity plan? Why are these areas and processes important?

Kirvan: Careful research into the business and how it works helps define business continuity and disaster recovery plans. This information is usually captured by performing a business impact analysis. Typically, all department leaders and senior staff within the organization are interviewed to learn what their business unit does and how it operates; how it contributes to the company's success; what organizations (both internal and external) it depends on for normal operations; what technologies, applications and systems are needed to perform daily activities; the data, such as files and databases, needed to conduct business; and the timeframes in which the business unit needs to be back in operation and have access to its data before its loss could have an adverse effect on the overall organization's ability to conduct business.

In this guide

This information is then used to identify the most critical business activities or processes; how quickly these processes and associated systems need to [be] back in service following a disruptive event; and alternate arrangements that could be launched to recover business operations.

Another important research activity is a risk assessment, which examines internal and external situations that could threaten the organization's ability to conduct business. It also identifies both perceived and actual vulnerabilities to the organization that could make threats become realities. This information is analyzed along with findings from the business impact analysis to provide an overall risk profile of the organization.

Q: Are cloud solutions a viable option to help with disaster recovery and business continuity? If so, how?

Kirvan: Cloud-based solutions for disaster recovery and business continuity provide another option that can help an organization recover from a disruptive event. Cloud-based business continuity and disaster recovery solutions currently provide additional data processing and storage options so business operations can resume and critical data can be quickly recovered following an incident.

For example, let's assume you want to ensure certain key business activities, such as payroll and currency trading, experience minimal or no disruption or downtime following an incident. You can define a cloud-based service that can

In this guide

quickly recover and restart these critical applications, as well as load the data needed to handle the system requirements. This can be done without the need for physical space for servers, peripheral systems, or even network connectivity. It can all be resident in a cloud-based service, ready to go when needed. Ideally, cloud-based solutions can provide another line of defense to back up existing IT operations. Many organizations are considering a hybrid approach, blending the resources in primary data centers with the backup capabilities of a cloud-based solution.

Next article

In this guide

Key Terms to Understand

Change control
http://searchdisasterrecovery.techtarget.com/definition/change-control
This isn't the first thing that most folks think of when discussing the business continuity/disaster recovery issue, but it can have a serious impact on disaster recovery. If you ignore it, it can destroy your disaster recovery plan.

Business continuity action plan
http://searchdisasterrecovery.techtarget.com/definition/business-continuity-action-plan
Sometimes called an emergency plan, this document has the essential information your organization needs to stay in business when a disaster occurs. It must state your business' essential functions in writing, should delineate which activities must occur for your business to maintain operations, and explain what it takes to put the plan into reality. It includes a contact list for your employees, suppliers, vendors and contacts; copies of key records; and an inventory of your company's equipment and software

Synchronous replication
http://searchdisasterrecovery.techtarget.com/definition/synchronous-replication
Asynchronous replication is the most broadly supported replication mode, supported by array-, network- and host-based replication products. However, synchronous replication guarantees data consistency between the replication source and target.

In this guide

Pandemic plan

http://searchcloudstorage.techtarget.com/definition/cloud-disaster-recovery-cloud-DR

A pandemic plan must document how the business' essential services will be provided in the event there is significant and sustained absenteeism. It must also explain how the business will implement and enforce non-pharmaceutical intervention. You'll also need to learn how to address a pandemic's effects on your company and how to get started with pandemic and disaster recovery planning.

Cloud disaster recovery

http://searchcloudstorage.techtarget.com/definition/cloud-disaster-recovery-cloud-DR

Many organizations have turned to cloud storage as a means of saving space and money. But if you're faced with a disaster, you'll need to make sure that data is readily accessible. And there are issues involving branch offices, whether it's appropriate for SMBs and whether cloud disaster recovery services are viable for the enterprise.

ISO 22301

http://searchcloudstorage.techtarget.com/definition/cloud-disaster-recovery-cloud-DR

ISO 22301 is a global business continuity management standard that includes detailed practices and procedures which will offer business continuity

In this guide

management professionals the methodology to support their efforts. It remains a proposed standard at this point, so organizations using an existing standard should continue to do so. When reviewing your overall business continuity management program, you may consider switching to the global standard.

Hot sites and cold sites

http://searchcio.techtarget.com/definition/hot-site-and-cold-site

Hot sites support your current IT production activities whereas cold sites are typically empty spaces that lack the equipment and personnel needed in the aftermath of a disaster, but do offer electricity, access to communication services, and preconfigured areas with furniture, phones, and more. When choosing between hot sites and cold sites, you must consider the level of the disaster, cost, and a variety of other factors.

Maximum tolerable period of disruption

http://searchdisasterrecovery.techtarget.com/definition/Maximum-tolerable-period-of-disruption-MTPOD

ISO 22301 is a global business continuity management standard that includes detailed practices and procedures which will offer business continuity management professionals the methodology to support their efforts. It remains a proposed standard at this point, so organizations using an existing standard should continue to do so. When reviewing your overall business continuity management program, you may consider switching to the global standard.

In this guide

Business impact analysis

http://searchstorage.techtarget.com/definition/business-impact-analysis

It's not easy to conduct a business impact analysis and it is incredibly time-consuming, but once you've completed the BIA, you can request resources and prioritize security efforts across the enterprise.

Next article

In this guide

Comparing Leading DR Products

http://searchdatabackup.techtarget.com/news/2240237722/Backup-and-disaster-recovery-software-2014-Products-of-the-Year-finalists

The 10 finalists in the backup and disaster recovery software and services category for the *Storage* magazine/SearchStorage.com 2014 Products of the Year award illustrate the variety of products available for data protection today. Products eligible for consideration in the backup and disaster recovery (DR) software category include backup and recovery software, cloud backup and recovery services, DR, snapshot and replication software, electronic vaulting and archiving software. Finalists are listed in alphabetical order.

Asigra Inc. Cloud Backup Version 13 Featuring Cloud-to-Cloud Backup and Recovery

The latest version of Asigra Cloud Backup adds cloud-to-cloud backup for Salesforce.com, Google Apps and Office 365. Backup data from these applications can be integrated with backup data enterprise-wide, and stored both locally and off-site for DR purposes. The software also offers an automated restore function to repopulate data created in the cloud for restore.

Axcient Inc. Virtual Appliance

Updates to the software-only version of the Axcient physical appliance include local and cloud protection for data and applications; increased failover speed for

In this guide

one or multiple servers; and faster recovery time for files, folders and full system images. The software is hardware-agnostic, allowing users to repurpose existing hardware.

Code42 Software Inc. EDGE Platform Version 4.1.4

With version 4.1.4, Code42 brought CrashPlan and SharePlan together, combining its fully featured online backup and file sync-and-share products into one product. The platform can scale to 100,000 or more devices per single deployment and can be deployed on-premises, in the cloud or in a hybrid configuration. Customers can run backup and sync-and-share products simultaneously, or each product by itself.

CommVault Systems Inc. Simpana for VM Backup, Recovery & Cloud Management

CommVault Simpana for VM Backup, Recovery & Cloud Management offers Web-based cloud provisioning for public, private or hybrid clouds that allows users to create, provision and manage virtual machines (VMs) based on pre-set policies across VMware, Hyper-V, XenServer, Amazon Web Services and Azure. The product also offers recovery in place for DR/business continuity, VM replication with Changed Block Tracking for faster backups, and new cloud reporting features.

Continuity Software AvailabilityGuard Software Version 6.3

The latest version of Continuity's AvailabilityGuard includes additional service-level agreement policy support, which allows users to specify availability

In this guide

standards for specific software products. Version 6.3 also added granular role and privilege support, new risk detection capabilities, access control features, a configuration wizard, and additional support and integration with Active Directory.

HotLink Corp. DR Express 4.0

This plug-in for VMware vCenter allows users to manage backup/DR directly from the VMware vCenter console. New HotLink DR Express features include expanded VM migration to cloud capabilities, bidirectional replication for file servers and database servers, and new analytics and diagnostics tools.

Symantec Corp. NetBackup 7.6

The latest version of Symantec's NetBackup software combines Changed Block Tracking with synthetic block-level backup aimed at eliminating the need for traditional full backups. Symantec also added recovery in place for VMs from deduplicated backup storage, integration with VMware vCloud suite, and physical-to-virtual recovery for Windows.

Unitrends Inc. Certified Recovery Suite

Unitrends added protection for physical servers, and hypervisor- and guest-level protection for vSphere, Hyper-V and XenServer in the latest version of its backup software. Also included is new testing functionality, automated failover and changes-only failback for entire applications and sites, a new management dashboard, and integration with Unitrends cloud for DR.

In this guide

Zerto Ltd. Virtual Replication 3.5

Zerto added off-site backup for DR in the latest version of its Virtual Replication software to streamline backup and DR for users. Backups are created from replicas at the target site to minimize the impact on production applications. The software can back up to a secondary site or cloud, and Zerto has added new management tools and APIs for cloud service providers.

