This paper was originally presented at the Southwest Fox conference in Mesa, Arizona in October, 2009. http://www.swfox.net

The Show Must Go On

Disaster Recovery and Business Continuity Planning

Rick Borup
Information Technology Associates
701 Devonshire Drive, Suite 127
Champaign, IL 61820
Email: rborup@ita-software.com

We all like to think it won't happen to us, but the truth is a disaster can strike anywhere at any time. Whether man-made or natural, there is a wide range of events that can seriously disrupt or even destroy a small business in a very short time. This session, which is geared toward the independent software developer, looks at the threats faced by small businesses and discusses measures you can take to help ensure business continuity while recovering from a disaster.

Overview

Business Continuity

The term business continuity refers to the continuous, uninterrupted operation of an enterprise. In the most general sense, therefore, a business continuity plan (BCP) is a plan to ensure that a business is able to maintain continuous, uninterrupted operation regardless of what happens, whether expected or unexpected.

It might seem odd to include expected events in a business continuity plan, but a comprehensive BCP could include things like succession planning for the pending retirement of a key executive or the planned change in executive or organizational structure following the sale or acquisition of a major business unit. However, while these are certainly important issues for large organizations, they are probably of little concern to the small or one-person business. Because independent software development businesses tend to be very small, this session focuses on how to anticipate and plan for unexpected events.

Unexpected events that might be addressed in a business continuity plan can cover much more than what one might ordinarily think of as constituting a disaster. This might include the planned response to the emergence of a disruptive technology or technologies, to market share threats from previously unknown competitors, to a dramatic change in economic conditions that significantly reduces revenue streams, and—of course—to disasters affecting facilities, equipment, and personnel.

Looked at in this way, it can be seen that the subject of business continuity planning is a much broader topic than disaster recovery planning alone. While no business continuity plan would be complete without including a disaster recovery plan, not all businesses—particularly small businesses—can necessarily benefit from the considerable effort needed to develop a comprehensive business continuity plan.

However, even the smallest business needs to give some thought to the potential threats it faces and to make plans for what it needs to do in order to survive and remain in operation following a disaster. This is the domain of disaster recover planning, which is the focus of the rest of this session.

Disaster Recovery

For purposes of this session I'm defining a disaster as any event, whether natural or man-made, that causes a significant, prolonged, and adverse effect on the business. Disaster recovery, therefore, is the process of restoring normal business operations following a disaster.

It follows that a disaster recovery plan (DRP) is a plan to restore normal business operations after a disaster. Although this may sound simplistic, an effective DRP requires careful planning and preparation along with ongoing testing and revision.

Disaster recovery planning

Following is a simple four-step guide for preparing a disaster recovery plan. While certainly not the only way to approach this process, the steps presented here should be suitable for use by small businesses that don't have the time or resources to invest in a more elaborate planning process.

Step One – Risk Assessment

The first step in disaster recovery planning is to conduct an assessment of the risks to which the business is exposed. In this step you attempt to answer the question: "What types of disasters is my business most likely to be affected by?"

Risk Factors

There are many risk factors that can cause a disaster. Some are man-made while others occur naturally, and your exposure to these risks may vary depending on where you live.

In some parts of the United States, your business may be highly exposed to the risks from certain types of violent weather or other natural phenomena that are common in that area, while being far less exposed to other types of natural events due to the lower probability of them occurring in your geographic area. For example, where I live in central Illinois we are acutely aware of the potential for disaster caused by tornados and severe thunderstorms, but we have much less risk of earthquakes and almost no risk of being affected by a wild fire. On the other hand, if you live in the Pacific Northwest there is little chance of being affected by a tornado but earthquakes and volcanic eruptions are potential threats, while in California wild fires may be the most likely cause of a disaster.

To help you assess the types of risks to which your business may be most likely exposed, consider the following categorized lists and think about the extent to which they apply in your situation.

Computer specific risks

- Mischief (innocent or malicious)
- Malware (virus, worm, rootkit, spyware)
- Hard drive failure (head crash, bad sectors, file system corruption)
- Physical damage (drop, crush, fire)
- Accidental loss
- Theft

Software specific risks

- Corruption of source code
- Theft of source code or other intellectual property

Natural events

- Earthquake
- Hurricane
- Tornado
- Wildfire
- Flood
- Volcano
- Pandemic disease outbreak

Man-made events

- Office fire (localized)
- Building fire (widespread, multiple offices and businesses affected)
- Hazardous materials spill
- Civil disturbance
- Terrorist attack
- Nuclear accident
- Nuclear attack

Rating your potential exposure to these risks can help you focus your efforts on those areas most likely to cause a disaster in your particular situation.

As you work through the risk assessment step, don't overlook the potential impact on your business of a disaster that affects someone else such as your power company, your Internet service provider, your email service provider, your Web hosting company, and so on. In other words, as you analyze the risks to which your business is exposed, remember to include the risks that can impact you indirectly as well as directly.

Step Two – Impact Assessment

Step two of the disaster recovery planning process is to assess the potential impact of each risk factor to which your business has significant exposure.

By definition, a disaster is an event that causes a significant, prolonged, and adverse effect on your business. Within the scope of everything that can be considered a disaster, however, there can be a wide variety of impacts on your business ranging from relatively minor and/or geographically localized on the one extreme to major and geographically widespread on the other extreme.

