

Materials for

## **AI.01**

# **The Sky Has Fallen! Disaster Recovery**

Dennis Kennedy  
The Dennis Kennedy Law Firm, LLC  
St. Louis, MO 63119  
(314) 963-0176  
dmk@denniskennedy.com  
www.denniskennedy.com

**ABA TECHSHOW 2005**

**April 1, 2005**

## **Table of Contents**

<b>Seven Ways to Avoid Disaster in Your Disaster Recovery Planning and Procedures .....</b>	<b>2</b>
<b>Ten Tips for Dealing with Disaster Recovery and Business Continuity Issues .....</b>	<b>4</b>
<b>Hot Topics in Disaster Recovery and Business Continuity Planning for 2005 – A Checklist.....</b>	<b>6</b>
<b>Top Legal Concerns in Disaster Recovery and Business Continuity Contracts – A Checklist.....</b>	<b>7</b>
<b>Software Police and Software Thieves: Stay Free By Knowing Your Rights.....</b>	<b>9</b>
<b>Negotiating Tips from Columbo .....</b>	<b>17</b>
<b>Resources for Learning About Disaster Recovery and Business Continuity .....</b>	<b>18</b>
<b>Biography .....</b>	<b>21</b>

## Seven Ways to Avoid Disaster in Your Disaster Recovery Planning and Procedures

What's worse than a disaster? How about doubling your disaster with a disastrous set of discovery plans, policies and procedures?

Disaster recovery and business continuity planning moved to center stage in IT planning issues in the last few years. While these subjects deservedly command the attention that they get, firms too often do not find the time and assets necessary to pay full attention to all the issues and execution of good plans often remains a problem.

The fact is that nothing sharpens a disaster plan more than suffering a disaster. However, as time begins to stretch out after the last disaster, the energy, focus and urgency of disaster plans tends to dissipate. Great plans and procedures gradually grow inadequate and irrelevant. They also tend to focus on "fighting the previous war." Part of a good plan is to address this inevitable inertia.

What steps can you take to improve your planning and procedures and prevent preventable disasters? While no plan can account for every contingency or be totally bullet-proof, the following seven steps will help you avoid adding insult to injury from self-inflicted disasters.

**1. Determine Your Core Business, Really.** They call it business continuity for a reason. Everything flows from accurately determining what your core business is, including priorities, policies and procedures. Unfortunately, if you ask everyone at a law firm what the core business of the firm is, you probably will not find a lot of consistency in the answers. If that is the case at your firm, you should be worried about other things than just disaster recovery, but lack of understanding of the core business almost certainly will lead to problems in the event of a disaster. It is essential that key managers and firm leaders be involved in the disaster planning process. It's also instructive to read and listen to the stories of firms that have made it through big disasters. Pay attention to what they focused on for both the short term and long term. **A common theme is enabling fee-earners to return to generating fees for paying clients as quickly as possible.** It's easy to focus too intently on technology issues when the big concern is generating cash flow to keep paying employees and moving forward. Be a pest and force the decision-makers to make decisions about core business elements that must be protected and quickly restored.

**2. Use Scenario Planning.** The easy approach to disaster planning is to create a checklist of issues and find ways to address each of them. Unfortunately, as the military maxim goes, no plan survives first contact with the enemy. Working through a number of "what if" scenarios will help you find holes in your planning and identify real and important issues. It is not a well-conceived plan if it is dependent on managing partners surviving and everyone returning to the office the next day. Wipe out the executive committee in a scenario and see how you plan works. Question your assumptions. Create plausible story lines. Do you like the movie "Die Hard"? Run your disaster plan under the Die Hard scenario and see what happens.

**3. Write the Plan As If You Will Have to Read it Someday.** Make no mistake – unless you have a written plan, you don't really have a plan. Take out your plan and really read it. Is it filled with platitudes and assumptions? Do you see steps that say nothing more than "Restore network operations"? Imagine you are not there and someone untrained has to pull out the plan and use it. Can they?

**4. Negotiate Great Agreements.** Firms are starting to look at outsourcing many aspects of disaster planning. What are your third party providers obligated to do under the contracts you have signed? Is it adequate or even helpful? Can you get out of agreements and move to other providers? What service levels must be provided? What happens if they are not provided? If you do not raise and negotiate issues, I guarantee you that the terms of any contract you sign will be more favorable to the provider than they are to you.

**5. Adopt a Portfolio Approach.** The modern approach to financial investments emphasizes diversification and mixing low-risk, low-return ("safe") investments and high-risk, high-return ("risky") investments in a basket that reflects your risk tolerance. The same concepts have recently migrated into the world of IT planning. You can also think of this approach as "not putting all your eggs in one basket." Consider a variety of approaches, overlapping techniques and both novel and standard approaches. Diversify your risks, responses and procedures.