Zetta Inc. DataProtect 4.5

Version 4.5 of DataProtect added new features, including direct-to-cloud server image backup with built-in WAN optimization, recovery in place, appliance-free server image recovery to any location, native VHD bare-metal recovery, expanded support for Exchange and SQL Server (including the ability to back up directly to a Zetta cloud), and two-factor authentication for security.

Next article

In this guide

Evaluating Products

http://searchdisasterrecovery.techtarget.com/tip/Tips-on-selecting-BC-DR-software

When launching business continuity and disaster recovery initiatives, consider using specialized BC/DR software to help you achieve your goals.

BC/DR software helps build BC and/or DR plans -- either generic plans or plans for specific vertical markets, such as universities or government agencies. Some also facilitate risk assessments (RA) and business impact analyses (BIAs), the results of which can be used to build BC/DR plans. Since incident management (IM) is a key part of BC/DR plans, most systems can help develop IM plans. More sophisticated systems have their own automated emergency notification (EN) capability, while others may have intelligent links into established EN products. Some systems can help facilitate exercises and support awareness and training activities.

Examples of key players in the market include Everbridge, COOP Systems, Strategic BCP, Binomial International, eBRP Solutions, IBM, Paradigm Solutions International, SunGard and TAMP Systems. For budget-friendly BC/DR software, please check out the Rothstein Disaster Recovery Online Bookstore.

In this guide

Today's systems come complete with powerful relational databases and predefined templates to write just about any kind of plan. Systems that facilitate BIAs can design the BIA questions, distribute questionnaires to users, then collect and analyze the data gathered. Your system can run on a PC or laptop, server or even a mainframe. Most of the hot products are platform-type systems accessed via the Internet or cloud-based solutions.

Pricing ranges from under $500 for a CD-based system (such as the one found in the Rothstein bookstore) to hundreds of thousands of dollars for multinode networked systems (e.g., SunGard's LDRPS). Small and medium-sized businesses (SMBs) may find the low-cost products appealing since the results are usually consistent with good BC/DR practice and are budget-friendly. At the other end of the spectrum, it may be better to choose either a premise/server-based system to ensure proper management oversight, or a Web-based solution that is easily scalable and requires minimal to no overhead.

Tips for selecting the right BC/DR software

1. Define your requirements before research software options. If you have no BC/DR at all, consider the CD-based products. If you already have a system, determine what enhancements you need.

2. Ask internally for previous experience. Inquire among your colleagues and others in the organization to see if any of them have previously installed BC/DR software, perhaps with a prior employer.

In this guide

3. Engage a consultant. Find someone who has experience planning, installing and managing BC/DR software. Hopefully, you can obtain a relatively unbiased opinion on specific products and solutions.

4. Prepare and distribute a Request for Information (RFI). This approach helps you gather information about prospective vendors. From this exercise, you may be able to identify some prospective candidates. If possible, try out demo systems (or live systems if available) to get a feel for a variety of solutions.

5. Prepare and distribute a Request for Proposals (RFP). This is often the next step after an RFI and is designed to demonstrate your true interest in procuring BC/DR software solutions. Be sure to schedule detailed demonstrations of working client systems (not specially configured demo systems) as part of the RFP process.

Summary

The process for selecting BC/DR software is similar to selecting pretty much any other kind of software. Since your investment could easily get into the tens of thousands of dollars, do the research, ask a lot of questions and make your choice based on your current and anticipated needs.

In this guide

Hardware

http://searchitchannel.techtarget.com/feature/WAN-technologies-in-network-disaster-recovery

Getting your WAN requirements right for network disaster recovery

Disaster recovery (DR) planning isn't just a matter of storage. It's about identifying the data that your client requires for daily operations, and then duplicating that data across the wide area network (WAN) in a timely and cost-effective manner -- striking a balance between WAN speed and connectivity costs. However, deciding just what data needs to be handled, how much WAN bandwidth is needed to accomplish that replication and how to maintain security across remote sites can be difficult for even experienced solution providers. The first installment of this Hot Spot Tutorial introduced critical WAN issues and site planning considerations for disaster recovery. This second chapter details WAN bandwidth factors, redundant connectivity concepts and the use of other technologies, like VPNs and virtualization, in disaster recovery.

WAN bandwidth requirement issues

In simplest terms, the WAN bandwidth needed for disaster recovery is the amount of data that needs to be moved divided by the time available to move it. For example, if your client must move 1,000 MB of data in 10 seconds, they would theoretically need 100 MBps (about 800 Mbps) of bandwidth. Consequently, more bandwidth is needed to accommodate greater data

In this guide

volumes or smaller timeframes. The trick for solution providers is to establish both numbers accurately.

File sizes are fairly easy to determine through an assessment of the client's business applications, but remember that not all changing data is equally important. Different data types can be protected in different ways to reduce data loads and corresponding bandwidth needs. For example, a client may accumulate 100 MB of new or changed data each day, but if 75 MB of that consists of noncritical data that doesn't really require DR protection, only concern yourself with the remaining 25 MB of "important" data. Noncritical data that is not protected by the DR site can still be backed up for later recovery.

Similarly, it is often possible to split DR protection by data type. Suppose that 25 MB of important business data includes 10 MB of transactional data and another 15 MB of email, documents and other business communication. A solution provider can architect a DR plan that supports the transactional data with real-time synchronous replication, while protecting the remaining data with asynchronous coverage over 30 to 60 minutes or some other appropriate timeframe.

Data volumes can be greatly affected by data reduction technologies like data deduplication -- removing redundant files or blocks from data. For example, a client's mission-critical database may change by 20 MB each hour, but data reduction techniques can drop the effective volume to 8-10 MB each hour. WAN optimization appliances can also be deployed to apply compression for smaller

In this guide

file sizes and TCP/IP traffic assistance (e.g., fewer handshakes and jumbo packets) for lower latency and better bandwidth utilization. Solution providers may need to monitor or track application activity on the client's network to gauge the actual data types and volumes that require protection.

Next is the issue of time. "If you want 100% data replicated 24/7, then you need high bandwidth," said Rand Morimoto, president of Convergent Computing, a network solution provider in Oakland, Calif. "But if you are okay with a two- to four-hour delay or even one-day delay on DR, then you can get away with really cheap and simple WAN bandwidth."

Real-time synchronous data replication will demand bandwidth that matches the peak file change activity. For example, if data within the client's organization is changing at 1 MB each second during a normal business day, expect to provide at least 8 Mbps of bandwidth in order to move those changes in real-time. Asynchronous data replication needs can dramatically reduce these demands by spreading out data changes over a longer period. So if that same client organization changes 50 MB of data in the space of an eight-hour workday, and the recovery point objective (RPO) allows that data to be replicated over 16 overnight hours, they would only need about 0.007 Mbps for the overnight job -- an almost negligible amount of bandwidth. If that same 50 MB replication job had to be completed in three overnight hours, the client would need 0.037 Mbps of bandwidth.

In this guide

There are other considerations when determining WAN bandwidth needs. First, don't figure the initial data load into bandwidth calculations. The initial transfer of data always takes a significant amount of time. For example, moving 10 or 20 or 50 TB of business data to a new DR site is universally asynchronous -- possibly taking several days to complete. Second, always consider that the client uses WAN bandwidth for everyday business activity, so any WAN bandwidth for disaster recovery should be added to the current business WAN bandwidth.

"The bandwidth required for DR dwarfs any communications for pure networking," said Bob Laliberte, analyst with the Enterprise Strategy Group in Milford, Mass. "We'd go from a GigE link [for networking] to an OC48 link [for DR]." Don't include the current WAN bandwidth in the total predicted for DR -- otherwise the DR activity may impinge on regular WAN activity and possibly result in poor network performance or access problems for the client.

Some clients with asynchronous replication needs may save money on bandwidth by throttling bandwidth up (e.g., buying more bandwidth from their provider) during replication periods or opting to replicate during the evenings or other periods of off-peak user demand on the network. Finally, figure in some added WAN bandwidth for future growth. This provides the client with a small buffer that ensures they can still meet data movement objectives into the future even as data loads grow.

WAN connectivity and provider involvement

In this guide

In many cases, the WAN link itself presents a single point of failure that can cripple a disaster recovery plan, so solution providers are sometimes challenged to overcome this potential weakness by using multiple WAN providers. "There's a clear cost/benefit scenario that needs to be calculated out at this point," said Dave Sobel, CEO of Evolve Technologies, a solution provider located in Fairfax, Va. The goal is to determine client uptime requirements and how much data loss will affect them due to WAN connectivity problems. Ultimately, a solution provider needs to help the client determine if the cost of a second ISP is less than the cost (and risk) of downtime. It's not appropriate for every organization.