Going back to the earlier example, if you live in the Pacific Northwest your exposure to the potentially disastrous effects of a volcanic eruption is higher than if you live in the Midwest, while your exposure to a disaster resulting from a tornado is higher in the Midwest than in other parts of the country. Although both can certainly be devastating, the impact of a volcanic eruption is likely to be geographically widespread while the effects of tornado are generally much more localized.

Your disaster recovery plan needs to take into these kinds of things into account. For example, a backup office location within ten miles of your primary place of business may very likely survive unscathed by a tornado that levels your home or office building, while a volcano or hurricane is much more likely to take out both. This influences your choice of a potential backup office location as well an appropriate off-site storage location for data and records.

Impact of a disaster

The immediate impact of a disaster is most likely to be the loss of facilities and equipment and, in the worst case, loss of human life. Although equipment and facilities can be repaired or replaced, given enough time and resources, they are likely to be unavailable for some period of time following a disaster. Since the whole point of a disaster recovery plan to is to enable the enterprise to continue functioning until normal operations have been restored, the impact assessment step is where you determine whether there is a need for backup facilities and equipment, and possibly for backup personnel.[1]

The most obvious way a disaster can impact facilities and equipment is by damaging them to the extent that they cannot be used until repaired or replaced. If you are a national or global enterprise with many production locations, the impact of a disaster at any one of these locations, while significant, might result in only a relatively small percentage reduction in production capacity. On the other hand, if you are a small business with only one location, the impact of a disaster affecting that location can result in a complete loss of

[1] Independent software developers tend to have it easy in this regard. “Facilities” most likely comprises only your home or office, while “equipment” is your computers and the software and data they contain. Both are relatively easy to relocate or replace, as compared say to a manufacturing plant with specialized equipment.

production capacity, at least over the short term. Therefore the same event may have a much more serious impact on a small business than on a large business.

A less obvious way a disaster can impact facilities and equipment is by preventing you from accessing these things even if they are undamaged. For example, a severe flood might ruin the facilities and equipment of businesses on the first floor of a building while leaving your second floor office and computers untouched. However, that same flood could easily prevent you from accessing your undamaged office or computers for an extended period of time, thus impacting you—at least in the short term—the same way as if your facilities and equipment had actually been damaged or destroyed.

Almost every business relies on Internet-based communications these days, and software developers are certainly no exception. During the impact analysis phase of your disaster recovery planning, consider the impact on your business of an extended power outage or an extended loss of Internet service or access to email. For how long could your business continue operating without those things? If the answer is "not very long", your plan should identify suitable alternatives and spell out your plan for transitioning to those alternates if it becomes necessary.

Step Three – Planning for recovery

In steps one and two you looked at the various risk factors to which your business might be exposed and you made an assessment of the impact various types of disaster could have on your business. Step three of the disaster recovery planning process is to figure out ways to reduce the potential impact of a disaster and to plan for recovery if one does occur.

Replacing equipment

Unless you choose to place a fully configured machine or machines on hot standby in a safe location, recovering lost or damaged equipment for the independent software developer mostly entails buying new computers. Because computers are a widely available commodity these days, one can assume that buying a new computer to replace a machine lost or damaged in a disaster is not going to be terribly difficult or time consuming. Even if your optimal replacement machine is not quickly available, you can probably find a suitable short-term replacement at a local big box store or from a mail-order outlet. Your recovery time objective (RTO) for equipment is therefore probably measured in hours or days rather than in weeks.

Recovering software and data

Recovery of software and data is another matter, because for these things you are going to be almost completely reliant on backups you have made yourself. There are so many ways to back up software and data files that the subject merits its own discussion, which follows later in this paper. This section focuses only what needs to be backed up.

Software development tools and utilities

One obvious class of files you will need to recover is the software tools you use in your development work. This includes commercial software development tools such as Visual FoxPro and Visual Studio, as well as other 3rd-party tools and utilities and perhaps even tools you have developed on your own.

Start by compiling a written list of the software you rely on in your everyday work. For each item on the list, include its name, where and when it was purchased, and the location of the installation media. For example, if you obtained software on a DVD, which DVD is it on and where is that DVD stored? On the other hand, if it's something you purchased and downloaded, from where did you download it and where is the original download file now stored? When trying to cope with the stress and uncertainty following a disaster, you will find in helpful to have all of this information recorded on a single list rather than scattered around in various places.

It's important to write this information down. Don't fall into the trap of thinking that you'll remember where everything is, which can be difficult even under normal circumstances but is particularly so when you're under stress.

Product keys, license numbers, etc.

In addition to having your installation media is, don't forget that in order to reinstall the software you also need to know the product keys, license numbers, or other such essential information. Even if you know where the physical installation media such as a DVD is located, and even if the product key is recorded on a sticker inside the DVD container, remember that both the DVD and its container could easily be lost in a disaster. Be sure to keep a separate written copy of your product keys, license numbers, and so on and store that information in a separate and secure location where it can be easily accessed in the event of a disaster.