**6. Focus on Failure and Redundancy.** There is a notion in disaster planning known as "elegant failure." The idea is that failures will happen and it becomes important to know what happens after the failure. In "elegant failures," the fix is a good and effective one. For example, if I have a backup email service that comes into action within one second of a catastrophic Exchange Server failure, I have an elegant failure. If my firm loses email service for three days and attorneys have to use Hotmail accounts for email, I do not have an elegant failure. Look at various points in your processes and procedures. Consider what happens when a failure occurs at each of these points and the options that you may have. Can you set up some elegant failures?

**7. Test Rigorously and Repeatedly.** When I was in school, we had fire drills on a regular basis. I have no doubt that we would have gotten out of the school safely in the event of a fire. On the rare occasions that I've been involved in fire drills or false alarms while at law firms, I had no doubt that few people would make it out alive if a fire actually occurred. It's important to test your plan, practice your procedures and do so on a regular basis. Lackadaisical practicing and testing guarantee poor results when something bad actually happens.

**Conclusion.** My best advice is to treat these matters as if they actually matter. Your livelihood and your life may be at stake one day and you will regret any half-hearted steps that you made in the past. Make time for disaster recovery, be a pest at getting answers to your questions, challenge assumptions, develop a thick skin for deal with the ribbing you are likely to take for being "too serious," and keep in mind that we live in volatile and dangerous world.

## Ten Tips for Dealing with Disaster Recovery and Business Continuity Issues

If disaster strikes, your success will be determined by your people. How will they react? How have they been trained? Have you given them the tools they need?

Many of the articles you will find about disaster recovery and business continuity tend to focus only on technologies to consider and the proper formats for your written plans. These are, of course, important topics, but you cannot overlook the human element.

Let's take a look at ten things that can get overlooked if you pay too much attention to only the technical issues, but that will play a vital role in your ultimate success.

**1. Identify the Key People.** What people will play key roles in disaster recovery? What happens if they are not available? Who are the backups? Who are your leaders? Who do you want with you in a crisis? Let's face it, some people will react better than others will in a crisis situation. Identify them. Assume that there is a disaster. Do you know who will be sitting in the room when the first decisions must be made? Why not?

**2. Select Your Teams.** Disaster recovery and business continuity both require a high level of cooperation and collaboration. In addition, people have to care about the organization enough to be willing to work at getting it back into action. Putting together teams and training them in advance will make a world of difference. Do you have your teams in place?

**3. Designate a Meeting Place.** Assume that your office is destroyed. Where will your business then be located? How will you know who is missing? Where will you meet to get things restarted? Designating places to reassemble may turn out to be the best first step you can take.

**4. Update Your Scenarios.** Pay attention to the news. Read the latest thrillers. Watch 24, other spy shows and suspense movies. How would your plan work in these scenarios? Play out different scenarios. Question your assumptions. Is your plan really just a plan to "fight the previous war"?

**5. Involve Lawyers and Clients.** Is disaster recovery just an IT function? I don't think so. Part of the learning from 9/11 is that clients are willing to help law firms get through difficult periods. Is your law firm willing to do the same for your clients? Are there ways you can make preparations in conjunction with your major clients own plans? Do you know what your lawyers will need, and in what order? Have you talked to your lawyers or are you just making untested assumptions? Make it a priority to have these conversations.

**6. Get Agreement on What Really Matters.** Setting priorities in a crisis can be impractical at best and impossible at worst. Think through these issues in advance. If all of your communications are wiped out, what do you restore first? If you make your decisions in advance, your task will be one of implementation. If you do not decide on priorities in

advance, you'll have many voices clamoring that their individual priorities matter most. In that case, everyone loses.

**7. Run Some Fire Drills.** In times of stress, we can get some sense of stability by performing routine matters that we have practiced before. Firefighters can handle completely new fire situations under enormous pressure because they have experience and they practice on a regular basis. Do some dry runs and tests. Evaluate what happens rigorously. If you fail in practice, what gives you confidence that you will be successful in a real crisis? Must you change your plans? Restore your backups and see what really happens. Reset the whole system on the fly and see if your procedures work. Give your people a chance to learn the skills that they will need and to practice enough to be comfortable. Reward successful drills and dissect what went wrong in failed drills.

**8. Publicize Your Procedures.** After 9/11, I checked and could not easily find evacuation and other procedures for my then law firm and the building I was in. Imagine how you increase the level of panic by not making procedures and instructions readily available in an emergency. Are you assuming that someone will activate the 911 system when no one is assigned that task? How many people have the authority to activate your off-site disaster recovery systems? What happens if they aren't available? Are they all still with your firm? Highlight the general approaches you will take and make the plan easily accessible.

**9. Get Top Management to Treat These Issues Seriously.** I am the son of a volunteer fireman, so I might think about some of these issues more than others do. Whenever I hear about firms where executive committee partners do not bother to participate in fire drills and other emergency matters because their time is too valuable, I become concerned that this attitude will filter through the organization, resulting in senseless deaths because fire alarms are not treated seriously. If top management does not help plan, participate in and endorse your efforts, there is little chance that they will be effective when a crisis comes, unless you are very lucky.

