Online Backup Guide for Service Providers
How to Start and Operate an Online Backup Service
By Rob Cosgrove

New and updated, the *Online Backup Guide for Service Providers* is a complete guide on starting and operating an Online Backup Service – the latest revision of Rob Cosgrove's industry defining *RBS Book* originally published in 1987.

TABLE OF CONTENTS

AND

SAMPLES

Buy the full electronic version at http://remote-backup.com

The printed trade paperback will soon be available at Amazon.com.

Contents

What is Online Backup?

I know, this seems like a chapter you could skip. After all, everyone knows what Online Backup is. Right? Read this anyway. I'm going to also tell you what your customers expect from you, and what Online Backup is NOT.

At its core, Online Backup means making a copy of data on a geographically distant computer for the purpose of protecting the data from loss like accidental erasure, hardware failure, computer theft or destruction. In the event of a loss, the backup copy can be restored.

There are several features of Online Backup services that the public have come to expect. All Online Backup services operate over the Internet. Some, like the kind that can be operated by RBackup software, can also support local networks, direct connections, and even telephone modems.

These are the most important requirements for all Online Backup customers – Personal and Business. These are the features they demand in a Service.

Personal and Business Requirements

Privacy – Users expect privacy. They don't want anyone else to see their data, either in transit across the Internet, or at rest on the backup servers. This is the most critical concern of online backup customers.

Encryption – Data should be encrypted before it is sent across the Internet, and it should be stored in its encrypted state. Encryption should be at least 256 bits, and the user should have the option of using his own encryption key, which should never be sent to the Server.

File-by-File Restore – Users want to be able to restore files themselves, without assistance from the Service Provider. So, the service should provide at some kind of simple restore procedure that at least lets users select files by name and/or folder. More advanced services (like RBackup and Mercury) also allow users to select files by searching for parts of filenames and folder names, by dates, by file type, by Backup Set, and by Tags.

Easy File Selection – NO file selection would be better. End users do not usually know which files need to be backed up. So, the online backup service should be capable of pre-selecting the most common file types and locations, discovering which files are used the most often, and automatically backing them up. It should also give the user some way to edit its selections.

Automation – End users want to set it and forget it. They want the Online Backup service to simply work. They often don't want to see progress screens, and they don't want to have to push a button to start a backup. The service should simply back up their files without any questions, and without any user intervention. This is easier said than done, and in the real world, may not be practical in all applications.

Web Access – Users want to be able to access their backed-up data from a web browser anywhere on the Internet, in case they are away from their computers and they need a copy of a file.

Reliability – The Service should work day-in and day-out, without failure. Users come to rely on their online backup service and unless they are told otherwise, they assume it is working.

Exception Reporting – If something goes wrong with a backup, the user needs to be alerted by an on-screen message and an email. Email alone is not adequate for exception reporting, since email does not have a guaranteed delivery. In the best online backup services, someone at the Service monitors all accounts and also gets a notice.

Ease of Installation – Some Online Backup services (who charge more than $5/month) offer to install the Client (or Agent) software either in person or by remote control. Customers *love* this kind of personal service, and are willing to pay for it – especially business customers. If you don't intend to install the software, customers will expect to be able to go to a website, pay for the service, download the software immediately, and start backing up. Some Service Providers sell CDs. Some pre-install their software on new computers, and on computers brought in for repair.

Business Requirements

In addition to these over-all expectations, business customers have some additional requirements.

Server Backup – Business customers expect their Online Backup service to be able to back up Windows Servers, and the special databases that run on them. This includes MS Exchange (Brick Level), SQL Server, Active Directory, System State, and open files.

Multiple Versioning – Businesses require that their Online Backup service keep multiple versions of their files at different points during their development so they will be able to roll them back to a point in time. The bookkeeper might want last month's copy of a spreadsheet. A virus might have infected the network on June 8, and the customer needs virus-free copies of his files from before then.

Flexible File Retention Policy – Some files need to be kept for up to ten years, while others can be deleted after ninety days. Some don't require deletion after a specific age, but

should be deleted after a number of versions. Business customers need a service that offers a flexible file retention policy that can be applied to an unlimited number of groups of files called "Backup Sets."

Regulatory Compliance – Some business customers are required to comply with government regulations that govern privacy, disclosure, and legal discovery. For example, Healthcare Providers are required to conform to HIPAA (see the chapter on HIPAA). Others are required to comply with Sarbanes-Oxley (SOX), Gramm-Leach-Bliley (GLB) and more. Different countries have different regulations. Since Online Backup services handle the data covered by these regulations, they must assist customers with proper compliance with the laws.