Usernames and passwords

Another class of critical information that should be written down and securely stored is your passwords. Some software stores your username and password on your computer so you don’t have to key them in by hand every time you use it. Email accounts are a good example of this. While convenient, it’s easy to forget what your email password is since you don’t have to enter it manually every time you check your email. If the computer you use for email is lost in a disaster and you can’t remember your password, you may be effectively unable to access your email even though you have acquired a new machine.

In other circumstances, you may need to know your username password in order to login to the website from which you can re-download important software you purchased.

Source code

The source code for software you have written or are working on is clearly a critical element in any disaster recovery effort. As with other critical files, the hard and fast rule is to always maintain a current backup, and preferably more than one. The section on backup strategies and tools later in this paper discusses several ways for doing this. The important thing is to adopt a backup strategy that works for you and then follow it religiously. As with other backups, the importance of maintaining off-site copies of your source code cannot be stressed too strongly.

Since this paper is being written for a Visual FoxPro conference, and since Visual FoxPro is a tool for developing database applications, you most likely work with a significant amount of data in your development work. Even if it's only test data, it would certainly be time consuming, probably difficult, and maybe impossible to re-create it all following a disaster. Keeping a current backup of your databases and other data files is therefore also a critical component of your disaster recovery planning process.

Visual FoxPro

At first it might seem like you don't need to back up Visual FoxPro itself. After all, you can simply reinstall and be on your way, right? However, consider the service packs you may have downloaded and installed but which are not be on a DVD or other physical media. Also think about the settings and customizations you have applied to configure the VFP development environment the way you want it. Backing up these things can save you a lot of time and reduce stress while you're struggling to recover from a disaster. Details on how to back up VFP are included in the section on strategies and tools for effective backups later in this paper.

Recovering physical facilities

As devastating as it would be to lose a home or even just an office to a disaster, those things can be rebuilt or recovered in the long term. Your disaster recovery planning efforts in this regard should therefore deal with securing an alternate place of business that you can use until the original is available again, or for permanently relocating your business if the original site is damaged or destroyed beyond reasonable recovery.

Backup location

If your primary place of business is unavailable following a disaster, especially if it's for an extended period of time, you'll need a suitable location from which to conduct business until your primary site has been relocated or restored. For the independent software developer, your choice of a suitable backup location may be as simple as temporarily working from home, if your office was damaged, or perhaps working from the nearest WiFi hotspot if your home office is unavailable for some period of time.

Although this may not take a lot of advance planning, it's important to think it out and to go ahead and make whatever plans may in fact be necessary. If your backup site is your home, think about which room(s) you'll work from; be sure there is enough space, a sufficient number of electrical outlets, adequate lighting and ventilation, and sufficient Internet bandwidth to accommodate your needs. If your backup site is the WiFi-connected café at the local bookstore, be sure you can connect to their WiFi network and find out how long the management may be willing to let you sit and work there without buying anything.

Risk of simultaneous destruction

Another important consideration when choosing a suitable backup site is to choose one that's unlikely to be affected by the same disaster that takes out your primary site. As an example, consider the potential impact of tornadoes here in the Midwest. Tornadoes in this part of the country typically follow a southwest to northeast path. While some tornadoes touch down only briefly, others can stay on the ground for miles. Therefore it would be unwise to choose a backup location that is relatively close to and either directly southwest or northeast of your primary place of business, because both sites could potentially be destroyed by the same tornado.

Unfortunately this is not at all true for more geographically widespread disasters such as hurricanes, which can affect very large areas. If you're located in an area that's at risk for hurricanes or other types of widespread disasters, an effective backup location may need to be tens or even hundreds of files away from your primary place of business.

Step Four – Testing your plan

An untested disaster recovery plan is nothing but shelf-ware. You know what I mean: written material that sits on the shelf, probably in a handsome binder, but never even gets looked at much less used. If you spend time developing a disaster recovery plan and don't test it, you've wasted your time.

While important, testing a disaster recovery plan is not necessarily easy and in some ways carries its own set of risks. Advance planning and coordination with affected parties can help make your disaster recovery test go more smoothly and effectively.

Planning for the test

If your test is going to affect other people, be sure to let them know in advance. For example, if conducting the test means your customers won't be able to reach you via normal channels of communication for some period of time, let them know what you are going to be doing and when. If your test is going to simulate a disaster to any realistic degree, be sure to inform an affected family members, neighbors, landlords, other tenants in your office building, and perhaps even local authorities in advance that it's only a test.

On the other hand, if you really want to stress-test the effectiveness of your disaster recovery plan, the test may be more meaningful if the people involved don't know it's only

a test. This is a bit risky because you have to walk a fine line between simulating a disaster while not causing genuine distress among the people affected nor significantly disrupting normal business operations. If done correctly (and I've seen it done), such a test is very effective because it simulates the psychological as well as the physical impact of a disaster. This forces people to rely on the recovery plan to a much greater degree than if everyone knows it's only a test.

Conducting the test

On the day of the scheduled test, deny yourself and your staff access to anything that is not part of your recovery plan. Strive to make yourself and everyone else who's directly involved believe that "this is real", and act accordingly.