**10. Deal with the Cultural Issues.** I've worked in places where people waited around when fire alarms went off to find out whether they were "real" or not. If an alarm is real, they've reduced their chances for survival. In the IT area, some firms have cavalier attitudes about backup and disregard other standard practices. In other firms, preparations for disaster and crisis are seen as subject for humor or even derision. Education must play a key role. You can make important points about these issues with humor, but training is no laughing matter.

## **Conclusion.**

Disaster comes in many guises. I was at a firm with the proverbial one-person IT department and one morning found an envelope on my chair with our IT department's pager, keys and resignation letter. We did not have a plan for this contingency. Fortunately, we had three people who could address the issues on the fly, but I didn't get any legal work done that day. Nothing sharpens your disaster planning like a good crisis. However, I have come to the conclusion that the more you can prepare for up front, the better off you will be. The key to your successful navigation of a crisis will be your people and your main goal is to get them the instructions, training and tools to be able to do the job when that unfortunate time comes.

## Hot Topics in Disaster Recovery and Business Continuity Planning for 2005 – A Checklist

- Data Recovery.** Almost every scenario contemplates a catastrophic loss of data. How will you recover and restore your data? Have you verified backups and tested your ability to restore? How much data simply will not be able to be restored? What are the consequences? How will you get your backup data? What is required to get your data back? Viable transportation? Internet or telephone access? What happens if you do not have them?
- Security.** As you ramp things up to get your business going again, have you opened your data and systems to outsiders? Is security continuity an element of your disaster recovery planning? What steps will you take to ensure security and confidentiality of information? Are passwords still secure? What might be compromised?
- Regulatory.** Do you have obligations under Sarbanes Oxley or other regulations? Are you handling medical data, trade secrets, material subject to discovery or data subject to court order? What about filing deadlines?
- Best Practices.** Are you keeping up with best practices in the industry? Where do you find them? What do you read, what seminars do you attend and to whom do you talk about these things? What can you learn from successful (or unsuccessful) experiences of others? What are your clients and vendors doing?
- Number of Locations.** Centralized or decentralized approaches? Minimize the number of data centers, but harden them? Use application service providers or other outsourcing services?
- Technology Choices.** Are you relying on proprietary, hard to replace or obsolete technologies? Do you have adequate licenses and replacement parts? Are there credit lines in place or vendors identified for fast replacements? Are you constantly evaluating the technology you use in comparison to what is becoming available? How dependent is your technology on a few key people? Are you doing it yourself when outsourcing or application service provider models make better sense?
- Grid and Infrastructure Issues.** Assume that your power or telephone system is taken offline for days or weeks. What will you do? Does your disaster planning consider those contingencies? What about loss of bridges or other key infrastructure? It's easy to say, "Well, I guess we'll all just stay home," but what will that mean on pay day?

## Top Legal Concerns in Disaster Recovery and Business Continuity Contracts – A Checklist

- General.** What do you expect will happen in the event of a disaster under your existing agreements? Now check them and see what they really provide. The provisions of disaster recovery services agreements will become extremely important in the event of a disaster. Do not be cavalier about signing standard contracts. Be prepared to negotiate for the language and obligations that you need from vendors.
- SLAs.** The three most important letters in IT contracts – SLA. SLA stands for Service Level Agreement, but SLA has come to mean the section of IT agreements where specific performance requirements (uptime, redundancy, support, service levels, et al.) are spelled out in detail. The more time you spend getting your requirements clearly listed, the better off you will be. Ideally, you want a vendor to provide a warranty that it will meet your performance requirements.
- Force Majeure.** A "force majeure" clause generally excuses non-performance in the event of catastrophic occurrences. In a disaster recovery contract, you want guarantees that performance *must* happen in certain catastrophic situations. Force majeure clause are generally considered part of the "boilerplate" of a contract and given little consideration. In a disaster recovery contract, they must be evaluated carefully and customized to ensure that you get the services you require when you need them.
- License Rights.** Watch out for surprises in license language. What happens if you have a software license limited to a certain location? Are you allowed to use it at your off-site disaster recovery center? What if that location is destroyed? Pay careful attention to limitation on the number of backup copies you can make and other limitations that may cause difficulties in the event of a disaster.
- Confidentiality and Security.** Disaster recovery is increasingly being outsourced. Do your contracts with vendors and service providers adequately address your confidentiality and security obligations and concerns?
- Assignment.** In the event of certain disasters, you might want to create a new entity or split the business into multiple new entities. Can you transfer software licenses and disaster recovery services to the new entities? Will the new entities have the right to retrieve or make copies of backup data?
- Exit Strategies.** A key strategy in disaster recovery is to create multiple options. Do you have the ability to quickly leave one provider and move to another provider? If you get nervous about a company or its prospects, is it easy to move to other providers? How quickly can you move? What does it cost to switch? How and when will you get your data back? Is a provider obligated to help you make a smooth transition to another provider?
- Liability to Third Parties.** Do you have recourse against a service provider in the event that you are sued by a client or vendor because your service provider failed to meet its

obligations? Do you specify in your contracts that service providers must meet your requirements on confidentiality, privacy and other regulatory matters? Might your disaster recovery procedures inadvertently waive attorney-client privilege or have other consequences.