While a second ISP can help clients achieve a level of redundancy in their WAN connectivity, experts like Laliberte note that ISPs normally use local telecom providers for the "last mile" connection between the ISP and the client, and even multiple ISPs may ultimately use the same local provider's cabling and other infrastructure. "You really want to find out what the carrier has -- is it aerial fiber, is it buried, what COs are they going through?" Laliberte said. Consequently, the advice is to "do your homework." Understand each provider's cabling and infrastructure and opt for providers that do not share any common cabling or other resources if possible. This kind of separation may not always be possible, limiting your available site selections.

But the issue isn't just limited to local carriers. "We've seen WAN providers hub out of San Francisco or out of the World Trade Center locations go down and

In this guide

bring down an entire region, so it is important that the WAN provider be evaluated for their basic resiliency," Morimoto said, noting that potential outages can affect multiple data centers within that same region. Review each SLA carefully and be sure that the WAN provider is able to guarantee the level of service that your client needs.

Multiple WAN connections are often used simultaneously, aggregating the available bandwidth for improved throughput. But it's important to balance network traffic across aggregated WAN connections just as you would with aggregated (redundant) LAN connections. Otherwise one or more WAN links may be underutilized, resulting in wasted bandwidth. WAN link balancers like the Link LB family of appliances from Elfiq Networks or the Edge series of appliances from XRoads Networks are designed to accommodate multiple WAN links, but solution providers must weigh their cost to the client against the cost of additional bandwidth.

VPNs, virtualization and hosted services in disaster recovery

Any DR plan should include some consideration of data security. Client data must often be moved and stored in a secure manner. Virtual private networks (VPNs) ensure secure data transfers between two points, but they are primarily an end-user technology and not widely used to synchronize data between DR sites. For example, an end user may employ a VPN to recover a lost file from backup storage at a secondary data center or out-of-region recovery site, but solution providers won't connect the main data center and DR site across a

In this guide

VPN. "VPNs are one solution to that problem," Sobel said, noting that SSL encryption for on-the-fly security or other encryption products to secure data before it's sent to the DR site are often more effective alternatives to VPNs.

Virtualization also plays an indirect role in disaster recovery by simplifying the hardware requirements at both the data center and the DR site. "It's easier to DR 25 servers than 100 servers, so if you can consolidate servers and then virtualize them, the recovery process is greatly simplified," Morimoto said. DR hardware is also simplified. For example, DR sites traditionally had to duplicate hardware found at the main site. Virtualization removed this requirement, allowing protected data to reside on a diverse range of hardware -- reducing costs and providing the client with dramatically more deployment flexibility.

Finally, solution providers may wish to consider recommending hosted DR services for smaller clients. Solution providers that already have a DR services infrastructure -- or resell hosting services for a larger provider -- may have a revenue advantage over other providers that would have to refer hosting services to a third party.

Still, the use of hosted DR services can alleviate significant costs for the client. "It plays a big role if the org doesn't already have two or more internal data centers to be used, so it's good for small businesses," Morimoto said. Hosted services are not necessarily a good fit for organizations that already have two or more staffed data centers. In this case, it's probably better to implement high-availability DR, since the basic infrastructure is already in place.

In this guide

Staffing Skills

Building staff-related disaster scenarios for BC/DR exercise planning

http://searchdisasterrecovery.techtarget.com/tip/Developing-a-disaster-recovery-and-business-continuity-training-program

Developing a disaster recovery and business continuity training programt are the options for VDI training, and who needs it?

If Disaster recovery and business continuity training is one of the most important parts of the BC/DR planning process. Awareness of the BC/DR program is often included with training activities, as stated in international standard ISO 27031 Section 7.5, “A coordinated program should be implemented to ensure that processes are in place to regularly promote DR awareness in general, as well as assess and enhance competency of all relevant personnel key to the successful implementation of DR activities.”

In this article we’ll provide strategies and tips that will help you develop your own disaster recovery and business continuity training program.

In this guide

Disaster recovery and business continuity training program strategies -- What's unique for BC/DR

Let's begin with strategies and activities to raise awareness of a BC/DR program. First and foremost is to secure senior management support and funding for BC/DR programs, which will include training and awareness activities. Visible and frequently occurring endorsements from senior management will help raise awareness of and increase participation in the training program.

The next key strategy is to engage your human resources (HR) organization in the training process. They have the expertise to help you organize and conduct formal BC/DR training as well as awareness-creating activities, such as department briefings and messages on employee bulletin boards. Encourage HR to include training on BC/DR in new employee orientation programs. If it's possible to require all employees -- other than BC/DR team members -- to participate in at least one training session annually, that should encourage employee acceptance and reinforce the importance of BC/DR activities.

Another important strategy is to leverage the Internet. If your organization has its own intranet with employee web pages, introduce a BC/DR web page that describes what your overall BC/DR program does, and include sections on training, frequently asked questions (FAQs), and click-on links to forms and services, schedules and other useful materials.

In this guide

Finally, it's important to communicate the BC/DR program and its activities to employees. Communications should be informative, educational, and should reinforce the company's commitment to the BC/DR program.

Building a disaster recovery and business continuity training program

Here is a list of activities for building a successful disaster recovery and business continuity training and awareness program:

1. Conduct a training and awareness needs analysis
2. Prepare a training and awareness policy and have it reviewed and approved by senior management, BC/DR management, human resources and other key departments
3. Assess existing staff competencies and understanding
4. Define desired outcomes from the training and awareness program
5. Establish an ongoing training and awareness program
6. Develop training tools using needs analysis results as a starting point
7. Develop and deliver various types of training programs (e.g., classroom, computer-based, test-based and instructional guides and templates)

In this guide

8. Ensure that employees, customers, suppliers and other stakeholders are aware of the BC/DR program
9. Establish and use metrics to identify training focus areas, and measure progress in improving training quality
10. Identify internal and external trainers, validate their teaching credentials and arrange for appropriate train-the-trainer programs
11. Establish recordkeeping of staff training and awareness activities

Types of disaster recovery and business continuity training (differing from traditional business training):

1. How to perform a business impact analysis
2. How to conduct a risk analysis
3. How to write a BC/DR plan
4. Emergency response activities, e.g., assessment, evacuation
5. Specialized recovery activities, such as recovering to hot sites or cold sites, third-party managed DR services
6. How to initiate work area recovery

In this guide

7. Responding to unique situations, such as a pandemic
8. Coordination with first responder organizations
9. Return-to-normal activities
10. Restoration of business systems and processes

Tips for benchmarking a disaster recovery and business continuity training program:

1. Compare the BC/DR training program with other organizations
2. Periodically survey employees to determine their level of awareness
3. Apply lessons learned from actual disasters to training
4. Link training activities to annual performance review and compensation
5. Provide department managers with monthly status updates on all training and awareness activities
6. Examine BC/DR training programs in use by vendors and specialized service providers to see if they can be leveraged into your program

Summary

In this guide

The success of internal BC/DR programs often hinges on the training of BC/DR team members and employees. Include a well-designed training component in your BC/DR program to maximize the value of your BC/DR initiatives and to ensure that employees are ready to respond when the unthinkable happens.

Elements of a BC/DR training program:

1. Prepare an annual schedule of BCDR training programs
2. Schedule and conduct ongoing BC/DR training programs that address a variety of issues, such as what to do when an incident occurs
3. Educate management at all levels on how the BC/DR program works and what their roles may be during an incident
4. In addition to management staff, train BC/DR representatives in their duties and responsibilities during an incident, e.g., assisting with evacuations, coordinating the activation of BC/DR plans within their business units and ensuring post-event follow-up and review
5. Train BC/DR representatives on their duties and responsibilities during normal business operations, e.g., collecting relevant data for a business impact analyses and risk assessments, facilitating interviews with subject matter experts and business unit leaders, coordinating exercises within their office site and/or business unit

6. Develop and present educational and awareness materials that can be distributed to all employees; update the materials at least annually
7. Coordinate BC/DR awareness and training activities, such as classroom training and web-based training, with human resources, public relations and other departments
8. Evaluate training program effectiveness and update training materials on a six-month cycle
9. Coordinate training activities with employee professional development programs

Building staff-related disaster scenarios for BC/DR exercise planning

http://searchdisasterrecovery.techtarget.com/tip/Building-staff-related-disaster-scenarios-for-BC-DR-exercise-planning

Building a disaster scenario with staff offers a broad palette of possibilities. Situations where key employees are impacted by something -- e.g., an accident, sickness or death in the family -- can provide a realistic start to a scenario, and

In this guide

should be part of your business continuity/disaster recovery (BC/DR) exercise planning.

One of the primary concerns in many organizations is the loss of key staff, especially those with knowledge about mission-critical systems or processes. A good way to reinforce this important issue in your BC/DR program is for the scenario to focus on the sudden loss of more than one key person: A critical system suddenly fails, and managers realize that nobody else is trained in how to use it.

In today's world, active shooters are a real possibility, so introducing an employee who suddenly "goes rogue" may be an interesting parallel challenge to the scenario. Make the scenario more interesting in your BC/DR exercise planning by adding a series of either simultaneous or seemingly unrelated events to the mix. And it's always good to set up a "pause" in the scenario to make the participants think the scenario is over, when in fact much more is coming.

