

*“In the wake of the terrorist attack on the World Trade Centre, many law firms have felt the need to come to grips with the grisly subject of disaster recovery. Disaster recovery plans fall into the same overall category as insurance – you have it because you can’t afford not to...”*

John Heckman, The Technolawyer Community

---

## **IV – SECURITY & DISASTER PREVENTION**

### **CONTENTS**

- A. Introduction – What can go wrong**
- B. What can we do? – Prevention & Cure**
- C. Best Practices Policies (I) – Backing Up**
- D. Best Practices Policies (II) – Protection against Hackers & Virus attacks**
- E. Best Practices Policies (III) – IT Use Policy for Lawyers and Staff**

### **ANNEXURES & HANDOUTS**

**Security & Prevention – Price Table**

### **RELATED BIZIBODY ARTICLES**

**The Importance of An Effective Internet Use Policy**

---

## **A. Introduction - What can go wrong?**

Tragedies can't be avoided, sometimes they just happen.

What can go wrong?

- Natural Disasters such as fire and flood;
- Theft (including sabotage by disgruntled employee);
- Terrorist action;
- Virus attacks

Also you can expect normal wear and tear from your computer systems; without routine systems administration housekeeping and vigilance, you can expect your server to overload or crash once after 4-5 years of continued operation.

---

## **B. What can we do?**

To what extent can you plan and prepare for disaster? With modern technology, quite a lot! Your aim is to reduce the impact. To do this, you should anticipate the worst scenario and put systems into place that will enable you to restore your data and systems so that you can take up exactly where you left off when the disaster struck with minimum downtime.

In terms of Prevention – this paper will show you how you can take steps to avoid the worst possible risks and implement the best practices policies for lawyers and staff including backing-up routines.

If despite your best prevention policies, disaster should strike, we show you how a well-executed Disaster Recovery Plan can help you to restore your data and operating systems with minimum loss of productivity and anxiety.

---

### C. Best Practices Policies I – Backing Up

1. **Network Solutions** – automatic back-up of data at the server level should be one of the primary incentives for installing a client-server network for your office. Routine backing-up of data can be timed to run automatically in the evening at the end of each working day. This is easily done and causes minimum disruption to office operations. The alternative is to rely on your staff to back up their work from their personal workstations onto removable storage media such as floppy disks or CD-Roms. This requires a sense of personal responsibility on the part of your staff; or else expend the resources of an office manager to monitor the actions of your staff.
2. **Use reliable Backing-up Software and Medium** – There are different types of backing up medium in the market today; comprising tape back-ups, backup drives (this is usually part of your server hardware and may comprise RAID or other fault tolerant drives in a mirror / duplex system); and removable media such as floppy diskettes, CD-Roms and Zip Drives.
3. **Test your Back-up Systems** – Tapes and other storage media will wear out if they are being used over again. Backing up media should be routinely tested for their accessibility and quality. You can do this by choosing a random selection of files and restoring the data from the backup media.
4. **Install a UPS (“Uninterrupted Power Supply”)** – This is an extra battery pack that automatically provides a power supply to your computer systems when it senses a loss in power from the electrical mains in your premises. The UPS should provide power long enough for you to back up all works in progress and shut down properly.
5. **Make Disk Images** – This is a complete snapshot of your hard disk drive (including programme files and configurations). The disk image serves to facilitate setting up of replacement workstations and enable continued operations in the quickest possible time. There are reasonable prices software on the market today (“Ghost” or “Drive Image”) that can help you create disk images within minutes.
6. **Off-Site Storage** – If your tape backups are kept in the office and the office burns down, it will hardly help you set up operations again in the quickest time. The cheapest way to set up an off-site storage facility for your data is to bring the backup tapes home with you in the evenings. Larger firms today regularly backup to a remote server through fast speed Internet connections. To avoid the cost of setting up and running a server in an off-site location, you may wish to consider ASPs that provide online storage facilities (eg, SafeTNet). Through the internet, you can have immediate remote access to your data. Most ASPs will also provide read & edit functions and search facilities. The downside of using an ASP for your data storage is – vendor stability and the related issues of data privacy and access to your data on termination of your contract with the ASP.
7. **Data Redundancy** – this can be easily achieved by saving data on the local as well as the shared drive. At the server level, the data should be automatically backed up into the storage facility; while at the workstation level, your staff will have all their work-in-progress on their own disk drives or on floppies. Document management systems can be programmed to save data on both the server and the workstations automatically.