- Costs.** How are services priced? Are increases permitted? When are costs re-evaluated or renegotiated?

## **Software Police and Software Thieves: Stay Free By Knowing Your Rights**

The clash between software companies wanting to protect their intellectual property rights and revenue streams and software users comparing their balance sheets to that of Bill Gates continues in full force and has begun to pull in a wider cast of characters. The “software police,” the most well-known of which is the Business Software Alliance (“BSA”), have moved from large enterprise targets to schools and small businesses. In 2004, law firms and lawyers who think that they are below the radar may find themselves getting a rude awakening.

As prices of hardware continue to fall, a computer user now finds that the cost of the software for a computer can easily far exceed the cost of the computer. Software prices have not dropped in the same way as hardware prices have and now account for a larger percentage of technology budgets.

The simple fact is that computer users hate to pay a lot for software. People will look at shareware, freeware and other types of software. They will use “loaner” copies, “borrow” someone else’s copy of a program, and install the program on multiple machines. The downloading of pirate copies, taking advantage of “highly discounted” prices, pretending downloaded “free” program files are not illegal, and using other “gray area” techniques have become increasingly common and cost software companies billions of dollars in lost revenues.

### **The Key and Often Misunderstood Subject of Licensing.**

Many people, including lawyers, simply do not understand the whole notion of software licensing. Software is not sold like other products. Instead, the “purchase” of software actually means buying the media containing the software and a license to use the software and the intellectual property rights associated with the software. Without such a license, your use and copying of the software would infringe these rights.

Unlike other products, you cannot do whatever you wish with a software program. Your use is governed by the license of intellectual property rights you receive. A license can “slice and dice” the intellectual property rights in a nearly endless number of ways – number of copies allowed, where the software may be installed, who can use it, and for what purposes, to name just a few.

If you buy a 12-pack of beer, you can share it with friends, take it anywhere you want, drink it out of the can or a glass, and even pour it on the ground and crush the can on your forehead. You get the idea. Imagine that you bought the beer and found that, simply by buying it, you agreed only to drink it yourself, only in your home with no others present, and you could keep it in a refrigerator but not a cooler.

That just doesn't seem right somehow, but that's kind of the way software licenses work. The typical software license puts any number of restrictions on the way you can use the software or, more precisely, the intellectual property rights in the software.

In general, if you copy or make use of a program without a license to copy or use it in that particular way, you will be infringing the rights of the owner of the intellectual property owner. The license, in essence, allows you avoid a claim of infringement. As a result, the general rule will be that if the license does not allow you to use software in the way you are using it, you simply cannot use it in that manner. Indeed, the presumption is that you cannot make the use unless the software license clearly authorizes it.

As a practical matter, however, these legal nuances are implemented by setting out a limited set of rights and specifying restrictions and prohibitions. We generally look at licenses to see what we can do more so than for what we cannot do. That is, of course, if we look at it at all.

### **How in the Heck Did I Agree to That?**

Most of us are familiar with software license agreements only as lines of small type that we see briefly as we click on the "accept" or "I agree" button in order to proceed with the installation of the software. These "clickthrough" licenses are easily today's most commonly unread legal documents.

The current state of the law is that a contract of this type will be considered valid and enforceable, assuming that there is a reasonable way for the user to access the terms of the contract and a reasonable way for the user to manifest assent. However, specific provisions, especially arbitration and choice of venue requirements, may be found unconscionable or otherwise not enforceable. This area of law continues to evolve, but, at this point, it is unlikely that a court will hold as a general principle that "clickthrough" contracts are not valid or enforceable.

Because of the way these license agreements are presented and because people rarely read them, the terms and conditions for the use of a software program often surprise the software licensees. You might have a good surprise – you can install a program on both your desktop and laptop computers for no extra charge – or a bad surprise – the license is limited to the specific computer that just died.

Obviously, it is a great idea to read the provisions of a software license before you agree to it. However, that practice is rare indeed and might even be impractical. For example, if we can only get the necessary critical security update from Microsoft that we need to protect us from a rampaging virus if we click on the "accept" button, can we meaningfully consider the terms of the agreement?

### **What Makes A Pirate?**

Once you understand the concept of licensing, the notion of piracy becomes much easier to grasp. Remember copying or making use of software will be considered an infringement of the software company's intellectual property rights unless the user has a license to make that specific use or copy.

If you do not have any license, act outside the scope of your license, or use the software in manner prohibited by the license, you are an infringer. Intention does not matter.

The most common violation is having more users on a network running a program than you have licenses. Other common violations include:

- Installing a program with a single license on multiple computers.
- Making more copies of a program than allowed (licenses commonly allow an operating copy and one backup copy).
- Using “upgrade” versions without having a legitimate underlying license.
- Improperly using academic and OEM versions of programs.
- Downloading or purchasing and using “free,” highly discounted or other dubious copies that do not contain legitimate authentication materials.
- “Borrowing” a program from a friend or using office software at home.