Centralized Management – Larger business customers might have an IT department, or at least one IT person on staff, whose job it is to manage the computers. He might also want to manage the online backups. So, some business customers want a centralized management console that can control and monitor all the backups for the company.

Fully Managed Service – Business customers demand a much higher level of service than Personal customers. They may expect to be able to phone in a support request and get immediate help, sometimes in the form of a personal visit by a technician. They will want their backups monitored proactively, and they will expect far more functionality and flexibility in their Service than Personal users do.

Redundancy – Some business customers want multiple copies of their backed-up data at different locations. This requirement might be satisfied by having two or more mirrored data centers, or by keeping a local copy of the latest version of backed up data on site with the business.

Accepted Encryption Technology – Blowfish is a great encryption technology. It is fast and very secure – up to 448 bits. However, it is not government-approved. Some businesses (like banks and brokerages) require the use of a "standard" encryption technology like DES or AES. RBackup supports six "standard" encryption technologies as well as Blowfish.

High Security Data Centers – Business customers are more conscious of the features of the online backup data center than personal customers are. They may require redundant Internet connections, biometric security, armed guards, backup generators, backup air conditioning, special fire suppression, redundant alarm systems, earthquake-proof buildings, and video monitoring.

Bulk Loading – Many business customers have large amounts of data that would make the first backup too big to go over the Internet. Of course, subsequent backups are smaller. But that first one can be huge. These customers will want to send their first backup on a portable USB drive rather than online. RBackup fully supports Bulk Loading.

Bulk Restore – Like Bulk Loading, full restores (while rarely needed) might take too long to do over the Internet. So, there should be a way to restore data from a portable USB drive instead. RBackup also supports Bulk Restore.

(CONTINUES)

How do I Compete With $5/Month Services?

*Y*ou see them everywhere – advertisements for companies like Mozy and Carbonite who offer to back up your personal computer for $5 a month, often offering "unlimited" storage space. So, how does a small Online Backup company compete? The answer is: Don't.

As a small <u>Online Backup Service</u> Provider with fewer than 1,000 accounts, you most likely cannot afford to sell services to home users for $5 a month unless you are using my Mercury service; nor should you want to.

If you have 5,000 or more accounts, then of course the economy of scale works in your favor. With the right plan and the right marketing, you might be able to profitably approach $5/month and address the home market. But let's just say for the sake of this discussion, you have fewer than 250 accounts.

250 accounts at $5/month would gross out at $1250 a month, or $15,000 a year. I don't know about you, but for the trouble of giving 250 customers an adequate level of service while maintaining your equipment and trying to turn a profit, I am not at all interested in this business. I'm not even interested at $10/month, or $15/month.

However, at $19.99 a month I'm bringing in $60,000 a year and beginning to show a little interest. At $29.99 a month I'm making $90K; and at a very reasonable $89.99 a month for the kind of business-class service I can offer with *RBackup*, I am VERY entertained by a $270,000 a year from my loyal group of 250 small business customers.

Now, please understand that I am not trashing the $5/month services. In high enough numbers, or with Mercury, $5/month can make money.

In a "Fireside Chat" sponsored by Future Forward (<u>FutureForward.com</u>) on Nov 23 2008 David Friend, CEO of Carbonite (one of the $5/month services) said that he has more than 15 billion files in storage. He spends about $50 to acquire each new customer, and charges $49.95 per year for his service. He says he keeps each customer for 4.5 years, so, David is paying $50 for $225. Hey, I'll do that all day long, no problem.
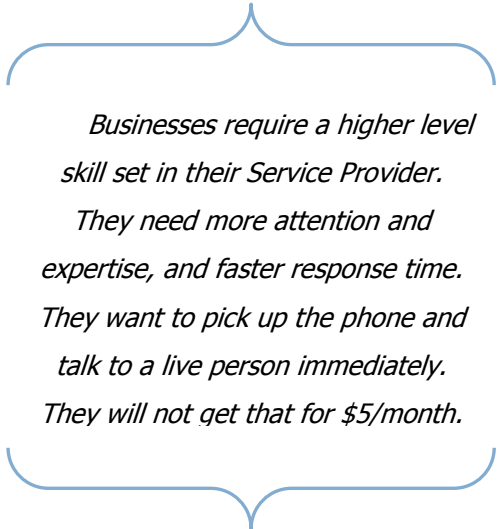
In a response to a blog posting asking how he knows how long he will keep a customer, David shows he's smarter than I am by explaining the following:

"In a recurring revenue business like Carbonite (or Netflix, or any subscription business) you estimate the lifetime of a customer based on the percent of people who renew at the end of each year. If 80% of your customers renew after one year, your average customer will be with you for about 4.1 years. If the renewal rate is 90%, then the average customer will be with you for 7.6 years. And so on. You don't have to wait until the end of four years to know what your average customer lifetime is. You know it after one year, assuming nothing changes in the future."