These BC/DR exercise planning scenarios focus on human-based scenarios, such as a disgruntled employee sabotaging an assembly line:

Scenario	Description	Importance
Disgruntled employee	While such events may	Someone who regularly

In this guide

sabotages a critical assembly line.	occur infrequently, they are always a possibility, especially where security may be lax, e.g., lack of security cameras in critical production areas.	works in a production area may, over time, identify potential weaknesses in the equipment and technology.
Employee enters critical process data incorrectly and fails to double-check the entry, and the resulting mistake causes a massive system outage.	Accuracy and care are two important criteria in any process-controlled environment; a simple keystroke could shut down a major system.	Improper entry of system commands and other coding is a potential problem; it may be necessary to build additional security challenges and checkpoints to minimize potential coding errors.
Social engineering helps a rogue employee obtain user access information which is sold to a third party to hack into	Social engineering can be very easy to do, given the use of partitioned cubicles and work areas. Laptops and workstations left on,	Unauthorized access to information is a key security challenge; social engineering must be included as a key part of

employee computers.	without being locked by the user, are prime targets for theft of information.	information security.
Union grievance causes key employees to walk off the job, causing slowdowns in order processing and fulfillment, and subsequent loss of business.	Relations with collective bargaining units can become disrupted; the outcomes of such situations, such as strikes and walkouts, could shut down a business.	Organizations that have unions must include this as a potential business-threatening situation.
Employee returning from an overseas trip contaminates other employees with an airborne human-to-human virus that sickens half of the staff.	This is difficult to address, in that the infected individual may not express the effects of the disease immediately.	Concerns about epidemics and pandemics (e.g., bird flu and swine flu) should be addressed in BC/DR plans because in each case it's a loss of people that affects the firm.

Member of IT security staff uses access privileges to steal intellectual property and sell it to a competing firm.	Despite careful screening of prospective employees, an employee could "go rogue" and use his access to steal information.	Employee-based situations should be factored into BC/DR exercises, not just situations involving a loss of technology or a natural disaster.

Create an employee succession plan for disaster recovery

http://searchdisasterrecovery.techtarget.com/tip/Create-an-employee-succession-plan-for-disaster-recovery

One of the most important questions to ask when developing a business continuity and/or disaster recovery plan is, "Who takes over if you're not available?"

Organizations of all sizes and types usually have one or more key employees whose loss could make it difficult or impossible for the organization to recover and resume business operations after a disaster. It is essential to not only

In this guide

identify these key individuals, but also to identify and prepare others to step in and assume all or most of their duties following a disaster.

Creating an employee succession plan with disaster recovery in mind is slightly different from a typical succession plan, which aspires to identify and groom employees who can be promoted into positions of greater responsibility upon the departure of senior managers. This article provides tips and a matrix for developing a succession plan for key employees other than executive management.

Organizing an employee succession plan

When launching a succession plan initiative, be sure to secure approval from your manager and then establish a partnership with your human resources department. HR should be able to help you organize your succession plan and may have relevant employee data that can identify existing skill sets and expertise. If HR doesn't have such data, it may be necessary to interview internal and external candidates for the succession plan. Once again, coordinate these activities with HR.

A business impact analysis (BIA) is an excellent way to identify key employees, because among the BIA's goals is to identify mission-critical business processes. When performing this activity, it's ideal to identify the employees who are currently performing those activities. Once you have identified the critical processes and employees who are responsible for performing them,

In this guide

coordinate with HR to identify other employees who possess the same or similar skills and perform comparable activities.

If no such employees are in the organization, it may be desirable to 1) hire new staff with the necessary skills, 2) train existing employees in the proper skills and/or 3) identify outside firms that can perform the tasks when needed.

Succession planning is often performed at executive levels in an organization, as replacing these executives may be a critical strategy to ensure the organization can sustain itself following a disaster. A key strategy of business continuity, therefore, is the creation of an employee succession plan.

The challenge is to take the succession planning process and perform it at non-executive levels in the organization. It's not uncommon to have mission-critical employees at almost all levels in an organization, not just at the top. A BIA can help identify these key players and their roles in the overall success and continuity of the organization.

Creating the skills matrix

If only one person performs a critical business process, this indicates a gap that needs to be addressed. If more than one person performs that process, it is desirable to identify *and document* all employees who perform the process. If only one person performs that process, work with human resources to identify one or more alternates who can back up the primary employee. Table 1

provides a sample skills matrix for identifying the necessary skills for a specific process and suitable candidates to perform it.

Begin by defining the mission-critical activity as identified in the BIA. Next, identify specific processes, tasks and/or activities that are needed to fulfill the requirements of the mission-critical activity. Identify suitable candidates who can perform the necessary processes to fulfill the mission-critical activity. In this example, Employee 1 is the person currently performing the key activity. An analysis of other candidates shows that Employee 2 has the highest number of required skills. Employees 3, 4 and 5 have some of the skills necessary.

Enter Name of Mission-Critical Activity	**Name of Employee 1**	**Name of Employee 2**	**Name of Employee 3**	**Name of Employee 4**	**Name of Employee 5**
Enter Critical Process 1	Yes	Yes	No	Yes	No
Enter Critical Process 2	Yes	Yes	Yes	No	No
Enter Critical Process 3	Yes	No	Yes	Yes	Yes

In this guide

Based on this assessment, you could say Employee 2 is the most likely candidate to back up Employee 1. It may be necessary to train Employee 2 with the skills to make that person *potentially* capable of replacing Employee 1 in an emergency. If the critical activity is sufficiently important to the organization, it may be necessary to train 1 or 2 additional employees to back up Employee 1 and 2. Once the employees have been trained, conduct exercises to ensure the alternate employees can perform the critical processes.

In addition, if it's possible, *document all steps of the critical process in detail* so it will be easy for alternate employees to follow the steps in performing the process in the absence of the primary employee.

As part of a succession plan, consider the value of cross-training employees. This means training employees in activities that are not their primary responsibility, but may be closely enough aligned with critical functions so that in an emergency, these employees can step in and assume the duties with minimal difficulty and time.

Pandemic planning and the employee succession plan

Infectious diseases, such as influenza, can affect people's lives and keep them out of work. Loss of staff due to illness caused by an outbreak of an infectious

In this guide

disease is a key business continuity concern. The loss of key employees due to an illness may be an even more serious threat to the business than the loss of systems or technology.

An employee succession plan is an important tool for keeping an organization up and running when employees are not healthy enough to perform their duties. It should not be limited to senior executives.

Next article

In this guide

Outsourcing

Building a DR site vs. Outsourcing disaster recovery

http://searchdisasterrecovery.techtarget.com/podcast/Building-a-DR-site-vs-outsourcing-disaster-recovery

A Depending on your business' continuity needs, it may be necessary to set up a secondary DR site. And with a remote DR site, your organization will have to decide whether to use a third-party vendor to provide DR service, or to build your own site. In our latest podcast, Paul Kirvan, an expert in the DR industry and board member with the Business Continuity Institute's USA chapter, explains some of the pros and cons of each option.

What are the pros and cons of building your own disaster recovery site versus contracting out the service?

One of the major challenges in disaster recovery planning is how to recover business operations to the point where business can be returned to as close to normal as possible following a disruptive incident. One of the popular strategies is to have an external site that can support business systems, applications and customer data until the primary data center can be returned to normal operation. Two approaches to this challenge are to build your own backup data center or

In this guide

similar facility and contract out for these services with suitably qualified third-party organizations. Key points in favor of building your own backup facility are management control of these specialized resources, utilization of them as alternate processing centers to handle heavy usage periods, security controls managed by your organization, and reduced likelihood of your data being intermingled with other organizations' data. Negative factors include start-up costs associated with building the facility, increased real estate costs and general overhead for the backup space, and costs for staffing the backup site. Points in favor of outsourcing disaster recovery include minimal or no start-up costs, shared costs of staffing and technology resources, managed security at the site and on-site expertise available 24-7. Downsides of a third-party solution include potential hidden costs or fees associated with declaring a disaster and potential unavailability of facilities if too many subscribers are already using the backup center. Among the key issues to address are costs (both upfront and ongoing), availability of resources (both human and technology) when needed, additional unplanned costs following a disaster, and contractual issues.

Define hot site, a cold site and warm site for the purposes of disaster recovery.

According to international standard ISO 24762, "Information technology - Guidelines for information and communications technology disaster recovery services" we can define these three important options as follows:

In this guide

A cold site is a type of data center which has its own associated infrastructure that includes power, telecommunications and environmental controls designed to support IT systems, applications and data which are installed *only* when disaster recovery plans are activated.

A warm site is largely a data center equipped with some or all of the equipment found in a working data center, including hardware and software, network services and supporting personnel, but *without* customer applications and data; these are introduced at the time when DR plans are activated.