Note that it is easy to inadvertently violate license provisions and lack of adequate recordkeeping often leads to problems. In other words, you can easily be a “pirate” without intending to be bad. By the way, the arguments that Bill Gates already has enough money and that you did not have money for licenses and did not believe that you would be audited do not carry any weight.

### **Bad Consequences – Whether or Not You Are Caught.**

Copyright infringement carries both civil and criminal consequences. In the United States, an infringer may be liable for damages and for any profits of the infringer attributable to the copying. Are you thinking that since you are small potatoes these damages won’t amount to much? Does the availability of statutory damages up to \$150,000 for each work infringed or criminal penalties of fines up to \$250,000 and imprisonment of up to five years get your attention?

What if it was an employee who did the pirating and you knew nothing about it? The law on vicarious liability for infringement leaves little doubt that you will be liable for the actions of an employee.

Even if you don’t get caught, software piracy can result in the introduction of viruses and security holes into your systems, non-availability of technical help, inability to get updates and patches, and the continued use of obsolete software. In today’s computer security environment, you are begging to become a hacker haven.

Ironically, the idea that you are saving money by going outside software companies’ licensing programs may well be misguided. Volume discounts often are available for as few as five copies of a program. Support, upgrades and other benefits are part of some licensing programs. Microsoft, for example, now has a rebate program for Office 2003 and a new

“home user program” that allows you to give your employees a copy of certain programs to use at home, which could be provided as a new employee benefit. Also, under Microsoft’s licensing program that allows you to use earlier versions of programs when you license current versions, you might be foolishly throwing away your money on cut-rate, dubiously-sourced older versions. Some Microsoft licensing programs even let you keep track of and manage licenses electronically.

Finally, be aware of the risks of promoting an atmosphere in your firm where bending the rules, ignoring requirements and even theft is tolerated. Remember the doctrine of vicarious liability for infringement. Software piracy may turn out to be the least of your problems.

### **Uh-oh, You Got an Audit Letter.**

The BSA and other software police are concerned with only the big offenders, right? Consider the example of the Internal Revenue Service. Visibly going after the little offenders with gusto helps keep everyone in compliance.

The fact is that in the great majority of situations, a phone call or an e-mail to BSA from a disgruntled (or law-abiding) employee or former employee will bring you under the microscope. The employee, especially one who has unsuccessfully tried to convince you comply with license requirements, will probably know what the violations are and where to find them. If his or her story is convincing, you may well receive a letter asking you to demonstrate that you are in compliance with your licenses.

It is important to emphasize that running out and buying the licenses you need after you get a letter does not cleanse you of the problem. It simply gets you to where you need to be from that day forward. You still are on the hook for the infringement that occurred before you came into compliance. Audit letters typically state that the software inventory must be accurate as of the date you receive the letter.

What about deleting extra copies and taking other steps to hide what you did after you get the letter? Seriously, what do you think? They taught you the answer to this one in law school, if not much, much earlier. Remember that someone who knew what you were doing turned you in and the auditing party has a good idea of what you were doing.

As a general principle, you do not want to ignore an audit letter. The BSA, in particular, can be very persistent. The BSA’s position is that complying with an audit request simply means counting the copies of the programs you have and then counting the number of licenses you have. What could be simpler? Don’t expect to get a lot of slack on extending the deadline for a response.

As a practical matter, the state of recordkeeping and software management in many organizations can best be described as “mayhem.” You will not realize the extent of this mayhem until you try to establish proof that you have valid software licenses. Stories of companies spending thousands of dollars in staff, management and legal time responding to audit letters are not uncommon.

What you are likely to find is a mixed bag of licenses that raises several problems. You may have too many licenses for one version of a program and not enough for another version. As a general rule, a license for a newer version will cover a copy of an older version, but not vice versa, but that is not always the case. You might find that your biggest infringement problem results from a program that is installed for everyone but used by only a few people. The Adobe Acrobat Writer, Microsoft Excel, and Microsoft PowerPoint are examples of programs that fall in this category. You will also find that you have software that you know that you paid for, but do not have any documentation or proof. Unfortunately, as a practical matter, the burden of proof is on you.

Assuming that you were not operating in flagrant disregard of your license rights, you will turn in your inventory results and proof of licenses, likely showing one or more shortcomings. As a practical matter, you will get an offer to settle by either deleting infringing copies or purchasing the needed licenses and paying a “settlement” amount to cover infringement damages in exchange for a release of claims against you. You may have some room to negotiate this amount down, but don’t expect too much.

It is worth noting that some lawyers recommend not responding to an audit letter, especially if the response admits liability. The software police, however, have no problem with pursuing litigation. In fact, at least one organization has a map of the United States on which you can click on a state and see a list of infringement actions in that state.

The results of receiving an audit letter, then, are loss of time and money, a possible news story about you, lots of stress, and ending up where you should have been in the first place on your software.