David says he spends a million dollars a month (as of this writing) on advertising. So, at $50 per customer, and discounting referrals, Carbonite must be signing up more than 22,000 customers a month, none of whom have dropped the service.

Recently, Dave announced an IPO plan that should take place in 2011. He wants to raise even more money for advertising so he can become the "Symantec of Online Backup." (His words, not mine)

Now, David is a smart guy with many successes under his belt. He has been able to attract sixty seven million dollars in venture capital for Carbonite. So, not only does Dave believe in $5/month services, so do a lot of other smart people with a lot of money.

Businesses require a higher level skill set in their Service Provider.
They need more attention and expertise, and faster response time.
They want to pick up the phone and talk to a live person immediately.
They will not get that for $5/month.

(CONTINUES)

Recovery Objectives

*M*ost small businesses that buy Online Backup services don't know the right questions to ask. However there are some things they should consider. Depending on the way you do business, you may want to use these in your Service Level Agreement or competitive marketing.

RTO – Recovery Time Objective - What is the acceptable amount of time between the loss of data and its recovery? If it is too much data (because of bandwidth) to download from a service based out of the area, and the service is too far away to deliver a USB drive to the customer, you have an advantage by being close enough to your customer to make the RTO very short.

RPO – Recovery Point Objective – The amount of data a business is willing to lose, in hours or days. If a business does not keep paper records of all transactions, it may never be able to recover data that is lost between backups. Can the staff enter a week's worth of transactions from memory? The more often backups are done, the shorter the RPO can be.

Data Value – The monetary cost of recovering data if there is no backup. Include salaries and overhead for re-entering work from paper records; loss of business while those employees are recovering data; drops in productivity because of low morale; loss of business because customers simply clicked to another web site; cost of legal action brought by customers or vendors; loss of business because of bad PR; the cost of recovering lost business with discounts and sales calls. This is a good argument to use when marketing your service.

Downtime Cost – The cost of a business, or part of it, being unable to operate for a period of time. Likewise, this is a good argument for marketing.

Disaster Recovery Plan – A written and periodically reviewed plan that can be executed immediately and automatically in case a disaster disrupts all or part of a business. This plan also specifies the actions to be taken during the Recovery phase. This book includes a sample template for a Disaster Recovery Plan, in case you want to offer to develop one for your clients as a part of your service. (See "*Disaster Recovery Plan*")

Different types of data have their own RTOs, RPOs and Data Values. Therefore, it sometimes helps to separate the different data types into backup sets that can support the various objectives. *RBackup* fully supports multiple backup sets with different recovery objectives. Here's a chart with some sample values.

Table of Sample Data Types and Recovery Objectives

Data Types	RTO	RPO	DV
Web Servers/Online Store	10M	10M	$350K
Accounting Systems	1H	2D	$4.5K
CRM	4H	1D	$25K
Email	2H	1D	$40K
Spreadsheets	1H	1D	$500
Presentations	15M	1D	$2.5K
Letters	1H	2D	$10K
Images	1H	2D	$30K
Music	2D	4D	$5K
Video	2D	4D	$15K
Transaction Data	10M	1D	$50K
Customer Database	30M	1D	$300K
Application Files	6H	1D	$3K
Active Directory	15M	2D	$15K
System State	15M	2D	$5K

What Makes a Successful Online Backup Company?

*H*aving spent the past 23 years putting Remote Backup companies in business I have seen thousands of Remote Backup services reach great success. I've seen thousands reach a comfortable level, and maybe more importantly, I've seen many fail.

Online Backup is one of those kinds of businesses that you can run part time, spending very little time and money on it. Even a small business with 25 clients can bring in $2500 a month of easy residual income with very little effort.

It's also the kind of business that you can spend a ton of money on, hiring staff and buying lots of equipment, and you can ramp it up to bring in millions.

If I have invested $250,000 in my business, and after a year I only have 25 clients paying me $99/month each, I would probably call that a failure. However, if I invest only $5,000 and end up with 25 clients at $99/month after a year, that might be a success.

Remote Backup companies succeed for many of the same reasons other startups succeed. Here are my top ten most important things to do when starting your business.

