THE INDIANA LAWYER.com

Start Page: Disaster! It lurks around the corner – protect data now

Kim Brand September 12, 2012

START PAGE
Kim Brand

You are hanging by a thread and you don't even know it. Your Internet connection is delivered by two wires that connect to a box on the outside of your office – and all that separates you from disaster is a cable removed from a jack on the wall.

You store critical information important to the success of a case or the reputation of your firm on a server that is out of warranty. You 'think' you have a backup – but you can't remember the last time you made one or where you keep it. Everything is working now. What could possibly break?

Computers have become so reliable that we seldom consider the possibility that something can go very wrong very quickly; credit that to the increased quality control that manufacturers achieve to remain competitive. The cost of a single support call can exceed the profit on a new PC. Warranty service is expensive, too.The fact is that thousands of PCs and servers in Indianapolis fail every year. Google, which

operates millions of hard drives, expects 10 percent of them to fail every year. Translate that your office: If you operate a network of 20 PCs, two of them are likely to stop working this year. If one of them is used by an attorney on a deadline you call that a VBD: Very Bad Day.

Given the hyper-dependence we have on our PCs, servers, networks and Internet, one would assume that a reasonable person would array multiple defenses against the most common threats. In my experience, that assumption would be uncorroborated by the facts. Few firms are prepared.

Pair threats with defenses

Backup is boring – Restore is exciting!

Backups should be tested regularly. Don't be put off by the complexity! Here is a simple backup audit rubric:

1. Create a file
2. Wait a while
3. Delete it
4. Attempt to get it back
5. Note the results: Did you get it back? Was it hard to do?

Practice this little procedure a few times a year. If you are lucky, you'll never need to conduct the drill for real.

Technology has provided us with tools that allow unparalleled productivity. And it would seem that these new gadgets create new threats to the safety of important information. But that would be incorrect; you only need to worry about three: acts of God, acts of violence and acts of stupidity.

Each requires a different defense. Offsite backups, surge suppressors and redundant hard drives are the best defenses against acts of God. Anti-virus and anti-malware software, secure passwords, firewalls and encryption programs repel miscreants who want to steal your data or destroy it. Mistakes and mishaps

are the most common threats.

A series of backups, good policies and procedures, and frequent training can help defend against those.

Inventory services

Maintenance of critical services is often overlooked in backup plans. Imagine that your Internet goes down. How would your firm cope without email

for two or three days? What if your phone system goes down? With modern VOIP systems they are likely to fail at the same time. Even simple problems can take a day to repair. Forget to renew your domain name? Misplace the bill for your DSL service? Maintenance in your building disconnects cables without warning? Each can take from hours to days to diagnose and repair.

TIP: A mobile phone configured as a 'hot spot' can deliver Internet service to PCs and laptops in a pinch.

A simple disaster recovery plan starts with an inventory of every service you depend on, whom to call when it breaks and what to do to work around an outage. Law firms depend on PCs and phone companies, Internet service and email providers, network admins and software vendors. Assemble the contacts, account numbers, service agreements and work-arounds *before* you need them. The list should be updated frequently and audited.

Backup is not disaster recovery

Be aware that a good backup is far from a disaster recovery solution. I recommend protecting the entire 'Value Stack' on a server or a critical PC:

• **Hardware**: vendor, repair/replacement arrangements
• **Operating System**: licenses, activation codes, etc.•
Configuration: users, groups and permissions
• **Application Software**: licenses and updates

• **Data**

Google these terms to find out more:

- Survivor or statistic
- Shadow protect
- Full server failover
- Disaster recovery journal

Generally this means

keeping an 'image' of the server or PC on multiple/inexpensive USB drives. Backup software may be included with your system … or added on. It may cost $1,000 or more. But the cost is negligible compared to the potential loss.

Remember: An unmonitored backup system is like not having a backup at all. The most important part of a good backup plan? Making someone responsible to make sure it happens.•

Kim Brand *is president of Indianapolis-based Computer Experts. He is also the inventor of FileSafe – the only on-premises server priced like a cloud service. He was recently appointed Adjunct Professor of Legal Informatics at IU. The opinions expressed are those of the author.*