### **Taking Charge of Your Compliance.**

Here are a few questions for you to consider. What feeling do you get in the pit of your stomach when you think about looking at the results of an audit of your software license compliance? When you try to picture the current state of your software license records, what do you see? How much work do you think it would take to get things in order?

You are not alone in your answers. It is hard enough simply to keep on top of licensing for one person using one computer. How many receipts, proof of purchase labels, front pages of manuals and similar proof of ownership items can you find for the software on your home computer? Can you trace your version upgrades back to the original program you bought? How many of your programs are you confident that you are using in accordance with the license restrictions?

The issues expand exponentially as you network an increasing number of computers for an increasing number of users in an increasing number of locations.

The excuse that you aren’t the only one violating licenses, of course, will carry no weight whatsoever when the audit comes.

What steps should you take to take charge of your software licenses and maximize your level of compliance? The following steps will help you avoid losing sleep over your software

situation, might even save you money and let you use newer software, and will give you credibility when you talk to your children about why they should not be illegally downloading music files.

- 1. Inventory Your Software and Hardware.** Everything starts with getting a handle on what you have and what you are doing. Some firms could not accurately tell you how many computers they are using, let alone all the software programs they are running. It is important to include hardware in the inventory because a few licenses require that a program be operated only on a certain computer or even on a specific processor. The inventory should result in a list of (1) all installed programs, (2) the computers each program is installed on, (3) all users of each program, (4) all uninstalled software disks, boxes, manuals, and other paperwork, no matter how old the program is, and (5) a brief description of what each program does, ideally with the name of the person who knows the most about the program. Make sure that the right people, including an outside consultant if necessary, are involved in the process and understand its timeframe and importance. Daily emergencies are very likely to intrude on this project.
- 2. Locate the License Agreements, Receipts and Other Documentation You Have for Each Program.** Unfortunately, you can only work with what you have. Scour your office for whatever might be applicable.
- 3. Match Up Programs and Licenses.** This task is likely to be both tedious and frustrating, but it is a job that has to be done. Using a spreadsheet (make sure at least the copy you use is licensed) to enter and track this information is a good method. Your information can be put in a chart format and calculations of numbers can be done automatically.
- 4. Make a Preliminary Assessment of Your Findings.** It's time to face the music. Look for obvious errors. Assess whether the findings make sense based on your memory of how the software was obtained. Identify both the major problem areas and the unexpected programs and users that you have found. You can also do a little triage to take steps to remove programs that are unapproved, clearly unlicensed or installed for users who do not actually use them.
- 5. Do Some Detective Work.** Seeing the initial inventory will probably jog your memory about what other records might be found. Letting others in your office know what records still need to be found may lead to clues about where records might be located. Going back to the sales representative or consultant involved with the software might help you locate originals, copies or other documentation you need. Remember that your right to use some programs may stem from a consultant's license.
- 6. Roll Up Your Sleeves and Study the Inventory.** Once you satisfy yourself that you have all of the information that you are going to get, study it carefully. You may find that this is the first time you have ever had a full picture of what technology you actually have. The list may well surprise you. Again, identify issues that can be dealt with quickly and easily.

- 7. Work on an Action Plan.** The bonus you will get from the inventory process will be that you can identify unnecessary costs and other inefficiencies. Are you paying annual maintenance fees for programs no one uses? Are expensive new programs even being used? Do you have more licenses than you need for certain programs? You also want to focus closely on programs for which you do not have a sufficient number of licenses. In some cases, you can handle these deficiencies by restricting the number of users or, in the case of obsolete or rarely used programs, by deleting them and moving on to different programs. At the end of this process, all the major issues should be identified and a list of next steps should be completed.
- 8. Read the Licenses.** As a general rule, you can assume your license agreements will be shockingly one-sided and not in your favor. You can focus on (1) the license grant language, (2) specific restrictions and prohibitions, and (3) any rights to transfer or assign licenses. Obviously, you will want to make note of any limitations or restrictions, but you will also want to look for rights that you may have, such as the right to install on a laptop or home computer, of which you were not aware. It makes sense to add a summary of the license terms to your inventory spreadsheet for quick reference. More bad news: the license agreements that you have may not be the license agreements that still apply. The Microsoft licenses, for example, have changed a number of times over the years. Corporate mergers might have an impact on some licenses and many software companies have gone out of business over the years.
- 9. Do Your Best to Get Things in Order.** As you might have guessed by now, the odds are quite low that you will be able to dot every “i” and cross every “t” on your software compliance. You will have to make some judgment calls based on your level of comfort with your documentation. You might change, delete or restrict the use of programs. You might consider purchasing additional licenses. In general, however, you want to reach a point where you are comfortable with your level of compliance.
- 10. Explore Today’s Licensing Alternatives and Other Options.** You may find that your situation is beyond repair, that you never want to let things get to state they were when you started, or that you simply want to find a better way to get your license compliance under control. You may also find that you are using programs from companies that are no longer in business. As mentioned above, today’s software licensing programs may offer you helpful licensing provisions, technical support and training options, upgrades to new versions, rebates, payment plans, volume discounts and license compliance management of which you were not aware. Any law office with at least five users (or the expectation of growing to five users) should definitely look into the Microsoft Open License Value program, but other software companies may also have good arrangements. If you have gone through this process, you will certainly now know the questions to ask.
- 11. Implement a System to Stay in Control.** Keeping in compliance consists of one part putting together a good system and one part picking the right people for the job. Be aware that there is a common perception that good technical people tend to be poor record keepers. It may well be the case that your bookkeeper or a secretary might be the right person to give the responsibility, especially if you do not have a full-time or part-time technology person. The system, however designed, should result in the keeping of an

