

CHAPTER 1: WHEN BAD THINGS HAPPEN TO GOOD COMPUTERS

What, me worry? That's the mantra of Alfred E. Neuman, poster child of *Mad* magazine¹. Alfred never seems to worry about anything. That's probably because he's a comic book character—only fictional folks can manage to pull off that level of detachment. But, come to think of it, I know some comic book characters in business who don't worry about anything, either. I don't know if I should emulate or pity them—because in business, worrisome things *do* happen. They happen all the time. I wouldn't have had an audience for the first *or* second version of *The Backup Book* if bad things didn't happen to good computers.



And bad things come in three flavors: freezes that lock up the computer, forcing you to restart; corruption of your files, applications, and hard drive; and loss due to theft, fire, outages, etc. What these three flavors *affect* ranges from individual documents all the way to the loss of your building(s).

I'm including this chapter to give you an idea of what *can* go wrong, as well as the chance that it can happen to you and to the assets of your organization. I'll walk you through what can go wrong by pairing each of the three flavors of what can

¹. <http://www.madmagazine.com>. I love *Mad* magazine, absolutely love it. Best rag on the racks.

happen with each of the organization's key assets. And to bring it home, I've added a survey we took that asked folks how often each of these things have happened to them over a three-year period.



	 Documents	 Applications	 OS	 Storage	 CPUs	 Network	 Power	 Building
Freeze		✓	✓					
Corruption	✓	✓	✓	✓		✓		
Loss	✓	✓	✓	✓	✓	✓	✓	✓

Table 1-1. What can go wrong

If you think none of this will happen to you, think again. You have a 2 percent chance of being in that miraculous minority—the fortunate few who've never had a bad thing happen.

I've never been so lucky.

THE MAIN THING

The Main Thing in this section is to familiarize yourself with the key assets your company has—and what can happen to them.

This should give you a starting point for the areas in which your organization should focus its efforts in creating a backup and disaster plan.

*The nitty-gritty you need to understand is the cold, hard fact that you **are** at risk—and to protect yourself against that risk, you must take preventative measures within certain cost boundaries to limit the impact of downtime.*

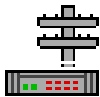
FROM MACRO TO MICRO—A QUICK LOOK AT THE STABILITY OF ASSETS



Okay, let's start with your building. Every company exists in one—except, of course, those that are in boats, tents, yak caravans, or the last few extant VW microbuses. Buildings are very robust, for the most part.



Every building is powered by electricity. This is necessary for seeing what in the world you're doing and for powering your computer system. Some buildings (very few) are powered by solar energy (like in Berkeley, California). Electricity is, for the most part, pretty dependable. Since electrical failure (too little or too much) is a cause of hard drive crashes, etc., we figured we'd leave it out of the survey.



Most companies inside buildings have their computer systems tied together with Local Area Networks (LANs). The computers use these networks to yak to each other and then talk to the rest of the world through The Network: the Internet. Networks are, for the most part, pretty secure and reliable. Because a downed network doesn't affect the data on your hard drive much (if at all), we chose to leave it out of the survey.



Sitting on the networks are lots and lots (okay, not so many lots, if you're a small company) of computers. Big ones, small ones, fast ones, slow ones. Now we're starting to get to the real meat of the digital asset world. Normally computers either break immediately upon arrival, one day after their initial warranty is up, or not until they're well beyond their usefulness.



Each computer has one or more storage devices, such as hard drives, Zip drives, CD drives, flash drives, etc. This storage space is where the information lives. Okay, some of it lives in the heads of the people who go home at night, but this isn't a book about employee retention, so we'll let that part slide. Storage devices are rated in "mean time between failure rates"—which means that they're destined for failure in your lifetime. So count on it.



Operating systems hold the software that is the engine of your computer. The main flavors are Windows (pick a variety from 95, 98, NT, 2000, XP, blah blah blah), Macintosh (OS 8 through X), and a gazillion flavors of Unix (Unix, Sun Solaris, the Linuxes, etc.). Operating systems—as they're shipped by the manufacturer—are pretty robust and very reliable. However, once installed, users generally gunk them up with their own extensions,² quickly making them less reliable. Operating systems are also a favorite target for the cretins who write viruses. The

good news is that most users have only a single operating system on their computer that they can screw up.