1. Write and follow a Business Plan, Marketing Plan, and Financial Plan.

These plans are literally the roadmap for your business. Sure, you probably have a rough idea of all of these plans in your head. However, they aren't "real" until you write them down on paper. The most successful Service Providers all have detailed and well researched Business Plans, Marketing Plans, and Financial Plans.

In this book I have given you a template for a business plan for an online backup service. You can use that as a starting point to plan your business. A business plan is essential. It will help you organize your thoughts, get your head out of the clouds, and force you to examine and reevaluate your resources and abilities to operate a successful business.

2. Take the business seriously.

Some Service Providers just don't run their business like a business. They don't devote enough time or money to it, they give up too soon, or they get into it without adequate research and find out that it's going to take more time and resources than they had hoped, and they just give up. The most successful Service Providers have a dogged determination to succeed, and are relentless in pursuing their goals.

3. Do proper research.

Running a successful Online Backup business requires the same skill set as running any other successful business. You have to know how to set prices, how to handle money, how to budget, how to navigate the morass of government regulations, taxes, and reporting requirements. You have to know how to budget time, and when to hire employees.

Online Backup isn't for everyone. Some people don't make it because the owners don't have the technical background to operate them. Some fail because they don't have the sales skills to sell it. Some select the wrong target market. Some sell the service too cheaply, or for too much. Many get all excited by the technology and the potential and just jump into it with both feet and very little preparation.

People who know how to run a business and learn quickly stand a higher chance of success.

(CONTINUES)

How to Sell Online Backup

*T*he Online Backup business is booming. Independent Service Providers like most of us are benefiting from a rising tide of public awareness in Online Backup as an inexpensive and better alternative to tapes and CDs.

What do the Successful Service Providers Do?

Just about anyone can sell Online Backup. However, after years of watching thousands of them, I have a very good idea of what makes the most successful Service Providers.

They pitch once, sell many.

Any time you can make a sales pitch once and sell multiple clients, do it. The top grossing Service Providers all have this in common. Many of them form partnerships with other companies who have clients who might need online backup.

They have existing clients who trust them.

This group includes computer shops, network consultants, accountants, computer repair companies and others who have existing customers with a trust relationship involving their computers or data.

It is much easier to sell to existing customers than to create new ones. So, Service Providers who already have relationships with their target market reach profitability quicker and have better long term success.

Many Service Providers use online backup as a way to create new customers for other services. The customers of business online backup services are loyal. We have found that offering online backup makes them more "sticky," less prone to move to another computer shop or CPA.

They have a contract with a distributer.

These Service Providers, similar to the first group, can access a pool of existing customers through one or more distributors. One Service Provider formed a partnership with a distributer who rented equipment to schools – MANY schools.

They signed a contract giving the distributer a percentage of sales. The distributer then promoted online backup to his clients. The result: 11,000 new online backup clients within four months.

They brand their software.

All the most successful Service Providers brand their Client software with their own company name, software name, and graphics. All *RBackup* software packages come with a customization and branding utility at no additional charge, even in the least expensive packages.

They have a niche market.

The flexibility and ease of branding the RBackup and Mercury software allow Service Providers to create customized client software for niche markets, which can be promoted through associations and trade groups.

For example, one Service Provider has branded several different versions of his Client software for different state associations of dentists. The associations approve and promote the software to their members and receive a percentage of sales.

They embed online backup software in other applications.

This is my favorite. I wish more people would do this. RBackup has a built-in ability to be embedded in other software, thereby adding an online backup capability to software that otherwise wouldn't have it. Some Service Providers use this feature to partner with the developers of other kinds of software.

For example, one Service Provider partnered with a company that sells restaurant management software. He created a customized client that operated in "stealth" mode, and could be launched by a menu item in the other application.

His client software was embedded in the restaurant management software's installer, so it is installed right along with that software. With RBackup operating in stealth mode, it never displays anything on screen. So, as far as the restaurants are concerned, their management software automatically backs up its own files online every night.

They have a crack sales team.

The technology is cool. However, it's worthless unless you can sell it. The most successful Service Providers are good sales people. They spend more on hiring sales talent than they do on technical people.

Even if you don't fall into one of these "most successful" categories, please realize that the industry is still in its infancy – still in flux. These categories will change with time and technology.

Advertising

Traditional advertising like print media, radio, television and outdoor have never shown a high ROI with online backup. You might never sell an account directly from traditional

advertising, but it is valuable as one of those "six contacts" you have to have with a prospect before he becomes a customer.