Put the plan into motion and follow what's written. Don't circumvent the plan, even if you can. For example, if the backup plan says a certain backup resource should be in location "A" but it's not there or doesn't contain all the files it should contain, don't pull that USB drive out of your pocket just because it happens to have the necessary files on it. Remember that you're testing the plan, not relying on circumstance to fortuitously bail you out during the test.

Make notes on things you forgot to plan for, and write them down. For example, if you find that your backup office site is unavailable during the test because of an unanticipated construction project going on in that building, make a note of it. If your backup media is inaccessible due to unforeseen circumstances, or if files cannot be restored from a backup, make a note of what happened and why.

Assessing the test and revising the plan

After the test is concluded, review what went right and what went wrong. Revise the plan to improve the parts that did not work as expected. If other parties were involved in or impacted by the test, either directly or indirectly, thank them for their patience and/or participation. If your customers were inconvenienced, apologize and remind them that your goal is to ensure you can continue to provide them with the expected level of service even in the event of a disaster.

Lather, rinse, repeat

Disaster recovery planning is an ongoing process. Your goal is to continuously improve your plan over time through repeated testing and revision. How frequently you do this is up to you. Testing once a year is probably a good rule of thumb, but remember to keep the plan up to date as things evolve and change in your working environment between tests.

Strategies and tools for effective backups

Backup strategies

For purposes of this section, the assumption is that your office and its contents, including computers, have been destroyed or are inaccessible due to a disaster. It's further assumed that you have access to a backup site from which to conduct business, and that you've been able to purchase new computers or at least secure the use of other computers not previously used in your business.

Putting yourself in this frame of mind when designing your backup strategy helps you to identify all the things for which you'll need to have current backups in order to continue operation and recover from the disaster. Imagine that you're sitting in a barely furnished office with nothing familiar around you and nothing but a newly acquired computer on the desk in front of you. Then ask yourself, what do I need to resume working and where am I going to get it? The answers to those questions define what you need to back up, how often you need to back it up, and where you need to store it so you can get to it when you need it.

What to backup

Perhaps the first thing to think about is how to effectively back up the content of the physical installation media (CDs, DVDs) for the software tools you use in your work. One solution might be to rip a copy of each disc for backup purposes. Another solution might be to store the originals discs in a secure off-site location, since you probably don't need them on a regular basis anyway.

As with most kinds of backups, however, there is a trade-off between security and convenience. If in the course of a day's work you find that you need the Visual FoxPro 9.0 installation DVD for some reason, it's convenient to have it right there in your office but it's not very secure from a disaster there. And while the DVD would be much more secure in a bank safe deposit box, it might be very inconvenient to take the time and effort necessary to go get it. What you decide to do depends on how much risk you're willing to take, and what your options are if a disaster occurs.

You should also backup software you have downloaded but for which there is no physical installation media. While you might be able to download another copy from the vendor if you need one, some software vendors restrict downloads to the first 30 or 60 days after purchase and on top of that it's always possible the vendor has gone out of business. The best bet is to keep your own copy of all downloaded software as part of your ongoing backup.

For software that's licensed specifically to you or to your business, it's generally useless to have the installation media without also having your license number, product key, or whatever is needed to install, activate, or unlock the software. You might also need to produce that number in order to prove that you're a licensed user if you need to request

another copy of the installation media from the vendor. Make a list of your product keys and license numbers and keep it current as part of your ongoing backup strategy.

There is a nice, free little utility called Magical Jelly Bean Keyfinder that can help you with this task.[2] It finds the registered product keys for certain software installed on your computer and displays them as shown in Figure 1. From there you can print the results or save them as a text file for documentation.

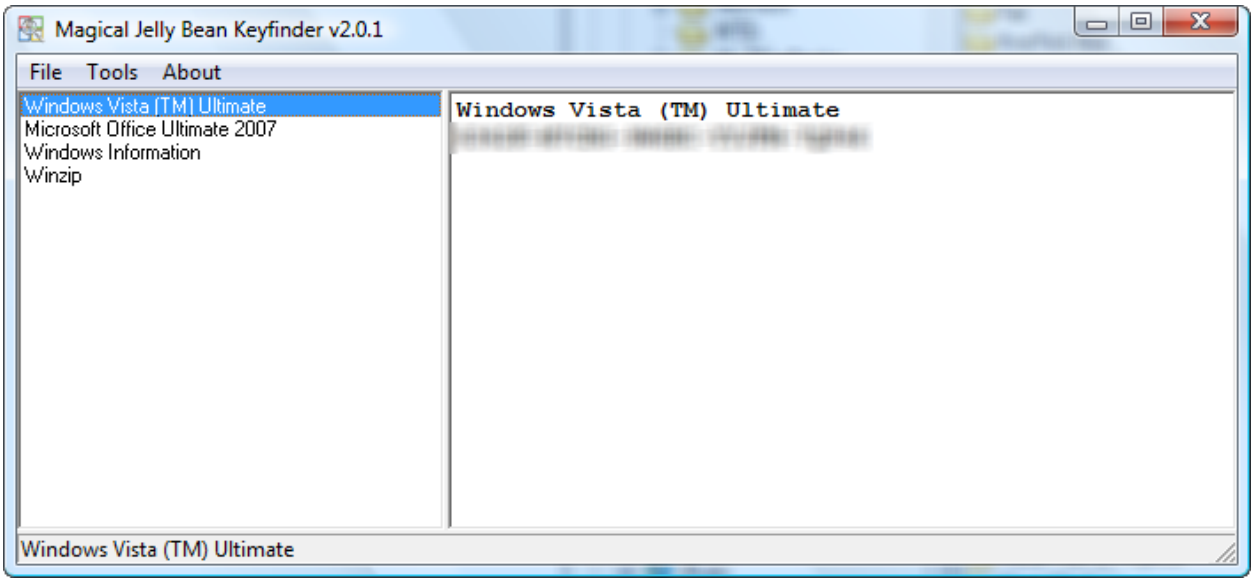

Figure 1: The Magical Jelly Bean Keyfinder finds and displays product keys for known software on your computer.