Applications (such as Microsoft Word) are the individual productivity tools that each user spends most of their time working on within their computer. My own computer has 92 different applications on it, and normally I use about eight of them at a time³. Most applications are installed and used as suggested by the publisher. However, others can be quite extensible. (On my computer, Dreamweaver has an additional 29 extensions.) Because applications are what users operate day in and day out, they're the whipping boys that bear the brunt of a computer's corruption and loss problems. When users freeze the computer, they're usually freezing an individual application. When viruses attack a computer, they attack the open (in-use) applications. Therefore, because of outside influences, applications are prone to problems.



Aside from sports-betting pools, documents are a company's most-frequently produced asset⁴. Documents are also *the* usual suspects when it comes to getting into trouble—like the time my dog ate my research report in college. How it got into my hard drive, I'll never know—the dog, that is. Documents get corrupted. Get erased. Get all sorts of havoc wreaked upon them. Documents are about as unstable as me taking a bottle of red wine on a visit to my mother-in-law.

-
2. Hey, I know what I'm talking about here. My own computer takes about five minutes to boot while loading the 23 additional system extensions I stuck on it.
 3. As I'm writing this, I have MS Word, Internet Explorer, Canvas, Fetch, Dreamweaver, and two databases open at once.
 4. A friend once told me that Hughes Aircraft really makes documents. Every so often, they manage to miraculously create an airplane, but that isn't their real focus.

FREEZES, CORRUPTION, AND LOSS—THAT WHICH CAN GO WRONG

Now let's put what can happen into perspective. Based on our international backup survey taken over a one-month period with more than 300 respondents in seven countries, here's how often things can go wrong over a three-year period.



Luck of the Irish: Some people have it; most of us non-Celtic types don't. Of those surveyed, 2 percent stated that over a three-year period, nothing had ever happened to their computer systems or the data on it. Wow, some people have all the luck in the world. That means that the *other* 98 percent of us are prey to evil leprechauns. Back to reality.

First stop, the frozen section.

Freezes

When freezing occurs, the computer simply “locks up” or stops working. The lights are on, but nobody's home. You type on the keyboard; nothing happens. You move the mouse on the desk; it doesn't move on the screen. When a personal computer hangs, it often offers no indication of what caused the problem; it's just sort of stuck in freeze-frame mode, affecting both the application and OS.



Table 1-2. Freezes

Frozen applications

Normally, frozen applications such as Microsoft Word affect only the document you're working on. When the application freezes, it can no longer access the document, and therefore whatever was added to the document since the last time it was saved will be lost. Sometimes application freezes can corrupt the application itself and you'll have to either restore or reload it. No big whoop. However, when

the chilled-out application is your web server, your database server, or your e-mail server (you get the point), it affects communications and productivity. Then it becomes a much bigger deal to bring the computer back to normal.

Frozen operating systems

A frozen application isn't the same problem as a frozen operating system. With a frozen application, the user can normally “force quit” the affected application and continue working because the operating system is unaffected.

When the operating system freezes, *everything* on the computer is locked down tighter than the cockpit of an Al Qaeda–chartered airplane. Whatever you were working on in your document—*from the last time you saved until the computer froze*—is forever lost. There's nothing there to restore—empiricist philosopher John Locke's *tabula rasa*. It's like having your short-term memory zapped.

When the operating system freezes, the only choice for the user is to restart the computer and hope for the best. Optimism is sometimes the only way to deal with cold, cruel reality.

How do freezes happen?

When a personal computer freezes, it often gives you no indication of what caused the problem. The computer could have crashed, or it could be something simple, such as the printer running out of paper. Usually a freeze is caused by input or data presented to a computer that is beyond its ability to cope (like asking it to do too many things at once, or aborting an operation at a critical stage). If a freeze happens in a single-task program (like MS-DOS, Windows, or Mac OS 9), the machine will cease to take input (“lock up”) and must be restarted (“rebooted”). If a freeze happens in a multitasking operating system like Unix, Linux, or Mac OS X, the user can force-quit the offending application and continue working. Sometimes.