PR (Public Relations, or simply Publicity)

PR has a high ROI for online backup services. However, don't confuse "publicity" with "advertising." Advertising is where you buy ads specifically designed to sell your service and ask for immediate action - YOU control the editorial content. Publicity, on the other hand, is a discussion of your service by a third party - you do NOT necessarily control the content. But, you CAN greatly influence it.

Publicity has been called the "secret pathway" to business success everyone wants. It's often called "free advertising," but this is incorrect. It is neither "free" nor is it "advertising." And, it's not always good. Bad publicity can ruin a company, where good publicity can make it rich.

Although publicity isn't technically "free," it IS often at a low price. In order to get publicity, you have to convince publishers, reports, producers, bloggers or others that your service is worthy of their time and their valuable editorial space.

So, in essence, you have to "sell" your service to those who might publish something about it. This can require telephone calls, personal visits, postal charges, wire service fees, and other indirect expenses. You might want to hire a professional to put together a press kit for you, or to write your press releases.

However, all of these potential costs of obtaining publicity almost always far outweigh the benefits of the right mention at the right time in the right publication or web site. Here's an example.

I used to advertise in a magazine called *Home Office Computing*. I paid about $2,000 a month for a 1/6 page black and white ad near the back of the magazine. In December of 1995 my Remote Backup Service Business Kit was favorably reviewed in an article in that same magazine.

Our sales as a direct result of that one article were three times our normal sales from our ad in the same magazine. It cost us about $50 for long distance calls, printing for a press kit, and overnight postage to get it to the reviewer. (These days reviewers expect emails and PDF documents, so you will rarely have an overnight charge.)

You should strive for as much good publicity for your business as possible. Your publicity efforts should be well thought out and pre-planned for maximum results.

The first and basic form of obtaining publicity is through what is known as the press or news release. This is generally a one page story about your service, or a current event related to data loss or disasters affecting business data. These publicity stories are generally sent out to all the

various media: local newspapers, radio and TV, trade publications, their online versions, and bloggers.

It's important to note that at the bottom line of a publisher's decision to use or not use your release are these questions:

- Does it fit in with the publication's or web site's theme?
- Is it timely? Is it related to current events?
- Does it support other stories and articles?
- Would my readers (listeners) be interested in this?
- Will it sell papers or generate clicks on my ads?
- Can I use this to generate buzz or attract ads?
- Is this good for search engine optimization?

The timing of your press release is always important. Try to associate your press release with current events in the news. A story on a large office building burning, leaving hundreds of businesses without access to their data, should prompt you to get a publicity release out to all the media on how your service could have helped.

(CONTINUED)

Operating an Online Backup Company

*Y*ou might start out with just a few clients and have ambitions to grow to thousands. My advice is geared toward companies who start out with a capacity to service fewer than one hundred end users, and who would like to scale up to thousands.

The quickest, least expensive way to start up a Remote Backup business is by sharing the resources of an existing company that has customers who are good prospects. This includes:

Internet Service Providers	*Independent Computer Consultants*
Regional Telephone Companies	*Web Developers and Programmers*
Alarm Monitoring Companies	*Accountants and Bookkeepers*
Retail Computer Shops	*Electronics Stores*
Computer Repair Companies	*Wireless Telephone Shops*
Network Engineers	*Airport Convenience Stores*

Employees

You will need at least two kinds of talent – technical and sales. Both are required, and are often found in the same person. There are many successful one-person online backup services.

Technical – The technical person in a small online backup company handles technical support, installs client software, installs and manages the Remote Backup Server. He or she also helps the Sales people understand the software and the technical aspects of the business, and might assist with sales in a technical capacity by designing a backup strategy.

Sales – The sales person is responsible for generating income. He or she might cold-call prospects, do follow-up, manage telemarketers, design advertising materials and call scripts, take orders, and do customer service. He or she will help set prices and service levels, track sales figures and goals, and might be the first person a customer calls for support.

Normal Expenses

You will need all the trappings of a regular business. This includes office space, furniture, computers, telephones, software, insurance, utilities, and a business license. If you plan to operate your own Remote Backup Server, you will also have the hardware, hosting, power, and Internet expense associated with that.

If you use Remote Backup Systems' Virtual Hosting plan (**http://remote-backup.com/vhosting.htm**) you will have a single startup fee and monthly expenses for software licensing and storage space.

Server Hosting

Many small Service Providers start with their offices at home, hosting their Remote Backup servers in data centers. Others have clients who are more comfortable knowing the server holding their data is closer to the Service Provider, so the choice is made to host the server in the same office.

