Imagine the following happening to you:

8:34 p.m., Sunday February 12:

You are a principal at Sharppens Inc., a mid-sized accounting firm. You have your own office in the company's own building, and are doing great work. All things considered, it's a very satisfying job — you thrive on the challenge of financial analysis, keeping up to date on the ever-changing world of tax regulations and deploying your considerable chops for your clients. But, at the moment, you are *definitely* making the most of your last few hours of weekend, kicking back with a good movie and a cup of tea. Suddenly, the phone rings.

It's the alarm company. The authoritative voice on the other end of the line informs you that there's been a break-in at Sharppens. You rush out to meet the police at your firm.

9:03 p.m., Sunday February 12:

You arrive at work and witness the devastation. Besides the physical damage to the forced doors, every last one of the computers is gone.

OMG the computers are gone! OMG the stuff on the computers is gone!

Including, you swiftly and sickeningly realize, *all your client files. And* your book-marked reference websites on taxation regulations, *and* all your contact information for clients and suppliers, *and…* The list goes on, but you don't even want to contemplate it.

You go back home; not to finish your tea, but to pour yourself a nice tall Alka-Seltzer, then toss and turn for a couple hours until you fall into a troubled sleep. One thought keeps resurfacing: The company depends on these missing files — ***What on earth are we going to do?***

9:05 a.m., Monday February 13:

You are sitting at your desk with a cup of coffee, stress-ball in hand, trying to figure out where to start. There are appointments both existing and to-be-booked, jobs to delegate, tax files to talk to the government about, audits pending, etc. More questions now spill out of the Big One that kept you up half the night:

- Where are the installation disks?
- How many bookmarks did I have?
- How many billable hours will I miss?
- Client files – can someone get them back for me?
- If so, how much is that going to cost?
- Who's going to key in the stuff from paper copies— and what will *that* cost?
- Do I even *have* paper copies to manually key in from?
- Where is it all stored?

- What will my clients think?
- Will I be able to do payroll this week?
- How long am I going to be out of business until I get this stuff all together?
- How secure was the sensitive data on those missing machines?
- Has that data been cracked, and is it being used for nefarious purposes RIGHT NOW?

The immediate aggravation is dealing with the insurance adjusters; with whom, despite the pressure, you naturally interface with your usual professional aplomb and finesse.

Then the big job starts: installing the programs on the computers, and then trying to get the systems back to what they were before the theft — the browser bookmarks, the local address books, the documents that were not backed up, the tax prep programs. Not to mention the initial near-impossibility of trying to remember what was on each unique system, beyond the standard Office install.

All this costs Sharppens Inc., and you, time and money — not just in the replacement of hardware, and the technical service to restore the systems and data, but in lost opportunities from missing files and the paralysis of the office while the restoration occurs.

What did the thieves do with the systems computers? To put it bluntly, they probably fenced the machines for a few bucks. But that still leaves you asking some disturbing questions: "What happened to the data that was on the hard drives of the computers?" "How many people did their banking from the office?" "*What can we do to stop this from ever happening again?*"

Challenge: As an accounting professional you are responsible for others' business

Good accountants have many systems: larger client or company systems that you join seamlessly and become an integral part of; as well as your own personal business systems that ensure everything you're responsible for keeps ticking along without interruption.

It's both a benefit and a hazard of today's business environments that much of the sensitive data required for you to do your job is stored and managed on computers. As an accounting professional, this can include SIN numbers, birthdates, passwords, personal and corporate financial records, tax returns — even whole audits.

You not only are responsible for your work and your advice to your clients, but also for the security of the private information they share with you. Of course, you do your best to protect your office by locking your doors and ensuring that you have appropriate fire protection for your paper files.

But what about the digital files that you are responsible for? What about the applications that you use each day to manage client information? What are the security risks associated with managing those files?

When the unthinkable occurs

The event can be physical and localized — flood, fire, cyber attack, power surge, or outright theft of a computer. Or, it can damage your data virtually, causing it to become corrupt or unstable, opening it up to access by unsavoury parties, turning it into a trojan horse to wreak havoc on your other files, or making it disappear without a trace.

The impact is not just limited to your own business: your documents, calendar, address book, bookmarks and cookies, programs and databases. Your *clients*' information is also at stake. As an accountant, you are obligated to do more to protect yourself if the worst-case scenario happens. Taking preventative and post-disaster measures will allow you to come out of the experience with your professional relationships, reputation — and data — intact.

According to Gartner Group and the IDC:

- up to 80% of corporate data resides on end-point desktops and laptops
- 15% of laptops suffer hardware failure annually
- 10% of laptops are stolen annually
- Lost Productivity is $177/hour

The financial repercussions of a catastrophic event are significant. Restoring a client's files is much like setting up a new account for them — by conservative estimates, it can take at least two hours. Simply multiplying any of the above stats by the number of computers in your firm will indicate how prohibitively expensive — finance- and productivity-wise — emergency data recovery programs can be.

Do the math:

Number of clients (X) average number of hours to rebuild files (X) the hourly rate for someone to rebuild the client file. The following calculation is based on 1000 clients with the assumption that it takes four hours to key in the information necessary to rebuild the client file and that you pay someone $25/hour to do this. (*This of course assumes that you have the information stored somewhere else that you can access to rebuild the files with!*)

1000 x 4 x $25= $100,000

Try this yourself with your own figures.
What's the risk in *your* office?