Corruption

We're not talking the House or the Senate here—we're discussing what happens during excessive freezes or when viruses attack good computer systems. They become corrupted. The other day, I was working on a different (more boring) version of this chapter. I bombed the computer twice. When I reopened the chapter,

it was completely rearranged for me. Too bad the arrangement was worse than the one I created myself. But that's what corruption does: It moves things around in an order you (or your spouse) didn't create.

Corruption affects not only software, but can affect your storage devices and your network, as well.



Table 1-3. Corruption

Document corruption

Document corruption usually happens after a couple of computer or application freezes in a row. When your document becomes corrupted, the only thing you can do about it is either restore the document (if you backed it up) or re-create the document. Survey Sez:

Files that were corrupted	
85%	chance it could happen to you over a 3-year period
30%	chance it could happen to you once in a year
15%	chance it could happen to you 3 times in a year
12%	chance it could happen to you 5 times in a year
8%	chance it could happen to you 10 times in a year
6%	chance it could happened to you more than 10 times in a year

Table 1-4. Corruption probabilities

Application corruption

Every so often, after I've bombed an application repeatedly, it becomes corrupt. The only other way applications become corrupt is if they get hit by a virus. Either way, you get to restore the document from your backup system, or you get to re-create it from original disks and downloads of new "updates," not to mention replacing all those additional extensions the user tacked on along the way⁵.

Now, when an application such as a database server becomes corrupt, it could corrupt or even overwrite the data it's working with. This is because data is updated in a database server's cache first. It's transferred to its target memory or disk only at certain times. Therefore, when the database application becomes corrupt, the chance of data corruption in its files is pretty good, too. Survey Sez:

Corrupted Applications	
55%	chance it could happen to you over a 3-year period
26%	chance it could happen to you once in a year
7%	chance it could happen to you 3 times in a year
6%	chance it could happen to you 5 times in a year
4%	chance it could happen to you 10 times in a year
3%	chance it could happen to you more than 10 times in a year

Table 1-5. Corrupted application probabilities

Operating system corruption

In its quick-fix amenability, operating system corruption is worse than either document or application corruption. If the operating system becomes corrupt, you can't even access the computer. When this happens, you're facing a bit of time before the system is back in operation, unless you wipe the drive and start again.

Operating systems can become corrupt due to virus attacks, freezes, or upgrades performed either by an individual who is "adding some special extension or control panel" or through an actual patch from the manufacturer. When Apple shipped an upgrade to its System 9.2 software, one of the upgrades was *much* worse than the preceding version. The patch wouldn't allow the end user to return to the previous state (without restoring the computer from backup or completely re-creating the system from scratch).

The problem isn't limited to just Apple, either. Some software manufacturers ship their software buggy as all get out, and it takes a while to figure out that it really

-
5. Okay, there's another type of application corruption that usually happens after you talk to an imbecile in Technical Support, like the guy my dad talked to at Kodak, who told him to remove part of his software package. However, we can't cover *all* of the bases, or idiots, here, so we'll leave the human-I-know-more-than-you-even-though-I-can't-spell-tech-support type of corruption out of it.

isn't your fault that nothing works. Karsten's experience with Windows NT 4 was a very interesting one...

I was assigned a project in Hong Kong installing the Quark Publishing System (QPS) at a business magazine. Everything went smoothly until we started working with QPS. The editors were happily typing their stories into the Windows text editor; graphics artists grabbed the finished stories and placed them into the layout. Suddenly everything froze, and all the applications connected to QPS stopped. In a frenzy, I asked everybody to stop working. I began rebooting every single machine, rebooted the QPS server, and checked all network connections, but found nothing. I exchanged the QPS server for a new machine, but no success.