Wherever the server is hosted, it will need the following equipment and environment.

Server Hardware – This is the server itself, and its storage space. The requirements for your server depend on the number of customers to which you want it to scale, and can vary from a single computer with internal storage for small numbers of users to clustered servers with large storage arrays.

(CONTINUED)

Delivering the Service

*T*o activate service you will need to deliver the Client or Agent to your customer and open an account for him on the server. This can be done as two separate actions, one manual and one automatic, or it can be done with full automation.

Full automation is usually the goal for services at a low price point. Partial or "no" automation is the goal for services at the higher price points.

Please see the chapter on "*Automating Your Online Backup Service*" for technical information on how to fully integrate your service with your web site.

Methods for Full Automation

Full Website Integration and Automation

(Order at a web site, pay with a credit card, download software immediately, recur billing automatically.)

This is the most popular method of automation. It requires the least amount of money to start up, your recurring billing is automatic, and it requires the least amount of manual intervention. Here's how it works.

A customer visits your web site and reads about your service. He goes to a shopping cart page containing several options for service plans. Maybe some plans have higher storage quotas, or are designed for Personal or Business use. There are usually different prices with discounts for paying in advance for longer terms of service.

The user selects the plan he wants and the term of service. The three choices for term are usually one month, six months, and one year. The user enters his personal information and pays online using a secure order form.

The industry is currently split on the efficacy of trial accounts. Some say the rate of conversion to live accounts is less than 15%, and that offering trial accounts can actually reduce ROI.

Payment methods are usually limited to credit cards, but some services allow PayPal and other payment methods. Credit cards are usually billed in advance for a period of time, and the payments automatically recur.

After the web site approves the charge, it offers the user a link to download the software, and it might (depending on the design of the website and server software) create a user account on the server and issue a serial number, which will tie the user and his software to his account.

The user installs the software, and can begin using his account immediately.

The shopping cart used here can be outsourced to a company like 1shoppingcart.com, or it can be built into the website by your web designer. My company has several products, including one fully self-contained, that can fully automate a sales, deployment, and billing process for Online Backup.

Full Web Integration with Trial Accounts

(Download trial-account software from a website. At the end of the trial period the software lets you enter a credit card number to activate a live account and start recurring billing.)

This works exactly like the first method, except that it usually has a much lower storage quota to start out, and requires no payment for the service up front. Rather, it collects a minimal amount of information from the user and deploys a free trial account for a period of time, usually fourteen to thirty days.

Near the end of the trial period, the software might begin displaying reminder messages, and the customer will begin receiving emails. At the end of the trial period the account will be frozen until the user pays for it or uninstalls the software.

When the software is uninstalled, the server will schedule the account and its data for deletion within a period of days, usually seven. If the account is frozen without the user uninstalling the software, the server will schedule the account and its data to be deleted for a much longer period of time, usually thirty days.

With the software still installed, the user is still receiving messages, so there is a much better chance he will decide to active his account.

When an account is deleted, the server will stop sending emails to the customer, or better, it will move the customer's email address to a follow-up list and begin a series of "Why didn't you sign up for our service?" emails.

If customers sign up for a live account, the payment and billing process works exactly like my first example.

The industry is currently split on the efficacy of trial accounts. Some say the rate of conversion to live accounts is less than 15%, and that offering trial accounts can actually reduce ROI. Trial accounts use up more drive space and bandwidth and increase tech support burden.

> *Offering a free trial and no commitment from users could cheapen your service, and is recommended only for the low-end Personal market.*

Other arguments against offering trial accounts are psychological. They allow customers to get away from your hard-selling website with a freebee and plenty of time to compare you with other services. You want to be the LAST website a customer looks at, not the first. Little pop-up messages can't sell as hard as a website can.

Offering a free trial and no commitment from users could cheapen your service, and is recommended only for the low-end Personal market.

(CONTINUED)

Best Practices

*T*his entire book is about Best Practices – the best way to sell your service, the best way to do telemarketing, the best way to select your software partner, and the best way to compete. In this chapter I concentrate on the best technical practices.

Identifying Data for Backup

Data can be categorized into three tiers: critical (integral to ongoing operations), important (valuable but not mission critical) and archival (required but not typically retrieved).

Usually, the customer just wants *everything* backed up. Of course this isn't possible at a reasonable price with today's technology. Most hard drives contain many gigabytes of data, most of which is non-critical and can be recovered from original distribution CDs and other sources. Computers are not yet fast enough to prepare that much data to transmit over the Internet in a reasonable amount of time, and upload bandwidth is inadequate.