[Click here to view Equipment & Software Price Table](#)

## **D. Best Practices Policies II – Protection against Virus Attacks & Hackers**

### **What is a virus?**

This is better explained by what it can do. A virus is a replicating code that attaches itself to a programme or data file. The virus may contain the “attack” programme also called the “payload” that can destroy data and programme files, propagate itself or send out data from your system to contacts in your address book. Viruses invade your system through several ways – the most common being attachments in an email, from an infected disk or CD-Rom or through files downloaded from the Internet.

### **How can you tell if you have a Virus in your system?**

- Inexplicable changes in the file sizes or available disk space;
- Messages flashing across your screen;
- Programme files not loading;
- Data loss or corruption

### **Protection against viruses**

The best safeguard against virus attacks is to use reliable anti-virus software. Put it on the server and have all the workstations on the network automatically updated. Anti-virus software will automatically scan all floppies and files before opening them and quarantines files containing identified viruses. It will also give you the option of “cleaning” the infected file or deleting it altogether. Your only responsibility is to ensure that you monitor and update the virus definitions on the software. A market leading anti-virus software like Norton Anti-Virus will send registered users regular notices and updates.

### **Protection against Unauthorised Access**

Your best safeguard against hackers and other unauthorized third party incursions into your computer systems is to install a firewall. A firewall is a series of filters that gives you control over who has the right to access your system via the Internet; simply put, it enforces an access/deny policy for your law office.

### **Features of a firewall**

Generally, firewalls use IP filtering language to filter a wide variety of attributes including source and destination IP address, protocol types, TCP/UDP ports etc.

Most have mechanisms for logging traffic and suspicious activity

Your proxy server can be configured to act as a firewall as it intercepts all messages entering and leaving the network; proxy servers can hide / mask your true address, implement protocol specific security and perform user authentication.

### **Types of firewalls**

Types of firewalls offer different levels of protection from simple screening routers working at IP levels to more complex application level restrictions via proxy gateways and servers. Hardware Firewalls (eg, Sonicwall, SOHO, WatchGuard) are often simpler and more efficient as they are optimized for one task; Software solutions (Zone Alarm, Norton Internet Security, McAfee Firewall) are cheaper but often not as reliable as hardware firewalls.

### **Implementing your firewall**

First – determine your access policy – what to allow in and what to block out

Second – Consider budget and level of professional IT resources (more complicated access policies can be notoriously difficult to implement)

Third – Draw up your network diagram, network protocols and IP addresses for mail, file server and web server

**E. Best Practices Policies III – IT Use Policies for Lawyers & Staff**

1. Training and Education – this is often the best way to foster a sense of personal responsibility in your staff. Often staff do not realise the potential liability when they misuse the office Internet; nor do they recognise the dangers of downloading virus-infected files from the Internet. Simple office regulations relating to workstation security, routine updating of virus definitions, saving all work on the Sdrive...etc can be easily implemented with minimal disruption to everyday operations
2. Set Appropriate Internet Use Parameters – Employees have a reasonable expectation of privacy. It is also impractical to enforce a total ban on the use of office Internet for personal matters. The key is to establish what they may or may not access on the Internet; including the use of office email for personal mail. A specific consistently applied policy grounded in legitimate business purpose will make it clear to employees that their personal email is neither private nor confidential and may be subject to monitoring by the firm at any time.
3. Be Prepared to Enforce these Policies

[Click here to read Bizibody article “The Importance of An Effective Internet User Policy”](#)