Finally I turned on the monitor of the file server that holds all layout data—and found that the server had died, simply showing the Blue Screen of Death (BSOD). I restarted the file server, and everybody started working—until the file server died again. Suspicious now that this phenomenon somehow had to be connected to the graphics people, I asked one of the guys to drag a file from his desktop to the file server. Bang!—it died again. So I started downloading and applying bug fixes (yeah, MS calls them “Service Packs”) from the MS website. What can I say—after installing the fourth Service Pack, it all worked just fine.

Survey Sez:

Corrupted Operating Systems	
65%	chance it could happen to you over a 3-year period
26%	chance it could happen to you once in a year
10%	chance it could happen to you 3 times in a year
5%	chance it could happen to you 5 times in a year
8%	chance it could happen to you 10 times in a year
4%	chance it could happen to you more than 10 times in a year

Table 1-6. Corrupted OS probabilities

Storage corruption

Storage corruption happens when the drive's logical system of arrangement or the physical drive gets messed up.

Each and every drive maintains a hierarchical system of organization. Sometimes those directories and pointer files become corrupted during a freeze, through a virus, or just plain old extended usage. If the drive's logical system is corrupted, the computer can't be accessed at all, very much like if the operating system goes down until the drive is completely reconstructed through restoration or simply wiping it and starting completely fresh.

Survey Sez:

Corrupted Hard Drives	
71%	chance it could happen to you over a 3-year period
32%	chance it could happen to you once in a year
10%	chance it could happen to you 3 times in a year
7%	chance it could happen to you 5 times in a year
5%	chance it could happen to you 10 times in a year
5%	chance it could happen to you more than 10 times in a year

Table 1-7. Corrupted hard drive probabilities

Network corruption

Many networks can become corrupt over time—especially large networks that become larger. We once had a client whose network was so vast and so corrupt that “storms” of bad information would fly through every so often—so often that the client called them “the pause that refreshes,” because the users would simply get a cup of coffee until it was over⁶. Network corruption causes “slowness” in computing, and can actually corrupt files as they're transferred across the network.

How do you corrupt your computer?

Teach it to smoke at an early age. Okay, I'm kidding. Sometimes, in the case of newly released software and hardware, it's shipped to you corrupted. In one case that we know of, a Sun UltraSparc III workstation was shipped to a university medical lab wherein the new 64-bit processor was causing data corruption in their medical experiment results. After losing about a week's worth of work—and *finally* being informed by Sun that a download was available, the Sun guys said, “We've identified a very rare occurrence in the SunBlade 1000 that occurs only

6. True story, that one. Absolutely true. Hard to believe—but true.

when running floating-point applications, like science and engineering applications. It is one of those far-corner occurrences where certain things have to occur in certain sequence for this [problem] to happen.” The guys at the university must have had that sequence down pat.

Viruses are a great system corrupter. Our website at Network Frontiers wasn't up one day when it started getting hit with the NIMDA virus. Thank the Lord we were running a Unix-based server instead of NT. And sometimes, even if the virus doesn't corrupt your system, applications, or documents, the virus cleaner may not be too particular with the files *it* attacks, and *it* can cause corruption, as well—talk about the cure being worse than the disease! Here are a couple of [download.com](#) comments about a particular anti-virus program:

After install I did not establish a Restore point, and I kept experiencing lockups after I downloaded. I ended up doing a complete F-disk and fresh install of XP. Second time, I established a Restore point, and again I experienced lockups.

This software detected the virus that had infected my computer, but in an attempt to cure it, sent my computer on a downward spiral that made it restart over 30 times. Now I have to open a program the minute Windows opens to trick my computer into not restarting. Even though I uninstalled the software, this bug persisted.