Here's an example. The computer I'm using right now contains 43.3 gigabytes of data. My Internet connection is fairly fast – 12 Mbps downstream and 3 Mbps upstream. So, assuming 100% efficiency, I can theoretically send all this data up to the Internet in 1 day, 8 hours, 4 minutes, and 26.67 seconds.

Only RBackup enables a Service Provider to ship recovery data to a client while maintaining regulatory compliance and 100% security and privacy.

That doesn't sound too bad. But, no Online Backup Service Provider is going to take my connection at 3 Mbps, and I'll never achieve 100% efficiency. The best I can hope for is an overall bit rate of (maybe) 900 Kbps, which is going to take 4 days, 10 hours, and 54 minutes. That's too long.

Most businesses have an upstream bandwidth less than 900 Kbps. 512 Kbps is more common. That would take twice as much time.

In addition to the time it takes to do a backup, we must consider the time it takes to restore, called the Recovery Time Objective (RTO). This is a more important number because it directly impacts a company's down-time in the event of a disaster.

What is the acceptable amount of time between the loss of data and its recovery? If there is too much data (because of bandwidth) to download in an acceptable period of time, the Service Provider may have to deliver the restored data on a USB drive. This is where physical proximity

to your clients is important. You could overnight a drive if your customer's RTO is twelve hours, and depending on what time of day the data loss occurred.

You can test your upstream and downstream bandwidth at the following link:

http://www.dslreports.com/tools

Then you can use one of my handy dandy online calculators to figure out how long it will take to do a backup:

http://remote-backup.com/calculators

Clearly you have to be selective about which files you back up.

Include & Exclude

Online backup software contains rules that govern which files are backed up and which files are not. In *RBackup* and *Mercury* files and folders can be included and excluded from backups many ways. I won't go into their specifics, but I will explain the basic concepts.

Backup Sets

Because different groups of files have different tiers (critical, important and archival) which coexist on the same hard drive, online backup software needs a way to assign include/exclude parameters and schedules by file groups called *Backup Sets*.

Some backup sets contain critical data that needs to be backed up every day and kept for twelve months, with a Recovery Time Objective of three hours, and the ability to do a point-in-time restore.

Some backup sets contain less important data that only needs to be backed up every two days, only kept for ninety days, and doesn't need point-in-time.

Part of your job as a consultant is to help your customers design a backup strategy that backs up the correct files often enough to meet the company's RTO and RPO, while archiving data for the required amount of time, and providing the ability to roll back through multiple versions by date or version number.

Synthetic Full Backups

In the old days when people backed up to tape drives a certain strategy had to be used. The most popular was Grandfather/Father/Son tape rotation. This method required 19 to 23 tapes and ensured that there were always backups of the seven most current days, the four most current weeks, the eleven most current months, and the most current year.

This method required keeping close tabs on which tape was which, and rotated them so most of the tapes received even wear from the tape machine, so they could be replaced in groups.

Restoring from tapes required finding the tape containing the backup that had the version of the file you want, and restoring it from tape. To do a complete disaster recovery required restoring first the most recent full backup, then all incremental backups since then. It was a long and arduous task. Tapes would break, or would become unusable because of heat, humidity, wear, and magnetic distortion.

What does this mean to you? It means that your customers have great freedom in restoring files quickly. It also means (and this is the biggie) that you only have to perform one full backup – EVER. All the others can be incremental.

When I designed the first Online Backup software, I predicted a problem with that kind of strategy, and saw an opportunity to employ a powerful function that tape didn't have – Indexing and database-driven restore.

This gave rise to what was later called Synthetic Full Backup - full backups that are built out of pieces of previous incremental and full backups already on the server without the need to re-send data to the Server. It saves a lot of time on restore and saves space on the Server.

In addition, it allows for creating full restores to any point in time, and the on-the-fly custom design of virtually any type of restoration of any subset or groups of subsets of full backups by date, file size, file type, backup set, drive location, customer-defined "tags," file name or folder name, or any other file attribute. Restores became very granular, and very fast, and could be done all in a single pass without the need to restore from multiple backup sets.

As far as I know, my *RBackup* and *Mercury* are the only two online backup packages currently available that can process Synthetic Backups.

Backup Types

There are two basic types of backups, and two more special cases supported exclusively by *RBackup*. The first two respect the "Archive Bit," a piece of information carried along with the file name by the operating system which is used by backup software to determine if a file has been changed since its last backup.