Passwords are another critical component of your backup strategy. Most of us have far more of them can we can remember, which is why utilities that store passwords in an encrypted file are so popular. Besides keeping track of your passwords, these utilities also make it possible to create a backup by simply making a copy of the file.

One of the most popular tools for this purpose is RoboForm. Personally, I use one called Password Agent. Among other nice features, Password Agent has a "to go" feature that installs the software and a copy of the encrypted file on a USB drive in one simple step. This makes it quite easy to keep a current backup of all my passwords.

Type of backup and backup frequency

The questions of what type of backup to use and how often to do it are intertwined. A full backup backs up all files and folders included in the backup set, thereby ensuring that the backup is current and complete. However, full backups—particularly of an entire volume

[2] The link to the Magical Jelly Bean Keyfinder website can be found in the Appendix, along with links for lots of other software and services useful for backup and disaster recovery.

on a hard drive—generally take quite a while to run and for this reason may not be done as frequently as might be ideal for 100% current recovery.

An incremental backup backs up only what's new or changed since the last backup. While this ensures that all new files and folders are backed up, it relies on the existence of a previous full backup when complete recovery is needed. Because it backs up fewer files, an incremental backup runs more quickly than a full backup and therefore can be run more frequently when time constraints are a factor.

Some backup tools must be run either in full backup mode or in incremental backup mode, creating a separate file each time. This can be a good solution in situations where you might be able to run a full backup only on weekends but can run an incremental backup daily. Complete data recovery from this type of backup can be cumbersome, though, because full recovery as of any given day requires restoring from the most recent full backup file followed by restoring from each successive incremental backup file.

Other types of backup tools make it possible to combine full and incremental backups in a hybrid fashion in order to maintain a current and complete backup at all times without having to run a full backup every time something changes, and without having to deal with multiple files when recovery is needed.

Tools such as the venerable Beyond Compare make it easy to synchronize a backup copy of selected files and folders with its original counterparts. The synchronization process overwrites older files on the backup media with the newer version of the same files, while preserving the files that have not changed. As an incremental backup, this takes only as long as necessary to copy the new and changes files, but the result is the same as if a new, full backup had been performed. And as with a full backup, you only need to go to one backup source to recover the current version of any or all files.

Online vs. local backup

In general there are two choices for how and where to create your backups: online backup to a remote server via the Internet, or local backup to removable media such as a CD, DVD, USB drive, or external hard drive.[3]

Is one better than the other? Both have advantages and disadvantages.

With online backup, the security and storage of the backup media is not your responsibility but it's also outside of your control. With local backup, you have to be responsible for securing and storing the backup media yourself, but it's also completely under your control.

[3] Tapes were once a popular format for backing up large volumes of data, but are giving way to more robust and reliable media with the advent of large capacity external hard drives and multi-GB USB drives.

With online backup, you rely on the service provider to make your files available when needed for recovery. With local backup you rely on access to your own backup media and its storage location when files are needed for recovery.

> **True Story**: I used to work for a bank where the data processing department made daily tape backups of the critical data from the mainframe computer. Each morning the tapes were placed in the bank's vault, where they were safely stored until rotated out for re-use again three days later. This seemed like a fine system until one night when, at about 2:00 AM, the third shift computer operators discovered they needed immediate access to certain files from the previous night's backup tape in order to complete the current night's processing. The bank vault, of course, was locked on a timer and could not be opened by anyone until 7:00 AM the next morning. Was the backup tape secure? Absolutely. Was this a good backup strategy? No.

With online backup, the backups are by definition stored off site. With local backup, you have to transport the backup media to an offsite location yourself.

With online backup, the service provider determines whether or not multiple generations of backups are kept for you. With local backup, you are responsible for keeping the desired number of backup generations and for rotating through the backup media correctly.

Automated backups

Many backup strategies I have seen are configured to run an automatic, unattended backup in the wee hours of the morning. This is especially true of file server backups, where it certainly makes sense because the backup may take several hours to run and usually needs to be done when nobody is working.

The benefits of running an unattended operation include lower cost (no personnel needed) and the ability to run it when nobody is accessing or updating the files that are being backed up. As with any unattended operation, however, there are risks with automated backups.

The main risk with an automated, unattended backup is that the backup might fail and nobody notices it. Moreover, it may continue to fail every day for an extended period of time if nobody is paying attention to the log files or error messages. I have seen situations where a staff diligently rotated the backup media every day, never realizing the backups were totally worthless because the backup job did not run.