Software programs can corrupt your hard drive as well as themselves. There's a certain indexing application that offers to “find anything, anywhere within the files of your computer.” Supposedly it works by indexing each and every file on the computer as well as the contents within each and every file on your computer. However, in reality, after a couple of hours of grinding through your computer's files, the indexing engine goes crazy, getting stuck in a deranged loop, indexing and re-indexing everything on the computer over and over again. When I contacted the company, their official statement read in part, “You may experience a corrupt index file that will use up most of the available space on your local drive. This will cause your system to function below its capacity.” Actually, it uses up so much space that the hard drive seizes up and dies. “You will notice delays executing programs, and will not be able to copy large files to your computer.” In reality, if it doesn't kill the drive completely, it causes the system to go so slowly that it becomes unusable. The entire hard drive has to be reformatted, and the entire operating system has to be reloaded—without the software, of course.

Loss

In its simplest form, loss is not having access to something. “I lost the keys in my house” could mean anything from the dog ate them to my wife moved them (again) to they fell off my desk into the garbage and are now very, *very* gone. Loss in the computer world means various things, based upon what is lost. You don’t really *lose* electricity, but rather the use of it. You don’t really *lose* a building (unless you’re in California, where they’re known to slide a few blocks downhill every rainy season). Let’s look at loss as it applies to corporate assets.









								
	Documents	Applications	OS	Storage	CPUs	Network	Power	Building
Loss	✓	✓		✓	✓	✓	✓	✓

Table 1-8. Loss

Document loss

You could have accidentally erased it. Or purposefully erased it but wanted to “undo” the erasure, only to find out you can’t undo that kind of thing. Or you could have created a completely new document named exactly the same thing and stored it in exactly the same folder as the opus you just finished writing—thus erasing the opus and replacing it with pretty much nothing. Survey Sez:

Trashed or deleted files	
90%	chance it could happen to you over a 3-year period
21%	chance it could happen to you once in a year
18%	chance it could happen to you 3 times in a year
12%	chance it could happen to you 5 times in a year
10%	chance it could happen to you 10 times in a year
11%	chance it could happen to you more than 10 times in a year

Table 1-9. Trashed files probabilities

Those are pretty high numbers for trashed files, but that’s an accurate reading of the situation. Here are the numbers (which aren’t as high) for the probabilities of

what can happen to you when files are accidentally overwritten—as I’ve done to myself twice so far this book.

Files that were overwritten	
77%	chance it could happen to you over a 3-year period
24%	chance it could happen to you once in a year
12%	chance it could happen to you 3 times in a year
9%	chance it could happen to you 5 times in a year
5%	chance it could happen to you 10 times in a year
9%	chance it could happen to you more than 10 times in a year

Table 1-10. File overwrite probabilities

Application loss

It’s kind of hard to lose an entire application, but people have done it. As a matter of fact, I’ve been asked “What happens if I delete my hard drive?” It’s a truism that while computers have gotten bigger and faster, users remain a little “challenged” at times—right, Gerron?

Trashed applications can also arise from people playing games at the expense of someone else’s computers. At a New York university, joking crossed the line into hazing. A female computer science undergraduate who declined to be named found herself the object of a hacker’s hazing rituals. “They trashed my computer, uploading non-lethal programs that would flash dirty pictures every thousand keystrokes, reset my configurations, and rearrange and delete my files. I was in tears. The guys thought it was a riot,” she says. Yeah, very funny.

Again, if the applications are “lost,” you have to either restore them or reload them from the original CDs or downloads.

Storage loss

One day, your hard drive will fail and you won’t be able to do anything about it. Unless you’ve planned for this event, you will lose all your data. If you didn’t plan, there’s nothing you can do—the data is gone forever. The following illustrations depict a few of the problems your drives can encounter. Although some of these problems relate specifically to drives with “open” formats, such as Zip and Jaz cartridges, others are universal.

Hard drives are basically racks of spinning aluminum platters that are approximately .075 inches thick. These platters have a 50-micron-thick coating of oxide for the reading and writing of information. Information is written to these platters by small read/write heads that pass over the drive platters but don't touch them. Information is passed back and forth via electrical current and magnetism.

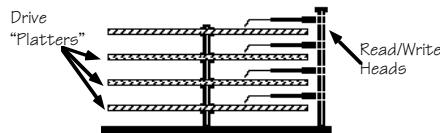


Figure 1-1. Hard drive platters and read/write heads

In the following picture, we show a drive platter and read/write head along with various particles that can cause problems.