Finally, a hot site is a fully equipped data center with the required equipment, computing hardware and software, and supporting personnel, *has* customer data and applications, and is fully functional and ready for organizations to operate their IT systems when DR plans are activated.

When designing the physical plant, is it enough that it is remote?

The proximity of a backup data center to the primary data center is an important initial design consideration. However, while a sufficient distance between primary and backup centers is key, it is also important to consider the impact of the distance between facilities on your staff. For example, members of your emergency recovery team may be reluctant to go to work at a significant distance for possibly an extended period of time. They may be concerned about their families or other issues.

In this guide

One of the critical design issues in building or selecting a backup facility is the source of commercial electric power. Often we are advised to find a location that is in a different power grid than the primary data center. While that is certainly desirable, it is not the only deciding factor.

Do you need to design it so it can resist natural or man-made disasters?

The first thing to do in this situation is to conduct a risk assessment of the areas in which a backup facility may be located. Carefully examine the surrounding region, its utilities, transportation, environment, weather and even crime rates. Review risk assessment findings to pinpoint areas with the least likelihood of disruptive events, knowing that it's still possible for the unexpected to occur. Any facility selected should be reasonably secure and have good physical and information security provisions to prevent unauthorized access. If you use an architect, be sure he or she has experience designing data centers and similar facilities.

How far away should it be?

A distance of 10 to 50 miles from the primary data center ought to be minimally acceptable, provided risk assessments of the prospective backup site locations are conducted. Always consider the impact of a remotely located data center on your staff, especially if it may be necessary for staff to relocate their place of work to a remote location for an extended period of time.

In this guide

Particularly when contracting for a DR site, should there be provisions in your agreement to practice a DR scenario with the site? Do vendors typically allow this?

Most third-party recovery site vendors encourage regular testing of the facility in accordance with a scheduled DR plan test. Ensure that your vendor will support at least one annual test of the facility. It's good if you can schedule more than one annual test, but this impact your DR budget.

What about mobile DR sites? We hear about some vendors parking a tractor-trailer with a portable data center in the back and using that. Is that a realistic option, or is a physical plant a better call, no matter what?

Mobile recovery solutions present an excellent alternative to fixed hot, warm or cold sites as well as building your own backup data center. Evaluate the costs for a mobile recovery solution based on what you think you will need in a disaster, remembering that the mobile trailer will probably need to travel some distance to your site after you have declared a disaster. Once the trailer has arrived, it will take time to set it up, and you will need to have provisions in place to connect power and communications to the trailer so it can begin functioning. Make sure the organization you contract with for such a service has a sufficient number of equipped trailers that your DR requirements can be satisfied. And make sure the firm has plenty of experience in disaster situations.

In this guide

Cloud disaster recovery offers data protection at low cost

http://searchcloudcomputing.techtarget.com/feature/Cloud-disaster-recovery-offers-data-protection-at-low-cost

Cloud disaster recovery and backup options have become more common, and some users say they provide a higher level of protection than traditional solutions -- at lower cost.

Disaster recovery (DR) means different things to different people. One IT pro's definition of DR might be simple file backup, while another might be referring to full standby server farms ready to take over production duties at a moment's notice.

At its most basic level, disaster recovery means storing backup data off-site, which increasingly means the public cloud.

For Prellwitz Chilinski Associates, Inc. (PCA), an architecture firm in Cambridge, Mass., nightly backups are the cornerstone of its disaster recovery plan. The data being backed up are large files architects generate using tools from vendors such as Autodesk Inc. and Adobe Systems Inc.

In this guide

For many years, PCA replicated its data between a pair of storage appliances provided by a local integrator -- one on-site, the other off-site.

"It was a great solution -- we had the local backups for quick access, plus the safety net of off-site backup," said Dan Carp, systems administrator for the firm.

Then, about two years ago, Carp began exploring whether cloud backup could be more cost-effective. Using the replicated data appliances, PCA paid about $14,000 annually to protect 700 GB of data. After a few fits and starts with various cloud data protection providers, it settled on Zetta.net, which stores almost twice the data it had on the data appliances, for about half as much money.

"I like to think of this as a life insurance policy -- I hope I never to have to use it," Carp said. But if that day comes to pass, users will access their files by copying them back to their systems, or by accessing them over the WAN at the Zetta.net data center.

Cloud backup for faster recovery times

Cloud backup is relatively simple, but recovering entire systems from the cloud leaves a lot to be desired, said Rick Vanover, product strategy specialist at backup and replication vendor Veeam Software.

In this guide

"Transferring a 200 GB file back down to your data center is not fun -- especially since you probably need it right now," he said.

Veeam Backup Cloud Edition software already supports backup to 19 different cloud object stores, including Amazon Simple Storage Service (S3), Amazon Glacier and Windows Azure, and Vanover said it is an increasingly popular backup target. However, upcoming versions of its software will also support a feature called Backup copy job with WAN acceleration, which allows administrators to pre-allocate known-good backup images on public cloud compute infrastructure, he said, for faster recovery times.

"You've effectively already put your backup infrastructure in the cloud," he said.

Indeed, backing up systems to the cloud is only half the battle, users say.

"Okay, so you've got your backup replicated to an offsite storage facility. Now what?" said Bryan Bond, a senior systems administrator with eMeter, a software development firm in Foster City, Calif.

The company recently began using the Recovery as a Service option from Bluelock, a cloud services provider based in Indianapolis. The service integrates replication software from Zerto Inc. to minimize the bandwidth and time necessary to copy virtual machine (VM) replicas to its environment. If and when disaster strikes, it spins those VMs up on the BlueLock Infrastructure as a Service (IaaS) simply by switching its DNS entries, Bond said. And because

Bluelock is based on VMware Inc.'s vCloud, it can do so without having to convert its VMware-based VM images.

Bond also explored "pilot light DR," in which a minimal version of an environment is left running in the cloud, ready to scale up and take over in the event of a disaster, but he ultimately decided that was overkill.

"As it is, the time it takes for us to return to operations is so short," he said. "Pilot light would have required us to re-architect our data to be aware of a cluster partner," using fancy networking techniques such as the Border Gateway Reservation Protocol (BGRP). "It's much easier to make a DNS change than it is to make the network complicated."

Weighing cloud DR options

IT professionals exploring cloud disaster recovery options have their work cut out for them, said John Morency, an analyst with Gartner Inc., a research firm based in Stamford, Conn.

"When I first began tracking this space five years ago, there were about five or six providers," he said. At last count, he had identified over 120 in the U.S. and offshore.

The viability of cloud-based DR services will depend greatly on the level of heterogeneity and support you need, he added.

In this guide

Compared with traditional DR services from the likes of IBM and SunGard Availability Services, cloud-based DR services give companies "the freedom to test as frequently as you want," Morency said. But for large enterprises with non-virtualized systems, "most cloud providers will not be able to support those configurations."

What are some roadblocks to cloud-based DR deployment?

http://searchdisasterrecovery.techtarget.com/answer/What-are-some-roadblocks-to-cloud-based-DR-deployment

When evaluating cloud-based disaster recovery (DR), the biggest challenge is that your application has to run in the cloud. For the most part, if you are talking about a mainframe application or a big box Unix application, those are not really compatible with the cloud. While you can do some very basic data parking and bring that data to another physical location in the event of a failure, you will not gain that much compared to shipping tapes.

Probably the biggest issue with cloud-based DR is compatibility and fit with the cloud. Once you have decided to send data to the cloud, you have to deal with data privacy and security issues. That may end up being a problem.

In this guide

If you can run a given disaster recovery application in the cloud, you must determine what you will gain from doing that. The nice thing about the cloud is that it is located somewhere other than your headquarters, which typically gives you geographic redundancy. Many cloud providers offer a dispersed form of geographic redundancy -- whenever you give them a byte of data, they will copy it many times to many different locations.

For companies that operate only one data center, the cloud is a nice way of getting access to geographic redundancy without spending the money to build multiple data centers that you might not need.

The importance of cloud recovery testing

http://searchdisasterrecovery.techtarget.com/tip/The-importance-of-cloud-recovery-testing

Brien Posey explains why it is extremely important to perform cloud recovery testing that simulates a real recovery following a catastrophe.

Regardless of the type of disaster recovery solution an organization uses, testing is essential. It would be a tremendous leap of faith to simply assume that a disaster recovery solution works as advertised and is configured correctly. Thorough testing is a must. The question is how to go about that testing.

In this guide

The only way to adequately protect your data is to have three copies. You need the original data, an on-premises backup (for quick recovery) and an off-premises (in this case, cloud-based) copy, so that you won't lose your backups if the data center is destroyed.

The reason I mention this is that this philosophy of data protection weighs heavily on the type of disaster recovery testing that you must do. If you are using the cloud as an off-premises backup solution to supplement your on-premises backups, then it usually means that routine restorations will be made from the on-premises backups. It also means that something must be really wrong if you are restoring from the cloud instead of from an on-premises backup. This could be something as simple as a bad tape, but it may very well be something of the magnitude of having your data center destroyed.