> **True Story**: I was recently troubleshooting a problem with my application running on a client's Windows network. While scanning the Application Event Log on the file server for clues to the problem, I noticed a curious pattern of message which, although unrelated to the problem at hand, invited investigation. Every night at 4:00 AM a Backup Exec job started up, and every 15 minutes thereafter a Backup Exec message was recorded in the log file. I checked the properties of several of these messages to see what they said. The message was: "Please insert overwritable media into the drive."

My feeling is that taking the human being out of the equation is always risky. An automated backup strategy can certainly be effective, but for any of my clients who want to go that route I advise putting in place a procedure that requires a person to look at the log files every day to be sure the backup job ran to completion and without significant errors.

Test your backups

The ability to restore files from your backup is equally as important as the ability to back up the files in the first place. If you don't test your ability to recover files from your backup, how do you know the backup is any good?

Naturally, restoring files from a backup into a live environment introduces its own set of risks. For one thing, the live environment might need to be shut down temporarily while the restore is in progress. Another risk is that the backup could fail or could restore only partial or corrupt data. In this case the live environment, which was fine before the test, might now be corrupt as a result of the test. For this reason, it may be preferable to test your backup by restoring files onto a non-production machine. That way you can at least ascertain that the backup media was readable and the files could be restored.

Something to consider when choosing an online backup service: be sure you can restore files from the online backup via the Web or using a different computer than the one you used to create the backup. If an online backup service to which you subscribe installs software on your machine, be sure you will be allowed to install the software on a different machine in an emergency without having to buy a new license, or that you can at least restore files from your online backup without having to install the vendor's software at all. In other words, be sure the service is not tied to just one machine because that machine could be unavailable due to loss or damage following a disaster.

Backup tools

The good news is that there are lots of fine backup tools and services available these days. There are too many to cover individually here, so I've listed several of them in the Appendix, grouped by category along with links to their website.

Backing up Visual FoxPro

Last but not least on your list of things to backup as part of your disaster recovery plan is Visual FoxPro itself. Start by making sure you have the original DVD for the version of VFP you are using, along with the product key.

Next, be sure you have a backup copy of any VFP service packs or hot fixes you have downloaded and applied. The VFP home page on MSDN still has a link to download Service Pack 2 (SP2) for Visual FoxPro 9.0. The older Service Pack 1 is no longer listed on that page, although you can find the download link with a search.

You may also want to make a backup copy of your VFP installation folder, which by default is C:\Program Files\Microsoft Visual FoxPro 9 (for version 9.0), as well as the runtime and other files in C:\Program Files\Common Files\Microsoft Shared\VFP. Naturally, if your backup strategy includes a complete hard drive backup then this and what follows are already taken care of.

If you've customized your VFP development environment in any way, you'll be able to get up to speed more easily following a disaster if you can quickly restore your familiar working environment on a new machine. To do this, make backups of your configuration files. This includes config.fpw and/or other configuration files you may be using, as well as your custom startup program if you use one. Mine is named vfpstartup.prg, yours of course may be different.

The options and settings you configure in the VFP Tools | Options dialog are stored in the registry. Visual FoxPro has a nifty little built-in facility that enables you to export these options to the output window in the debugger. To do this, open the VFP debugger, then go back into the VFP IDE, select Tools | Options from the main menu, and hold down the Shift key while clicking the OK button on the Options dialog. VFP writes all the options to the debugger output window, from which you can save them as a file.

While you could re-enter all your VFP options from the listing created in this way, it's a lot easier just to export the entire registry key so you can later import on another machine. To save your VFP options as a .reg file, open the registry editor and navigate to the HKCU\Software\Microsoft\Visual FoxPro\9.0\Options key. Right click on the key, choose Export, and enter a file name to save the key and all its values, as illustrated in Figure 2.