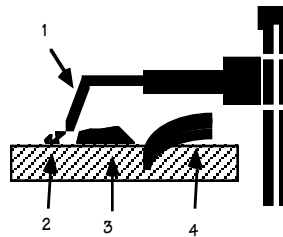


Figure 1-2. Particles and their relative sizes

This is the read/write head of the hard drive mechanism, and it isn't supposed to touch the disk. This allows very small dust particles to fit between the disk's surface and the read/write head without causing any problems. Sometimes, however, it just doesn't work that way.

1. This item shows the relative size of a smoke particle. These are usually 250 microns thick—large enough to cause interference between the read/write head and the disk's platter.
2. These items show the relative sizes of fingerprints and dust, which can cause even more interference problems.
3. A human hair is 3,000 microns thick (yes, even you folks with “thin” hair). A hair causes extreme problems immediately.

4. Even if your disks are kept free of these hazards (that is, they're hard drives and are therefore sealed), general usage over time causes the disk to fluctuate and begin to have problems.

Performance is at its best when the read/write head is hovering over the disk at 100 microinches. Over time, “stuff” builds up on the disk’s surface, and the read/write head begins to hover higher in the areas of more buildup and lower in the areas of less buildup.

Thus, the read/write head hovers in an erratic pattern. Sooner or later, the head comes in contact with the recording area of the disk and a head crash results. When a head crash results, it creates a dimple in the surface of the drive. And whatever info was there (where the dimple is now) is obliterated. If the crash is hard enough, it causes the oxide to flake off and you’ll begin to lose a *lot* of data.

Computers

Computers either work or they don’t. And it doesn’t matter if the memory is bad, the motherboard, daughterboard, or poor cousin-in-law-board is broken—the whole thing is out of commission until it’s fixed.

And that means that whatever was on the computer is now unavailable until either the computer is replaced or the information is restored to another working computer (or completely rebuilt from scratch). Survey Sez:

Broken Computer	
64%	chance it could happen to you over a 3-year period
35%	chance it could happen to you once in a year
5%	chance it could happen to you 3 times in a year
5%	chance it could happen to you 5 times in a year
5%	chance it could happen to you 10 times in a year
3%	chance it could happened to you more than 10 times in a year

Table 1-11. Broken computer probabilities

Baggage handlers I once watched a baggage handler (mauler is a better word) toss my computer onto a ramp when an air carrier forced me to check it because of limited storage space. It was gone forever. Even worse, I had to wait to put my drive in a new container.

Thieves Twice while I was CIO of a company, someone posed as a maintenance person—and stole two of our computers right off the desks of people in the office. How do we know? We caught the person on his third attempt.

Survey Sez:

Having to replace a lost or stolen computer	
28%	chance it could happen to you over a 3-year period
19%	chance it could happen to you once in a year
2%	chance it could happen to you 3 times in a year
2%	chance it could happen to you 5 times in a year
0%	chance it could happen to you 10 times in a year
0%	chance it could happen to you more than 10 times in a year

Table 1-12. Lost computer probabilities

Network

Yes, you *can* lose your network, or at least network connectivity within your organization or out to the “real world.” As we state elsewhere in this book, during our first online survey about backup, Excite@Home decided to go belly up. AT&T, who was licensing the service through them, assured us that we’d be operational within three days. Ha! The system came back up after four days, but the services we had contracted with them haven’t come back up yet. We had to move our equipment to another location in order to reestablish connectivity.

If you lose connectivity, you haven’t necessarily lost data—unless you have a split system in which part A is on one side of your lost connectivity system, and part B is on the other side, with no way to share data. We’ll talk more about that when we cover the loss of organizational functions and systems.

Power

Yep, it goes away sometimes—especially in San Francisco. Many years ago, while we were writing the second edition of this book, they were building a McDonald’s on the same location where Dirty Harry saved the coffee shop. And as chance had it, during the writing of the book, the electric company knocked out the power seven times. Ouch.