It works like this: Whenever you edit a file, the operating system automatically toggles the Archive Bit ON. When the file is backed up, the backup software can toggle the Archive Bit OFF. This makes it very quick for backup software to scan the drive for files that need to be backed up. It just looks for those with the Archive Bit turned ON.

Incremental Mode – Backs up files that have been changed since the last backup, and then turns the Archive Bit off.

Differential Mode – (Exclusive to RBackup) Backs up files that have been changed since the last backup, but leaves the Archive Bit ON. This special type of backup is used when an end user wants to use RBackup AND regular tape backup software at the same time. Tape backup software is not typically smart enough to have a Differential Mode, so the procedure is to run the tape backup AFTER the online backup. The files are backed up online, and then backed up again to tape, and their Archive Bits are turned OFF by the tape backup software.

Full Mode – Backs up all selected files regardless the setting of the Archive Bit.

BitBackup Mode – (Exclusive to RBackup) Backs up just the parts of files that have changed since the last backup. For example, if only one paragraph changed in a document, BitBackup will back up just that paragraph. This saves time and bandwidth, with the added bonus of also maintaining a local Data Store for immediate restoration at full internal network speed. This also provides a local backup AND online backup for redundancy.

Some software, like *RBackup* and *Mercury* can operate without using or changing the Archive Bit at all. Rather, they use more reliable methods like cataloging the date and time stamps.

> **RBackup's first backup is always a Full Backup, after which it automatically switches to your selected backup mode, even if your first full backup is a Copy to Disk using a portable USB drive.**

Servers

Let's have a look at a typical small Server that contains a mix of critical data (Exchange Server, System State and Active Directory), important data, and archival data.

Typically 70% of data on a server never changes, or changes very rarely. There are usually many old files that are not being used and might never change, but the end user wants them backed up. If you (as the service provider) have a hands-on relationship with the customer, the decision on how to categorize the data should be made by interviewing the end user to determine what applications his business relies on and what data usually changes.

RBackup works on Windows servers. It will automatically detect *Exchange, SQL Server, Active Directory and Sharepoint*, and will display icons for you to use to back up these special

databases. These applications are always considered "critical" and should be backed up frequently.

A typical small Windows server might have three backup sets, designed like this:

Backup Set 1 (Critical)

Included: MS Exchange, SQL Server, System State, Active Directory
AutoSelect: OFF
Backup Type: BitBackup
Schedule: Daily
Keep Latest Version: ON
Retention Period: 365 Days
File Selection: Modified Date/Time

Backup Set 2 (Important)

Included: All MS Office Documents
AutoSelect: ON
Backup Type: BitBackup
Schedule: Daily
Keep Latest Version: ON
Retention Period: 180 Days
File Selection: Fast Pick

Backup Set 3 (Archival)

Included: manually selected folders and files
AutoSelect: OFF
Backup Type: BitBackup
Schedule: Weekly
Keep Latest Version: ON
Retention Period: 30 Days
File Selection: Archive Bit

Workstations

Workstations are desktop or laptop computers that may or may not be networked with more powerful Servers. Employees do virtually all of their work at the consoles of workstations. Servers are rarely operated by employees for day-to-day tasks, and may be locked away in a closet.

Workstations and laptops usually have different backup and restore requirements than Servers, and sometimes need only one Backup Set. Servers are usually administered by someone who is more computer-literate than people who use workstations, so the directory structure of a Server is usually more standardized and easier to back up.

Workstations, however, can have valuable files virtually anywhere on their drives. If the computers were installed and the software configured by a professional, you might be able to depend on critical files being in the right folders. Otherwise, you may have to search for them. *RBackup* and *Mercury* have features that can locate critical files automatically.

Recommended Include and Exclude Rules

Here are the most important folders to consider when designing a backup strategy for workstations and non-networked computers, along with my opinion of their importance and recommendations for including or excluding them.

Personal Files (Critical-Include) – Windows computers usually store personal, user-generated files in a folder structure whose root is a virtual folder called *My Documents*. Depending on the application you use to look at the file system, this folder can also look like: *C:\Documents and Settings\[User Name]\My Documents* Mac computers store personal files in a folder structure whose root is called *Users*.

Start Menu (Critical-Include) – This is where Windows computers store their application shortcuts and group folders. There are two Start Menus – one for the logged in user and the other shared by all users. They are: *C:\Documents and Settings\[User Name]\Start Menu* and *C:\Documents and Settings\All Users\Start Menu*.

Desktop (Critical-Include) – Windows and Macs store their desktop shortcuts and other objects here. For Windows there are two – one for the

(CONTINUED)

(END OF SAMPLES)