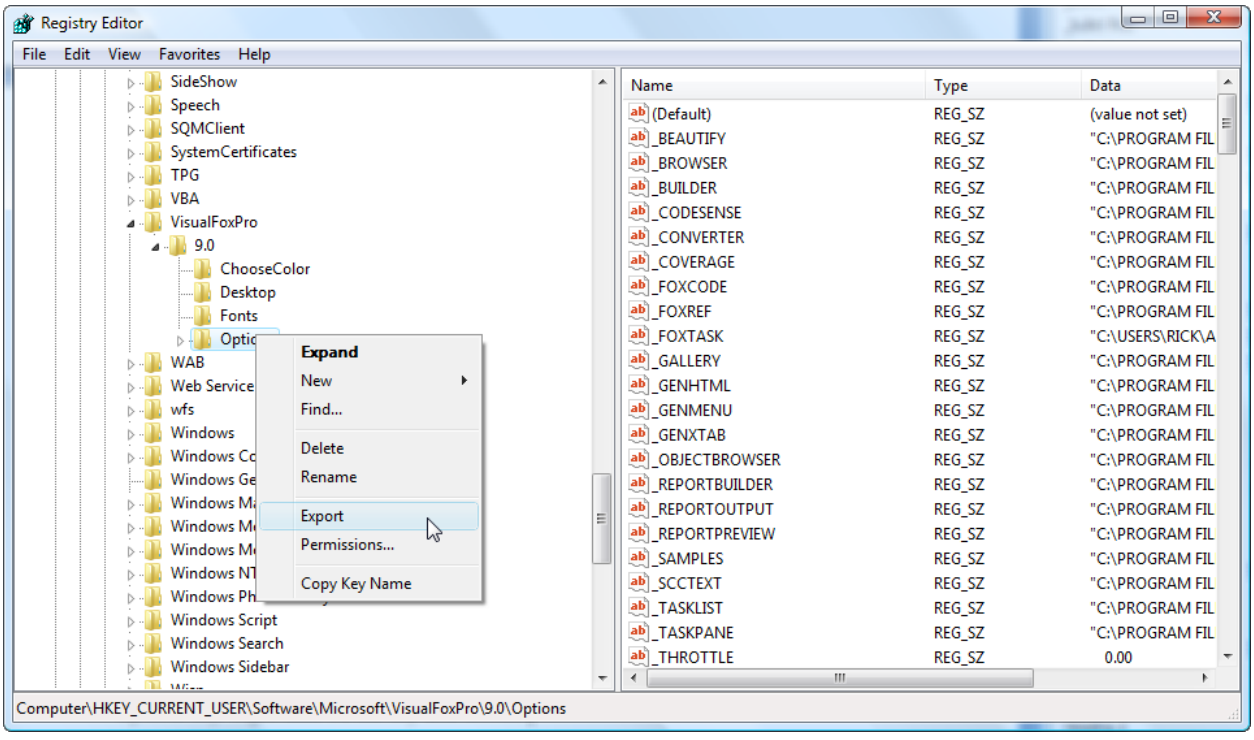

Figure 2: The VFP options are stored in the registry, from which they can be exported to a file using the registry editor.

As always, the standard caveats apply whenever you are working with the registry: be careful, make a backup first if you're unsure what you're doing, don't change or delete anything you don't understand, etc.

Finally, you may want to save your Intellisense Manager settings. By default, these are stored in a Visual FoxPro table named foxcode.dbf located in the VFP installation folder. The Visual FoxPro system variable _foxcode specifies the full path and name of this file.

Automatically backing up project files as you work

In addition to any backups you make as part of a regular, ongoing backup strategy, you may want to make immediate backups of VFP source code files as you work. If you mark the Make backup check box on the IDE page of the VFP Options dialog, as shown in Figure 3, VFP automatically makes a .BAK backup copy of any .PRG file you change.

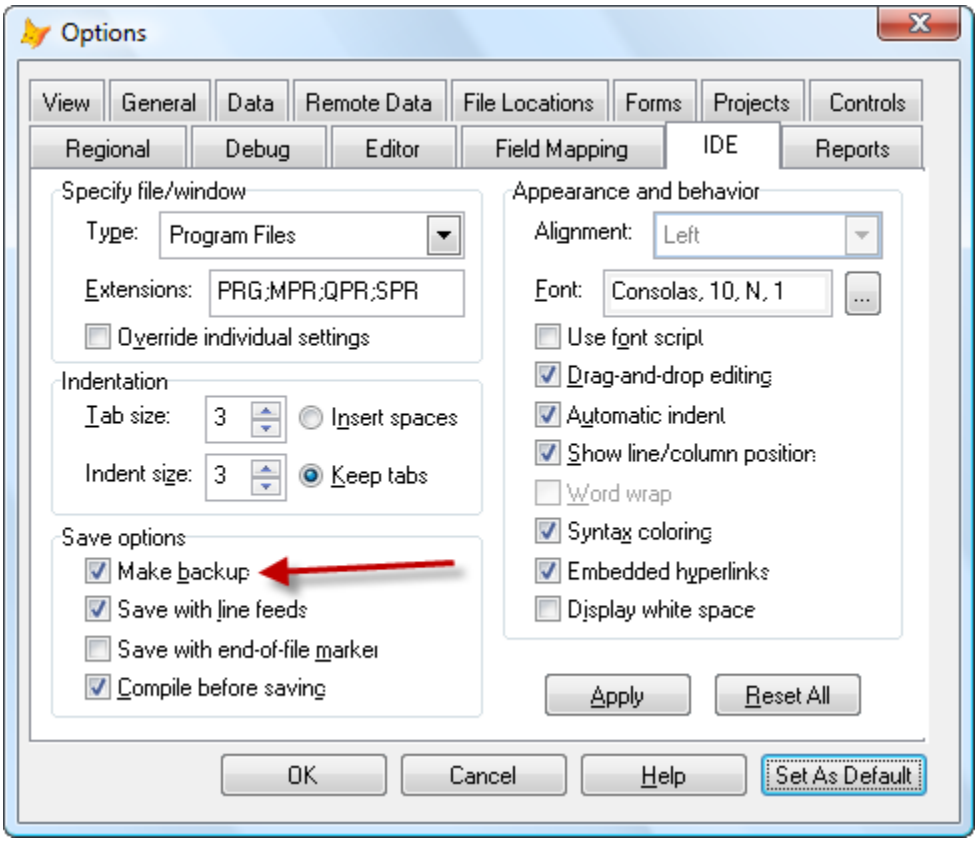

Figure 3: If you mark the Make backup check box, VFP automatically makes a backup copy of program files when you change them.