When the power goes out, it can cause document and computer corruption for any computer that isn’t on an alternate power source. If you’re wondering, that’s a bad thing.

Too much power creates electrical surges. Too little power creates brownouts. No power is a blackout. None of the three are welcome. Here’s what can cause them:

Transformer Failure Nobody in Chicago ever planned for emergencies caused by floods. What could flood in Chicago? The lake has never risen above normal levels, and the Chicago River is fully regulated by the locks and dams of the Chicago River Trade Authority. Nevertheless, in 1992, Chicago did flood. Somehow, the river leaked into the old coal tunnels that run beneath most of Chicago. These tunnels were used back in the early 1900s to deliver coal for furnaces in the larger buildings and had since been abandoned. When the river poured into these tunnels, it also poured into the basements of most of the downtown buildings, causing the electrical systems to send high-voltage energy throughout the buildings before being destroyed. Many companies had to temporarily relocate while the entire electrical system for these buildings was rewired. Some companies survived; others didn't.

Small brown-outs, sags, and surges Over 90 percent of all electrical problems are associated with power fluctuations that drop (brownouts and sags) or rise (surges) too much and too quickly for the computer system to accommodate. However, power outages in commercial buildings are usually both sporadic and short-lived, and can be worked around fairly easily.

Building

All references to September 11th aside, buildings fall down, burn, etc. This doesn't happen that often, but it does occur. When you lose the building, you lose access to all computer systems in it. And if this is where you were keeping your backup tapes, guess what? You lost access to them, too.

Cuban cigars Lighted tobacco products are on fire, even though the burning is usually contained to the end of the cigar or cigarette. The smoke can be a potential hazard, too, as was the case in this story I heard. A well-liked corporate MIS director's wife had just had a baby. The excited new father, who had just come back from overseas with a stash of smuggled Cuban cigars, passed them out to everyone in the office. A few of the "old boys" gathered at one of the desks, lighting up en masse. Now, I don't really know how this happened, but supposedly it was the combination of all eight men smoking in one small space that caused the sprinkler system to activate. Since it was an old building, water, instead of Halon, shot out of the sprinklers, drenching two computers on the desk and blowing out the monitors. Because the monitors' power cords were connected to the backs of the computers, one of those was lost, too.

Construction dust One day, a client called to ask me about a certain type of hard drive's reliability. Apparently, half a dozen of them at his site had broken recently. I told him that

the optical drives were normally very reliable, but that all things wear out over time. I asked how long the client had owned those hard drives, thinking that the mean-time-between-failure rate might have been reached, but two were new and the rest hadn't been around for long. After further questioning, I found out that a construction project was going on in their area. When the drive manufacturer's service representative opened the hard drives, he found the culprit: They were caked with construction dust.

Plumbing leaks

If you're in an old building, it might behoove you to check on your upstairs neighbor. In Chicago, there are a great many old buildings that have been rehabbed. I worked in one of these. In my office, there was a hole in the floor big enough for a ping-pong ball to drop through. Next door was a service bureau operating several film-processing devices. Often, as they were changing the highly acidic fluids in these devices, some of those fluids spilled onto the floor and consequently down to the office below. I'll leave the gory results up to your imagination.

Survey Sez:

Having to recover from a Disaster	
31%	chance it could happen to you over a 3-year period
17%	chance it could happen to you once in a year
5%	chance it could happen to you 3 times in a year
2%	chance it could happen to you 5 times in a year
0%	chance it could happen to you 10 times in a year
0%	chance it could happened to you more than 10 times in a year

Table 1-13. Building loss probabilities

PUTTING IT INTO PERSPECTIVE

In the second edition of our backup book, we used a pyramid we stole⁷ that I really like and that we've since modified. Based upon Maslow's hierarchy of human needs, this pyramid shows the hierarchy of loss—or, as seen differently—potential risks. At the nitty-gritty, risk analysis is really about continually asking the question “To what degree can the company tolerate the loss of information or networking systems ordinarily provided?” Here's what you *can* lose (the most important is on the top, but if you couldn't figure that out, you'd better head out of the computer aisle and limp over to the self-help section).