That being the case, it is extremely important to perform cloud recovery testing that simulates a real recovery following a major catastrophe. It is a good idea to do this testing from an isolated network segment, so that your production network is not visible to the recovery process.

There are a couple of reasons for doing this. First, you will want to make sure that the recovery testing does not in any way interfere with the production network. Second, following a real-world catastrophe, the resources on your production network wouldn't exist.

In this guide

The goal behind your first test is to determine what it actually takes to recover your data from the cloud. As you benchmark the recovery process, you might very well discover that bandwidth limitations make it impossible to recover data from the cloud quickly enough to adhere to your service level agreements.

Obviously, Internet access is a requirement, but, depending on how you have backed up and secured your data, there may be other requirements as well. For example, I once saw a situation in which an organization was unable to recover cloud data because they lacked the necessary digital certificates. Not every organization protects their cloud backups in the way that this particular organization did, but it is vitally important to find out if any external components are required to facilitate a recovery (such as a certificate authority) before a disaster actually strikes.

Once you have confirmed that you are able to recover data from the cloud, the next type of testing that I recommend doing is performance testing. When disaster strikes, your bosses and the organization's customers will demand to know how long it will be before service is restored. On-screen progress bars are notorious for being inaccurate. The only way to really know how long a recovery will take is to do benchmark testing.

As you benchmark the recovery process, try using a variety of data types, because cloud backups tend to rely heavily on deduplication. Deduplication helps data be transmitted over the Internet more quickly than it otherwise could be. The problem is that some types of data deduplicate better than others. As

In this guide

such, you will likely find that some types of data can be restored much more quickly than others. You can use your benchmark testing results to develop a plan for the order in which data should be restored in the event of a real emergency. You could perform the fast restorations first to get as many resources online as possible before delving into the longer duration restorations.

If recovery from the cloud is too time-consuming, then the next logical step is to look for ways to make the recovery process faster. Some cloud providers, for example, will ship you a copy of your data on tape or on a removable storage device in an effort to expedite the recovery process.

You should check with your backup provider ahead of time to determine whether they offer such a service, what the service costs are and what the turnaround time is for receiving a physical copy of your data. It is also a good idea to make sure that the data is in a format that you can actually restore. For example, it does no good to receive a tape containing a copy of your data if you don't have a tape drive that can read the tape.

As you work to test cloud-based disaster recovery, be sure to work through a variety of disaster recovery scenarios. For example, you might start out by testing your ability to do bare metal recovery, but you should also test application-level recovery, file and folder recovery, and infrastructure recovery. Infrastructure recovery involves recovering infrastructure components, such as the Active Directory, DNS servers, DHCP servers and enterprise certificate authorities.

In this guide

As you work through the various recovery types, you should be sure to document the recovery procedures, so that you don't have to resort to using trial and error during a real recovery. Different types of recoveries will inevitably require you to use different recovery procedures. Familiarizing yourself with and documenting these procedures will help to make the recovery process easier (and reduce the chances of making a mistake) in the event of a real disaster.

Conclusion

It is extremely important to verify the recoverability of your cloud backups before disaster strikes. The most effective way to accomplish this is through comprehensive testing that simulates a number of different disaster recovery scenarios.

Next article

In this guide

Planning for Deployment

Free disaster recovery planning templates

http://searchdisasterrecovery.techtarget.com/Disaster-recovery-and-business-continuity-planning-templates-Free-downloads

When it comes to creating and documenting business continuity (BC) and disaster recovery (DR) plans, it's necessary to expend a significant amount of time and effort. One potential way to ease this burden is to use disaster recovery or business continuity planning templates to help guide you through this process, which provide ready-made formats, layouts and containers for the various types of information you'll need to assemble and record during that process.

Disaster recovery templates can help with everything from preparing an IT risk assessment -- to mapping out the details needed in disaster recovery plans, such as key contacts information, step-by-step service resumption activities, delivery and recovery from off-site data backups and more.

We've compiled our best resources on disaster recovery and business continuity templates to help make your disaster recovery planning process easier.

In this guide

NETWORK DISASTER RECOVERY PLAN TEMPLATE

http://searchdisasterrecovery.techtarget.com/Network-disaster-recovery-plan-template

In this article and associated network disaster recovery plan template, we'll examine the issues that should be addressed when preparing and deploying a network disaster recovery plan for voice and data communications.

BUSINESS IMPACT ANALYSIS QUESTIONNARIE TEMPLATE

http://searchdisasterrecovery.techtarget.com/tutorial/Business-impact-analysis-questionnaire-template

In this tutorial on business impact analysis questionnaires, you'll learn why they are a key factor in the BIA process, what types of questions you should include and how many, and, finally, we've provided a business impact analysis questionnaire template to help you get started.

SERVICE-LEVEL AGREEMENT TEMPLATE

http://searchdisasterrecovery.techtarget.com/Free-service-level-agreement-template-for-disaster-recovery-programs

In this article, we'll examine the elements of an service-level agreement for BC/DR activities and also provide you with a free service- level agreement template to help you get started.

BUSINESS CONTINUITY POLICY TEMPLATE

http://searchsmbstorage.techtarget.com/Free-business-continuity-policy-template-for-SMBs

In this guide

This article and our free, downloadable business continuity policy template will provide a useful starting point for preparing a business continuity policy.

EMERGENCY MANAGEMENT PLAN TEMPLATE

http://searchdisasterrecovery.techtarget.com/tutorial/An-emergency-management-plan-template-for-business-continuity-planning

In this tutorial, we'll examine what's needed to prepare an emergency management plan that addresses not only the initial incident response but also the longer term support needed to manage the emergency to a suitable conclusion.

DR PLANNING FOR YOUR HELP DESK: A HELP DESK TEMPLATE

http://searchdisasterrecovery.techtarget.com/Disaster-recovery-planning-for-your-help-desk-A-help-desk-template

In this article and associated help desk template, we'll examine the issues that should be addressed when preparing and deploying a disaster recovery plan for a help desk.

INCIDENT RESPONSE PLAN TEMPLATE

http://searchdisasterrecovery.techtarget.com/Free-incident-response-plan-template-for-disaster-recovery-planners

It's important to have an incident response plan in addition to your regular disaster recovery plan. Incidents are situations that could turn into a disaster if not handled properly, and are often the first step in detecting a disaster. When an out-of-normal condition in your organization occurs, it must be acknowledged

In this guide

as quickly as possible, assessed as to its nature and severity, and some sort of response initiated.

SAMPLE BUSINESS CONTINUITY TEMPLATE FOR SMBS

http://searchsmbstorage.techtarget.com/Sample-business-continuity-plan-template-for-SMBs-Free-download-and-guide

For many small- to medium-sized businesses (SMBs), business continuity planning activities pose a formidable challenge, especially from the perspectives of time, money and resources. We've tried to simplify this process for SMBs in this guide and free template.

VOICE COMMUNICATIONS DISASTER RECOVERY TEMPLATE

http://searchdisasterrecovery.techtarget.com/Voice-communications-technology-disaster-recovery-planning-template

In this guide, you'll learn how to keep your voice communications up and running in the event of a disaster, how to write a voice over IP (VoIP) disaster recovery plan, and then you can download our free template and get started.

EMERGENCY COMMUNICATIONS PLAN TEMPLATE

http://searchdisasterrecovery.techtarget.com/Developing-an-emergency-communications-plan-A-template-for-business-continuity-planners

The business continuity management process contains several important steps. Communicating information during and following a disaster to relevant parties is a key priority. In this guide, we will examine an emergency communications plan for business continuity planners, and then you can download a template to help

In this guide

you with your emergency communications planning that can be adapted to a variety of incidents.

DATA CENTER DISASTER RECOVERY PLAN TEMPLATE

http://searchdisasterrecovery.techtarget.com/Data-center-disaster-recovery-plan-template-and-guide

A data center disaster recovery plan focuses exclusively on a data center facility and its infrastructure, e.g., physical location, construction, security, power sources, and environmental systems. In this guide on data center disaster recovery planning, learn about the most important ingredients in a successful data center DR plan, who should be involved in the planning process, and how to get started.

DISASTER RECOVERY TEMPLATE FOR ASSESSING YOUR DISASTER RECOVERY SITE

http://searchdisasterrecovery.techtarget.com/A-free-disaster-recovery-template-for-conducting-a-physical-assessment-of-your-DR-facilities

A key activity in business continuity (BC) and disaster recovery (DR) planning is a disaster recovery facilities assessment. This physical site assessment goes through an extensive checklist of building elements, such as power and heating, ventilation and air conditioning (HVAC), and identifies situations in which a risk may be present.