accurate, up-to-date inventory that can produce the information you need quickly. As part of the process, the license terms for any new programs must be read and understood. Finally, consider adding the discussion of acceptable software use to your orientation materials for new employees, employee or office procedures manual or employment agreements.

**12. Lead by Example.** In cases of wide-scale software piracy, you will probably find in the firm leadership either a tolerance or encouragement of license violations. Your staff will react to what you do more so than to what you say. When you take a new program home to load it on your home computer, download unauthorized programs, ignore requests to buy additional licenses as your firm grows, or instruct your tech person to install “academic” or OEM versions of programs, you send a message that will almost certainly result in license compliance problems. On the other hand, when you show your staff that you pay for all your software, turn down requests to install unlicensed software, routinely request and make sure that any additional licenses are ordered and paid for when needed, and publicly check license terms when a question arises, you create an environment where compliance with software licenses will be as nature and commonplace as compliance with your other important procedures and practices.

### **Go Forth and Sin No More.**

As a small firm or solo lawyer, you need to know that you may well be the target of a software compliance audit. Many audits are initiated on the basis on a tip from people who know your practices. Violating software license terms may have serious consequences, including business costs, civil liability, criminal penalties, and serious security vulnerabilities. Dealing with an audit request will be time-consuming, expensive, and embarrassing. You don't have to think and act like a pirate to be a software pirate under intellectual property law.

Good software compliance makes good business sense. In today's world of licensing programs, even small firms may qualify for discounts, special programs and other benefits. Even the smallest firm is likely to find that its software use varies significantly from its license rights. Using the twelve-step process set out in this article will help you address your license compliance issues now and bring you many benefits in addition to protecting you in the event of future audit.

## Negotiating Tips from Columbo

My daughter and I have been watching reruns of the old Columbo TV show. It struck me that there are some good lessons to learn from these shows about contract negotiations. Consider these:

**Do Not Underestimate the Opposing Party.** The criminals always make the assumption that Columbo is not an opponent who matches up to the high opinion they have of themselves.

**“Bear with me; I’m just trying to understand this.”** Columbo often uses this tactic to get his adversary to spin out explanations of events in ways that show contradictions. Try this: “Bear with me; I’m just trying to understand how if your software infringes someone’s copyright, and we can’t even see the source code, why should we bear that risk instead of you.”

**“My superiors want me to tie up all the loose ends.** You know how they can be.” This tactic is actually a variation of #2. The advantage is that you can keep a friendly relationship and blame the boss.

**Be Polite But Persistent.** Columbo uses a very high level of patience combined with a dogged persistence. He remains personally likeable while continuing to move toward his goal. The opposing party still likes you, but they just want you to stop coming back to the same point about the damage cap, and may become willing to give on the point.

**Ask for the Opposing Party’s Help.** A good tactic when you reach the endgame stage. “Can you help me out? If we can just get these two points, and they really aren’t big ones, then I know we’ll get the signature and put this one to bed.

**“Just one more thing.”** Columbo says this signature line just as he gets to the door to leave, as he seemingly remembers a small point - almost as an afterthought - that, in fact, was the main point of his conversation. Psychologically, Columbo’s opponent has already mentally “closed the door” on the conversation, dropping his or her guard, and leaving an opening to make the point with greater effect.

## Resources for Learning About Disaster Recovery and Business Continuity

*Eight Best Practices for Disaster Recovery – CIO Executive Council*  
(<http://www.cio.com/go/index.html?ID=801&PMID=34625&s=1&f=1>) – Great starting place.

*Baseline Magazine* (<http://www.baseline.com>) – Excellent coverage of practical technology issues.

*ComputerWorld* (<http://www.computerworld.com>) – Covers many practical IT and business issues.

*CFO.com's Technology Section* (<http://www.cfo.com/channel/1,5357,6,00.html?f=topic>) - CFO Magazine does a great job of covering technology issues from the point of view of a business decision-maker. Often you can find solid, practical information on today's most important IT issues, such as a recent comprehensive article on Sarbanes Oxley compliance.

*CIO.com* (<http://www.cio.com>) CIO magazine (the print version is free to qualified subscribers) consistently provides articles and other resources on a variety of contracting issues and trends, usually with excellent real life examples.

*DennisKennedy.Blog* - <http://www.denniskennedy.com/blog/> - My blog (with an RSS feed) covers a number of topics, but will occasionally mention items useful on the topics of disaster recovery and business continuity issues.