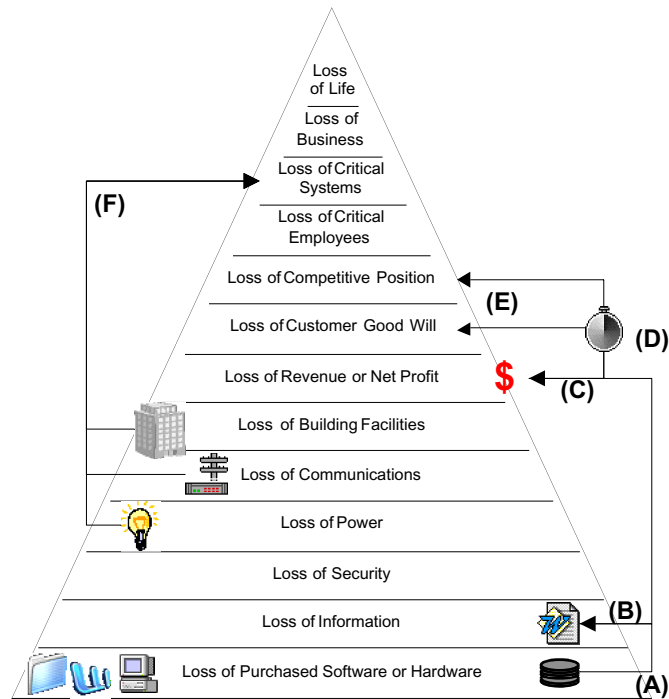


Figure 1-3. Hierarchy of loss

⁷. *Disaster Recovery Planning: Networks, Telecommunications, and Data Communications*, by Regis J. Bates (McGraw-Hill, 1992).

Different labels are associated with a few levels of loss on this diagram (A through E, and F). Before we cover A through E, I want to cover F, as F really isn't in the purview of this book.

- F. If you lose power or communications, or if you lose access to your building's facilities, there's a good chance that you'll lose access to your critical systems, as well. Losing all power or all communications access to your data (or the data center itself) will automatically cause you to lose the use of your company's critical systems. Since this is a book about backup and we have only limited information in our power outage section, we can't cover all of the things that are necessary for continued power use, communications use, or building use. Call us and we'll refer you to other writings or consulting services.

If, however, you're concerned with hardware loss that causes information loss, you're in the right place. You want to stop this chain of events from occurring:

- A. You lose your computer system or hard drive or operating system (to a virus or attack of some sort). Whatever happens, the net result is that you can't access whatever data you had on the system.
- B. If you can't access the data on the system, you've effectively lost that data, and it has to be re-created somehow. If you have a backup, re-creation of that data is done through restoration and making any changes necessary to bring the data back to the point it was at the latest backup.
- C. If you can't restore the data, you'll have to re-create it. Re-creating the data costs time—which, as we all know, is money. At best, the additional time it takes to re-create the data will affect the bottom line—and not in a nice way. At worst, you won't have time enough to re-create the data, and the client will leave a cooling breeze in his wake after he shuts the door behind him.
- D. If you can't re-create the data in the time frame necessary to meet your client's demands, you'll—at minimum—not only lose revenue (or net profit) on this project, you'll lose client goodwill. If your tardiness on projects continues, and you lose enough client goodwill, you'll lose the client.
- E. If you lose enough clients, you'll lose competitive position. If you're wondering, losing competitive position because the network administrator didn't create a good backup plan usually provides the network administrator the opportunity of seeking alternative employment—yep, you're history.

In this book, we offer a simple way for you to calculate the costs of downtime and create a backup plan budget based upon cold, hard bottom-line numbers. Using our forms (found on the website), you can easily identify costs associated with downtime and come up with some pretty straightforward budgets.

Throughout, remember to balance your budget with the value of that which you are protecting. While the topic is backup and disaster recovery, the theme is based upon solid business decisions and not the hottest, coolest technology available.