However, other types of files such as forms, reports, menus, and class libraries are not automatically backed up even when the Make backup check box is marked. Visual FoxPro

does not provide a native way to automatically create backups of these types of files as you work, but VFP does provide project hooks so you can use a project hook class to implement this behavior.

The FoxPro Wiki has an example of a class to backup these types of files; see fox.wikis.com/wc.dll?Wiki~ProjectHookExamples~VFP. Also, Rick Schummer has incorporated this backup feature into his WLC Project Builder and Project Hook tools, which are available for free from www.whitelightcomputing.com/prodprojectbuilder.htm. The WLC Project Builder is a most excellent tool that provides a consolidated interface to all of the options you typically want to manipulate when building a project. I've used it for several years and found it to be a real time saver, plus you get source code so you can see how it works and create your own subclasses for customization if you want to. When implemented, this project hook creates .ftk and .fxk backup files for reports, .stk and .sxk backup files for forms, .vtk and .vxk backup files for visual class libraries, and .mtk and .mxk backup files for menus.

Summary

A disaster can happen to any business at any time. Some of us may have been more fortunate than others, and some of us are exposed to more risks than others, but none of us is immune. The time and effort you invest now to create an effective disaster recovery plan will pay off handsomely in the future if you ever have to face the real thing.

Appendix

Following is a list of references, software utilities, and services you may find helpful in creating an effective disaster recovery plan for your business. The categorization is mine, and some of these tools may offer features that fit in more than one category.

General references

Department of Homeland Security – Disaster Preparedness Web site for businesses
www.ready.gov/business/index.html

National Preparedness Month 2009
www.ready.gov/america/npm09/index.html

Offsite backup, storage, and synchronization services

PC Magazine 2009 Utilities Guide – Backup/Sync
www.pcmag.com/article2/0,2817,2348839,00.asp

Mozy Online Backup (Mozy Home, Mozy Pro)
mozy.com

SQL safe backup
www.idera.com/Products/SQL-Server/SQL-safe-backup

Spare Backup
www.sparebackup.com

Dr. Backup
www.drbackup.net

Remote™ Data Backups
www.remotedatabackups.com

ADrive™
www.adrive.com

IDrive®
www.idrive.com

XDrive® [no longer in business]
www.xdrive.com

Box.net
www.box.net

Elephant Drive
https://www.elephantdrive.com

Amazon Simple Storage Services (S3)
aws.amazon.com/s3

Microsoft Live Sync (formerly FolderShare)
sync.live.com
www.foldershare.com

Dropbox
www.getdropbox.com

YouSendIt
www.yousendit.com

Windows Live™ Sync (formerly FolderShare)
www.foldershare.com

Windows Live™ SkyDrive
skydrive.live.com

SendSpace
www.sendspace.com

Syncplicity
www.syncplicity.com

Norton Online Backup
www.symantec.com/norton/online-backup

SugarSync
https://www.sugarsync.com

SOS Online Backup
www.sosonlinebackup.com

Carbonite
carbonite.com

Genie Online Backup
www.genie-soft.com/products/online_backup/default.html

Barracuda Backup Services
www.barracudanetworks.com/ns/products/backup_overview.php

BackBlaze
https://www.backblaze.com/

External hard drives, network attached Storage (NAS), etc.

ioSafe, Inc.
iosafe.com

Iomega
go.iomega.com

Seagate FreeAgent® Desktop and Portable Drives
www.seagate.com/www/en-us/products/external/freeagent

Desktop backup software

System and/or file backup

Acronis® True Image
www.acronis.com

PicoBackup
www.picobackup.com

Genie Backup Manager Pro
www.genie-soft.com/products/gbmpro/default.html

NTI Shadow
www.ntius.com

Second Copy
www.centered.com

ShadowProtect
www.storagecraft.com

Norton Ghost
www.symantec.com/norton/ghost

Username and password backup

RoboForm
www.roboform.com

RoboForm2Go
www.roboform.com/pass2go.html

Password Agent
moonsoftware.com/pwagent.asp

1Password (Mac)
agilewebsolutions.com/products/1Password

General purpose file compression

WinZip®
www.winzip.com

PicoZip
www.picozip.com

7-zip
www.7-zip.org

Uninstallers

Unclean uninstaller utility from PC Magazine Utilities
www.pcmag.com/article2/0,2817,1560662,00.asp

Revo Uninstaller from VS Revo Group
www.revouninstaller.com/

Commercial hard drive data recovery

Iomega Data Recovery Services
www.iomegadatarecovery.com/

Do it yourself hard drive data recovery

SpinRite
www.grc.com

Zero Assumption Recovery
www.z-a-recovery.com

Laptop security and recovery

Lojack for Laptops
www.lojackforlaptops.com/products/standard.asp
www.absolute.com/products/lojack

Laptop Cop
www.laptopcopsoftware.com

MyLoki
http://loki.com

Prey
http://preyproject.com

Undercover for the Mac
www.orbicule.com/undercover/mac

MacTrak™
www.gadgettrak.com/products/mac

Other

Magical Jelly Bean KeyFinder
www.magicaljellybean.com/keyfinder