In this guide on disaster recovery facilities, learn what should be covered in a disaster recovery facilities assessment, how to perform one and then download

In this guide

our free disaster recovery template to help you conduct a physical site assessment. You'll also learn what areas should be covered in an assessment, and key building

RISK ASSESSMENT TEMPLATE

http://searchdisasterrecovery.techtarget.com/Risk-assessments-in-disaster-recovery-planning-A-free-IT-risk-assessment-template-and-guide

In this guide on risk assessments in disaster recovery planning, learn how to get started with a risk assessment; how to prepare a risk assessment; and natural vs. man-made hazards in the risk assessment process.

DISASTER RECOVERY TEMPLATE FOR YOUR BUDGET

http://searchdisasterrecovery.techtarget.com/A-disaster-recovery-budget-template-A-free-download-and-guide

To help make your budgeting process easier, SearchDisasterRecovery.com has provided a free downloadable disaster recovery template that will help you get started with your budget.

PANDEMIC RECOVERY TEMPLATE

http://searchdisasterrecovery.techtarget.com/Using-a-pandemic-recovery-plan-template-A-free-download-and-guide

Pandemic plans differ slightly from traditional disaster recovery and business continuity plans in that they focus more on people and somewhat less on technology. Each type of plan provides a structured approach for responding to situations that threaten an organization's ability to sustain operations.

In this guide

Considering the health threat to employees from by a pandemic, a carefully designed pandemic recovery plan can help the firm remain viable, even with a reduction of staff.

USING DR AND BC TEMPLATES

http://searchdisasterrecovery.techtarget.com/tip/Using-disaster-recovery-business-continuity-templates#usingDRandBCtemplates

As you use disaster recovery and business continuity planning templates, don't forget to think outside the box. That is, you'll want to make sure you've covered everything that's relevant to your organization's disaster recovery or business continuity efforts, rather than just following somebody's blueprint unthinkingly. That's why a good shakedown from a recovery practice drill is so important to vetting all such plans, whether they derive from a template or not.

IT DISASTER RECOVERY TEMPLATE

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

An information technology disaster recovery plan provides a structured approach for responding to unplanned incidents that threaten an IT infrastructure, which includes hardware, software, networks, processes and people. Protecting your firm's investment in its technology infrastructure, and protecting your firm's ability to conduct business are the key reasons for implementing an IT disaster recovery plan. SearchDisasterRecovery.com's free

In this guide

downloadable IT disaster recovery template will help facilitate the initiation and completion of an IT DR plan.

BUSINESS CONTINUITY AND DISASTER RECOVERY TESTING TEMPLATES

http://searchdisasterrecovery.techtarget.com/feature/Business-continuity-and-disaster-recovery-testing-templates-A-free-download-and-guide

Business continuity and disaster recovery plans are useless until you test them. Fortunately, many types of disaster recovery tests are possible, ranging from simple to very complex. The key to business continuity testing success is to incorporate testing as part of the overall business continuity/disaster recovery management process.

But testing can be a major challenge to many organizations. They require management support, time for preparation and execution, funding, careful planning and a structured process from pre-test through test and post-test evaluation.

SearchDisasterRecovery.com has created a free business continuity testing template and guide to show you how to build and execute your test

A BUSINESS IMPACT ANALYSIS TEMPLATE

http://searchdisasterrecovery.techtarget.com/feature/Using-a-business-impact-

In this guide

analysis-BIA-template-A-free-BIA-template-and-guide

A business impact analysis is a key part of the business continuity process that analyzes mission-critical business functions, and identifies and quantifies the impact a loss of those functions (e.g., operational, financial) may have on the organization.

SMALL BUSINESS DISASTER RECOVERY PLANNING TEMPLATE

http://searchsmbstorage.techtarget.com/Sample-business-continuity-plan-template-for-SMBs-Free-download-and-guide

To make the disaster recovery planning process easier, we've collected our top five resources on business continuity planning for SMBs, starting with a free, downloadable business continuity plan template. Explore our resources on small business disaster recovery planning.

Disaster recovery planning guide for the midmarket

http://searchcio.techtarget.com/Disaster-recovery-planning-guide-for-the-midmarket

This CIO Briefing is part of the SearchCIO.com CIO Briefing series, which is designed to give IT leaders strategic guidance and advice that addresses the management and decision-making aspects of timely topics. For a complete list of topics covered to date, visit the CIO Briefing section.

In this guide

Business execs undercut value of DR planning

When it comes to disaster recovery, CIOs get it -- business execs don't.

Not only do they undercut the importance of such planning, but they also fail to understand how technology failures can affect their companies, says a new survey conducted by Harris Interactive Inc. and sponsored by SunGard Availability Services.

Seventy-one percent of IT executives identified business continuity and disaster recovery planning as very important or crucial to business success. Only 49% of business executives felt that way.

"I'm a little surprised that overall, businesses are still lagging," said Mark McManus, vice president of IT research at Computer Economics Inc. in Irvine, Calif. "The idea of disaster recovery was always an IT process, but it has really morphed into business continuity, which is an overall company process more than just IT. In many businesses, business continuity isn't even controlled by IT."

Learn more in "Business execs undercut value of disaster recovery planning." Also:

- **Remote backup: Making the business case to your CEO**
  CIOs are being forced to take a closer look at their remote backup plans

as they staff more off-site workers and face continual compliance concerns.

Outage brightens outlook on virtualization

LAS VEGAS -- When a series of electrical snafus took down the Las Vegas Valley Water District's (LVVWD) data center, its network administrators were vindicated. Yes, server virtualization really is a good idea.

Senior network administrators Dave Trupkin and Greg Hearn told attendees at Gartner's Data Center Conference that they had begun converting a select number of the utility's 200 servers to virtualized servers in the years prior to the power failure to combat server sprawl.

Trupkin had virtualized some infrastructure servers, installed two VMWare ESX host servers and introduced VMotion, which allowed him to move virtual servers from box to box with almost no downtime.

As virtualization improved performance, Trupkin thought the results would increase acceptance of the technology in his organization. But the utility's developers were slow to do so. Every problem the developers had was now a virtualization problem, whereas before it would have been an application problem, Trupkin said.

"We still didn't have full acceptance of VMWare," Trupkin said.

"Until we had the disaster," Hearn added.

Find out what happened in "Power outage brightens Las Vegas utility's outlook on virtualization." Also:

- **A 13-hour power outage puts disaster recovery plan to the test**
  When a blown electrical transformer left his data center in the dark and 30% of his company's employees cut off from their offices, CIO Richard Ridolfo put his new disaster recovery plan to the test.

- **Disaster recovery: Test, test and test some more**
  Storage managers in New Orleans thought their disaster recovery (DR) plans were solid. Hurricane Katrina showed them otherwise. These dramatic stories are testimony that a DR plan is worthless unless it's been tested, updated and then tested again.

CIOs not making time for business continuity

Many midsized to large companies have no business continuity plan. But it's not because they don't see the value in it.

They just can't seem to get around to doing it.

According to a survey sponsored by hardware and software vendor Hewlett-Packard Co., 55% of respondents said their companies couldn't agree on a technology solution for business continuity. Forty-nine percent said they simply

didn't have time to plan. A lack of experienced internal resources was cited by 59% of respondents, and 34% said they lacked the data needed to make a business case for implementation.

Palo Alto, Calif.-based HP surveyed 564 IT decision makers at large and midsized companies.

Learn more in "CIOs not making time for business continuity planning." Also:

- **Gartner: Existing business continuity plans will fail in a pandemic**
  Existing business continuity plans will not protect a company during an avian flu pandemic, says a Gartner analyst. Business continuity plans assume a geographically specific disaster, while a pandemic will strike everywhere nearly simultaneously.

- **Business continuity planning standards and guidelines**
  An excerpt from Chapter 1: Contingency and Continuity Planning of "Business Continuity and Disaster Recovery for InfoSec Managers," by John W. Rittinghouse and James F. Ransome.

Taking control with archiving

Though some say e-discovery is the chief driver of archiving system adoption, there are many reasons to use the technology, such as freeing up storage space, improving system performance and providing for disaster recovery.

In this guide

At the Barbara Ann Karmanos Cancer Institute in Detroit, CIO George Yacoub has to contend with the ever-growing volume of email in a Microsoft Exchange environment. "We have a lot of researchers who do most of their correspondence via email," Yacoub says. "The pressing issue for us is that users are running out of disk space." He recently deployed an archiving system from EMC Corp. to help manage storage and prevent the hospital's 1,700 end users from pushing inbox capacity -- currently 250MB -- to the limit.

Find out what role disaster recovery planning played in "Taking control with archiving." Also:

- **Unified messaging: A beneficial part of any DR plan**
  Many companies are implementing unified messaging solutions as part of their disaster recovery plans. Experts agree that a consolidated messaging environment can dramatically improve the rebuilding process after a disaster.

- **Force majeure meets disaster recovery**
  Don't let a contract's force majeure clause excuse your vendors from disaster recovery responsibilities.

DR plans for your data warehouse

In this guide

When was the last time you reviewed and tested the business continuity and disaster recovery plan for your data warehouse? Do you even have a disaster recovery plan for your data warehouse?