Number of clients	Number of hours to recreate client file	Hourly rate to key in files	Total cost of re-creation of client files

What are the options?

The concept of data security is complex; there is no one size fits all solution. It's up to you to choose the right system for your requirements, and after a needs assessment a variety of solutions can be deployed, including those below:

Server Backup Solutions: (from Wikipedia)

- **Tape** - a data storage device that reads and writes data on a magnetic tape. Typically used for offline, archival data storage. Provides sequential access storage, unlike a disk drive, which provides random access storage.

- **Network-attached storage** (**NAS**) **-** file-level computer data storage connected to a computer network. Potential include faster data access, easier administration, and simple configuration. Remones the responsibility of file serving from other servers on the network

- **Storage area network** (**SAN**) - a storage device (ex.: disk arrays, tape libraries, optical jukeboxes) appended to servers, that appear locally attached to the operating system. Typically has its own network of storage devices that are not accessible through the regular network by regular devices.

- **Cloud (or remote backup services)** – Backs up your files via the internet to a remote location, safe from threats your physical office may experience. Can protect against some worst-case scenarios such as fires, floods, or earthquakes, that would destroy any backups in the immediate vicinity along with everything else.

Other aspects of security to consider

- **Virus protection:** Like a flu shot for your servers and workstations, it has to be updated so that it retains its protective abilities. Don’t make the mistake of thinking that the free anti-virus program that came with your computer is going to do the trick, though — usually you have use of it for a 90-day trial, at the longest. If you feel that going the whole nine yards is too expensive, or that you’re safe because you don’t go to “bad” websites, it really is only a matter of time! A flu shot hurts too — but not as badly as getting a full-blown case of the flu

- **Malware protection**: Malware are malicious programs (hence the name) intended to disable your computer or network. They often enter your computer through a virus. Malware programs are sneaky — you think you’ve gotten rid of them, but they can morph and lie in wait. The only sure way to get rid of them is to format your hard drive. It’s better to prevent them in the first place by subscribing to a legitimate protection program — of which DFC has several options.

- **Firewalls:** Firewalls can be software on a server, or an appliance. A good firewall will turn your network into the equivalent of a heavily armed fortress. However, they are complex to configure and only true professionals should handle this. Often firewalls come with subscription services for malware, anti-virus, anti-spam, etc.

- **Outsourced support**: Every firm has someone who is “good with computers”. With the threats to your data becoming more sophisticated by the day, it’s time to enlist professionals. Nowadays, you don’t have to hire an expensive, and no doubt heavily-booked, tech guru. Managed Service Providers (MSPs) are a solution. MSPs usually set up their systems to monitor and predict your IT infrastructure. They work on a subscription basis and the choices run the gamut from the very basic to the most comprehensive possible. A potential bonus is that you never have to deal with IT again, as it is all done remotely. (Except for physical issues, like replacing hard drives — but that can always be done on a planned basis, after hours).

- **Physical:** This means securing IT assets so that it makes it difficult for unauthorized personnel to access them — for example, caging your server and leaving the key with a trusted team member.

- **Data encryption services:** For laptops and desktops, organizations have two choices: to encrypt files and folders on the **hard drive** only, or to use “**full disk encryption.**” Full disk encryption eliminates the need for an employee to decide which files are sensitive enough to encrypt — it simply scrambles all of them. Frequently, users underestimate the confidential nature of their files — only encrypting their files on their home and C: drives, for example, being unaware that temporary and swap files are equally sensitive and must be encrypted as well. Full disk puts and end to the guesswork, and returns the control and safeguarding of data to a centralized source — you.

DFC: the compatible choice

DFC offers many competitively priced choices under the umbrella of our **DFCRestore** service, which will allow you and your company to focus on your business with the maximum possible peace of mind. We support all the current business platforms and will recommend the best possible solution for your practice after a needs assessment.

Consider too, DFC’s turn key, DFCRestore, Desktop as a Service, (DAAS) includes virtual workspace, on-site storage, remote back up and technology services to manage desktops & laptops in an all-inclusive monthly service. Practically, this means that if you experience an unforeseen event, in which your computer or data (or both) are compromised, we can get them safely back to you in *under an hour* — with savings of up to 80% compared to typical desktop management costs!

If you ever experience a hardware failure…
If you ever have corporate data lost or stolen…
If you are in need of disaster recovery capabilities on your PC’s…
If you require security and protection for your corporate data and applications…
If your users need a secure way to transfer their applications, data, and settings to any workstation…

… We can help you! Go to www.dfc.com/restore.php to download a chart of the services we offer.

2:36 p.m. Thursday August 6:

Having recovered and used the February robbery as a learning experience, Sharppens Inc., has invested in and implemented a DFCRestore subscription. And it pays off today, as a faulty skylight gives way during a freak summer storm that strikes during your annual off-site company picnic. You hop on your motorcycle when the janitorial staff alerts you to the problem, and arrives to find your office and two others thoroughly soaked, and the computers ruined. So what happens *this* time?

One simple call to DFC, and your rescuers swing into action. You order new workstations, and within a day of their delivery, all programs, personal data, secure files, bookmarks, databases, address books — every last snapshot of kittens wearing silly hats used as desktop wallpaper — are restored to their grateful users.