*Don't Skip on the Details: Structuring and Documenting the Real Content of Outsourcing Agreements* (<http://www.outsourcing-journal.com/issues/apr2002/legal.html>)

*Drafting Successful ASP Service Level Agreements*  
([http://www.internetindustry.com/mag/01\\_02su/18dra/](http://www.internetindustry.com/mag/01_02su/18dra/))

*GigaLaw.com* (<http://www.gigalaw.com>) - A great site for all sorts of practical (emphasis on practical) articles on a variety of e-commerce, IP and other legal topics.

*It's All in the Fine Print* (<http://www.utsystem.edu/OGC/intellectualproperty/contract.htm>) - The University of Texas has created a great set of resources for handling technology contracts. It includes checklists, explanatory material and other help.

*Let's Make a Deal: Negotiating Skills for IT Managers*  
(<http://www.computerworld.com/managementtopics/management/story/0,10801,86195,00.html>) – As this issue's feature story suggests, getting good contract language requires good negotiation skills. My job as a lawyer gets much easier when you do a great job of negotiating terms.

*License Agreements: Forms and Checklists*, by Gregory J. Battersby and Charles W. Grimes, editors (Aspen Publishing) - A very good "forms with analysis" book on licensing

agreements that comes with a CD-ROM Includes 60 sample agreements, introduction and analysis of forms, and clauses and discussion of hot issue topics.

*Negotiate This! By Caring, But Not T-H-A-T Much*, Herb Cohen – Herb Cohen wrote his classic negotiation book, *You Can Negotiate Anything*, over twenty years ago. In 2003, he finally followed it up with *Negotiate This!* book, which has met with rave reviews.

*Seven Key Questions for Drafting Effective Exit Provisions* (<http://www.outsourcing-journal.com/issues/aug2002/legal.html>)

*Ten Essential Ingredients for a Solid Service Level Agreement*  
(<http://www.documentiq.com/resources/tips/191-DocumentIQ%20Tips.html>)

*Ten Steps to a Successful Security Policy* (<http://www.computerworld.com/securitytopics/security/story/0,10801,85583,00.html>) - Protecting your security obviously takes more than covering security issues in contracts. This article sets out the standard practices for developing a good security policy.

Thomas Haggard, *Legal Drafting in a Nutshell* (West Publishing Co.) - This handbook contains much useful information about good drafting and explains a large number of standard terms, approaches and conventions. I wholeheartedly agree with Haggard's maxim that legal drafting is about problem prevention.

*Working with Contracts: What Law School Doesn't Teach You*, by Charles M. Fox, is exactly what the subtitle describes. In about 300 pages, Fox provides a primer on a whole range of contract clauses and techniques and a good reference for particular questions that may arise. Written by a lawyer, the book also provides clients with a good description of the role lawyers play in the contracting process. Highly recommended and for \$35, a pretty good bargain. From the Practising Law Institute. ([http://www.pli.edu/product/upprog\\_prod\\_detail/product\\_overview.asp?wtype=4&ptid=6&stid=43&pid=EN00000000009379](http://www.pli.edu/product/upprog_prod_detail/product_overview.asp?wtype=4&ptid=6&stid=43&pid=EN00000000009379)).

## **A Collection of Good Articles**

*Preparing For The Worst*  
(<http://www.computerworld.com/newsletter/0,4902,92265,00.html>)

*Classic Mistakes* (<http://www.computerworld.com/newsletter/0,4902,92268,00.html>)

*A Business Continuity Checklist*  
(<http://www.computerworld.com/newsletter/0,4902,91587,00.html>)

*Data Recovery Planning: The First Step*  
(<http://www.computerworld.com/newsletter/0,4902,91614,00.html>)

*Disaster Homework* (<http://www.computerworld.com/newsletter/0,4902,92289,00.html>)

*Disaster recovery tips from users*

(<http://www.computerworld.com/newsletter/0,4902,92259,00.html>)

*Protect Your Business Against Disasters* (<http://www.smallbizpipeline.com/57300225>)

## Biography

Dennis Kennedy (dmk@denniskennedy.com) is a well-known legal technology expert, technology lawyer and blogger. After spending many years in large law firms, he is a now solo practitioner in St. Louis, Missouri who concentrates his practice in computer law and also provides legal technology consulting services and seminars. He is member of the ABA Law Practice Management Section's Council, Webzine Board and the ABA TECHSHOW 2005 Board. An award-winning author and speaker, he was named the 2001 TechnoLawyer of the Year by TechnoLawyer.com for his role in promoting the use of technology in the practice of law and also received a 2001 Burton Award for Legal Excellence for an article he co-wrote on computer law. His blog (<http://www.denniskennedy.com/blog/>) and his web page (<http://www.denniskennedy.com>) are highly-regarded resources on technology law and legal technology topics. He has also taught classes in Intellectual Property Licensing and Drafting as an adjunct professor at the Washington University School of Law. He graduated *magna cum laude* from Wabash College in 1980 and *cum laude* from the Georgetown University Law Center in 1983.