While natural and geopolitical disasters -- including tornadoes, thunderstorms and increases in oil prices -- are on the rise, they are not the biggest threats to your business intelligence (BI) environment. According to research by *Information Age*, a leading U.K. magazine for executives, most IT executives believe the greatest threats to the continuity of their IT operations are internal system failure (65%) and viruses (45%). Meanwhile, natural disasters registered at 32% and power and communications outages at 33%.

Ten years ago, there was little need to create a disaster recovery plan for data warehouses and the reports and applications they support. At the time, the vast majority of data warehouses were loaded in batch on a monthly basis from a half-dozen or so source systems. Most loads were fairly small and even the biggest data warehouses were less than a couple of hundred gigabytes in size. Not surprisingly, most data warehousing teams didn't have a disaster recovery plan, let alone a backup strategy. The common sentiment back then was that if the data warehouse crashed, you could simply refresh the data warehouse in its entirety from source systems once everything came back online.

Learn more in "Disaster recovery plans for your data warehouse." Also:

In this guide

- **Disaster recovery plans: Points to consider**
  A comprehensive disaster recovery plan is critical to surviving a crisis, especially in an SMB environment. But evaluating your disaster recovery needs is no small task. This tip explains what to consider when designing your disaster recovery strategy.
- **Disaster recovery plans: Best integrated into daily operations**
  Expert Russell Olsen explains how to define your IT universe, the first step in developing a solid disaster recovery plan.

Next article

In this guide

Calculating ROI

http://searchdisasterrecovery.techtarget.com/podcast/Getting-management-buy-in-for-your-disaster-recovery-policy

Getting management buy-in for your disaster recovery policy

This was the first in an ongoing series of podcasts we'll be recording with the BCI, which will cover a wide array of topics of interest to BC/DR professionals.

Click here to listen to the podcast on getting management buy-in for your disaster recovery policy, or read the transcript below.

One of the biggest challenges we hear about from our readers is selling business continuity and disaster recovery planning to management. First off, why is that? With disasters all over the news, wouldn't you think it'd be an easy sell?

Somehow, over the years, business continuity and disaster recovery have acquired the reputation of being investments with minimal or no real return. I'm still trying to figure those things out myself. But, for example, it's not uncommon for organizations to make significant investments in programs and plans that may never actually be used—that is a real issue. But you can make a claim that companies buy insurance to protect them, shouldn't business continuity perhaps be considered a type of insurance?

In this guide

Disaster recovery evolved from the IT world, and it is perceived as an IT activity, although it can very easily reside in other departments in the organization, such as an audit function, a risk management function (or) even part of a management department. Business continuity evolved from DR, and differentiates itself (because) DR takes a larger, more holistic view of the entire enterprise—not just systems, networks, data and people, as disaster recovery would do.

Both are important business activities. So we have an interesting dilemma: Business continuity professionals are rarely both experts in the profession and salespeople. So we are good at what we do, but not necessarily good at making that known to the right people in an organization. And our difficulties selling business continuity and disaster recovery is probably one reason that we have difficulty getting senior management to agree to business continuity/disaster recovery programs.

What are the most important things to address when presenting the need for BC/DR investment to management?

Once you've been able to get an audience with a senior executive or a group of senior executives, perhaps a steering group or something like that, business continuity professionals have to fully understand the organization, how it operates, the risks the organization faces, the vulnerabilities that may exist, both internally and externally, and the organization's fundamental strengths and weaknesses.

In this guide

Business continuity people need to be able to communicate that knowledge to senior management, and do it in such a way that management can acknowledge and accept the risks as well as the potential remedies available to them, such as a business continuity activity. Once they accept this, they ought to be better prepared to approve investments in business continuity and disaster recovery activities. Senior management must be aware that risks exist, threats and vulnerabilities exist, and they are ultimately responsible for ensuring the organization can what I like to call anticipate, prevent, mitigate and recover from unplanned events. And the better that we—as business continuity professionals—are able to help senior management understand those situations, the better our chances are of getting our programs approved.

Are there any overlaps with other aspects of business where BC/DR can be addressed in a streamlined manner?

One of the things I've learned over the years is that when you present business continuity to management, you got to make sure it's defined in the context of the entire organization. Don't be too focused on one piece of it, (such as) the IT organization, or whatever.

It is also important to align BC with governance, risk and compliance (GRC) activities, because these activities, among others, are also the responsibility of senior management. And again, this is one of those situations that sometimes doesn't happen with business continuity. GRC are recognized and accepted—by and large—by senior management. So business continuity probably should

In this guide

position itself as a fourth issue, to address with GRC. At some point in time, an unplanned disruptive event can occur, and GRC activities will not necessarily be able to respond to such an incident, whereas a business continuity program will be able to respond. So that's why we like to think that business continuity is yet another important part of the overall GRC activity.

Do you have any tips for getting additional stakeholders on the same page?

One of the things that seem to work if you can make it happen is to somehow get people throughout the organization to think about business continuity, what we like to think of as embedding business continuity into the corporate culture of an organization.

Most organizations—whether they're two or three people, or 100,000 people—have some sort of fundamental culture in terms of how the company operates and how people interact with each other. So given that, business continuity professionals need to reach out to all members of the enterprise, especially enterprise management team members. Now, doing this requires not only outreach to internal management, but also to external stakeholders such as investors and key vendors.

Business continuity professionals need to have a clear, concise message about the risks facing the enterprise and, stepping forward, how a business continuity program can prevent, mitigate and recover the enterprise from disruptive

events. Now if we take that to a technology perspective, a business continuity professional's message can include—and should specify—proactive measures in place that protect and recover critical systems and data. But ultimately, business continuity people need to be a visible, active, engaged part of the enterprise so that they can continually send out and reinforce the message that business continuity is an important part of the organization and its culture.

Next article

Budgeting

http://searchdisasterrecovery.techtarget.com/A-disaster-recovery-budget-template-A-free-download-and-guide

A disaster recovery budget template: A free download and guide

Putting together a disaster recovery (DR) and business continuity (BC) budget can be time-consuming and complicated if you haven't done it before. Most find it difficult because they either don't know how to manage the budgeting process, or they focus too much on each budget item.

In this guide on disaster recovery budgets, learn how to manage DR and BC costs, who should fund DR and BC programs, and how to convince management you need more money for DR and BC planning.

To help make your budgeting process easier, SearchDisasterRecovery.com has provided a free downloadable disaster recovery budget template that will help you get started. Download our disaster recovery budget template, and check out the rest of our IT disaster recovery budget planning guide.

Next article

In this guide

Expert Tips and Advice

Disaster recovery checklist for new building owners
http://searchdisasterrecovery.techtarget.com/answer/Disaster-recovery-checklist-for-new-building-owners
Independent DR expert Paul Kirvan offers a disaster recovery checklist for new building owners in this Expert Response.

DR/BC planning for an older building
http://searchdisasterrecovery.techtarget.com/answer/DR-BC-planning-for-an-older-building
A discussion of specific considerations for disaster recovery and business continuity planning in an older facility.

Obtaining flood insurance for a data center in a flood zone
http://searchdisasterrecovery.techtarget.com/answer/Obtaining-flood-insurance-for-a-data-center-in-a-flood-zone
What steps you should take when investigating flood insurance options for a data center located in a flood zone?

Evaluating emergency power supply options
http://searchdisasterrecovery.techtarget.com/answer/Evaluating-emergency-power-supply-options
Independent disaster recovery consultant Paul Kirvan discusses what you should consider when evaluating emergency power supply options.

Five things you must do before a hurricane to protect your business
http://searchdisasterrecovery.techtarget.com/answer/Five-things-you-must-do-before-a-hurricane-to-protect-your-business

In this guide

Paul Kirvan lists five disaster-preparedness things you must do in the days leading up to a hurricane to protect your business.

Five essential DR tasks for hurricane preparation
http://searchdisasterrecovery.techtarget.com/answer/Five-essential-DR-tasks-for-hurricane-preparation
Brien Posey outlines five hurricane preparation steps to take if your organization does not already have a formal DR plan in place.

Protecting contact/call centers
http://searchdisasterrecovery.techtarget.com/tip/Protecting-contact-call-centers
A smooth call-processing flow is vital to the productivity of your contact/call center. Use these three tricks to help minimize interruptions.

Defining BC/DR strategies and responses
http://searchdisasterrecovery.techtarget.com/tip/Defining-BC-DR-strategies-and-responses
Paul Kirvan shares tips on how to translate business continuity and disaster recovery strategies into specific action steps.

Next article

In this guide

Getting more PRO+ exclusive content

This e-guide is made available to you, our member, through PRO+ Offers—a collection of free publications, training and special opportunities specifically gathered from our partners and across our network of sites.

PRO+ Offers is a free benefit only available to members of the TechTarget network of sites.

Take full advantage of your membership by visiting http://pro.techtarget.com/ProLP/

Images; Fotalia