

Is my Business at Risk? Are my Computers Safe and Secure? How to find out!

If the computers in a business are not safe and secure - the business is at risk.

The 10 areas detailed in this document provide a basis for assessing your risk exposure.

1. Computers accessing the Internet

Spyware is surreptitiously deposited on a computer without the user's knowledge or consent and most of it originates from legitimate websites that have been compromised.

51% of spyware comes from accessing legitimate websites such as banks, financial institutions, and other businesses.

(Source: Websense, Jan'08)

If a cyber criminal can get his malicious software onto a major company's website for just an hour or two, they may be able to infect 100's or 1,000's of computers. For a hacker, who can earn money for every successful computer infection, this is a very lucrative result.

It only takes one computer in a connected network to be compromised, and then all other computers connected to that network are at risk.

Is **every** computer running the latest:

- antivirus, anti-worm, anti-Trojan software?
- anti-spyware software?
- spam filtering software?

Is this software up to date and regularly updated?

Are regular antivirus and anti-spyware scans run (daily, or at worst - weekly) on all computers in order to detect malicious software?

2. Email Management

Emails are now a legal document and, depending on what business you are in, emails to/from clients may need to be kept for up to 7 years or more.

Are emails being backed up daily?

Our experience tells us that most businesses don't actually know. And that most don't even know what to look for to ensure their emails are backed-up.

3. Backing-up documents

Are all relevant documents being backed-up regularly e.g. Word, Excel, PowerPoint, Access databases, financials (MYOB, QuickBooks), contacts, etc.?

A regular backup is daily or no less than weekly. A backup carried out on an ad-hoc or occasional basis is not an acceptable regime. In our experience, companies that say they do a backup every 'couple' of weeks, inevitably have intervals of months between backups.

Are checks carried out to try and restore from a backup? All too often we hear about attempted restorations from a backup that fail.

Tape backups have a 30%+ failure rate due to human, physical, logical, operational reasons.

Is the backup data stored offsite? A fire, theft or storm that results in loss of the computers and the backup, is going to make recovery extremely difficult.

Is the backup data encrypted to protect it from others gaining un-authorized access?

4. Disaster Recovery Plan

Having back-up in place is not a disaster recovery plan. e.g. being able to recover a client document from backup is of little use if you do not have a computer able to open the Word document and then print it or email it.

A disaster recovery plan should enable a business to quickly recover from a disaster in a way that allows the business to continue operating without major limitations. So, you need a separate disaster recovery plan to augment your back-up plan.

A key part of the disaster recovery plan is the ability to restore the key computer(s) in the event of a complete failure (hardware or software). The way to do this is by means of hard drive imaging.

Unlike tape backups, imaging captures a complete copy of the data on a computer - documents, programs, operating system etc. This allows for the complete restoration of a computer, either on the same hardware or on replacement hardware.

Disaster recovery imaging should be run daily - but not less than weekly.

If disaster recovery imaging is carried out, is a copy stored offsite?

5. Computer Clean-up

Over time, computers get clogged-up with unnecessary data - some which could put your business at risk. This can slow down a computer and may even be a security risk. This unwanted clutter should be cleaned up on a regular (weekly) basis. eg. cookies (which keep track of websites you have visited), temporary folders (holding information no longer required), registry settings (that are no longer relevant), history of websites visited, etc.

Are there arrangements in place to run a regular "clean-up" process on all computers to ensure they are kept running correctly?

6. Software Security Patches

Microsoft and other software vendors regularly release "patches" to fix security problems uncovered in their software. To avoid being at risk, these **must** be applied soon after their release.

Microsoft releases patches every 2nd Tuesday of every month (i.e. 2nd Wednesday here), which are graded critical, important and moderate.

Note: Having Windows Auto-Update set to ON may give a false feeling of security. It is possible for a patch installation to fail, or even for large numbers of patches to be completely missed (we are aware of a case where patches had not been installed for 6 months, but the user was totally unaware there was a problem). To be sure, it is necessary to visit the Microsoft Update website and run a check.

7. Remote access to your computers, network

Accessing an office network from a home computer is a common arrangement that many businesses have in place. If the home computer is used by children, this is a sure way of infecting your office computers. The way in which children use computers greatly increases the risk of a computer being infected with malicious software (children are fearless and will "click" on anything - not understanding the possible ramifications of that "click").

Home computers being used to remotely connect to an office network should not be used by children. Ideally, that home computer also needs to be protected with the same security regime as run on the office computers.

8. Wireless access

When using wireless access, special attention needs to be paid to making sure that the correct level of security/encryption is implemented. Deploying a wireless router according to the standard set-up instructions will result in a completely "open" network that will allow others to connect to your system wirelessly. It also means that your computer and the data it holds is at risk.

9. Technical advice

When there is a need for technical advice (should we implement document management? or VOIP phone services? Which computer or multi-function printer do we need? etc.), who do you go to? If the person providing the advice is getting a sales commission or other such payment, there is likely to be a conflict of interest. What is being recommended may well be the option that provides them with the most profit – and not the best solution for you.

Advice about computer hardware or software should be provided by an unbiased computer expert.

Note: The local computer shop or your children, spouse, friends, etc. are **not** good sources of such information.

10. Purchasing New Hardware and Software

When new computers are needed, what is best? a cheaper "no-brand" or a more expensive brand name?

A widely held belief is that you can save money by sourcing "no brand" computer equipment from your local computer shop. This is a myth, as the apparent savings quickly disappear when you take into account the need to purchase genuine software and add a proper 3 year warranty. Additionally, there is the question of quality.

All computers should be quality brand names not a "white" box or no-name computer. And always get a 3 year warranty. No ifs or buts!

By: Peter Philipp, Director of TechOnline Pty Ltd. (T: 03-9886-9630)

TechOnline is the first Managed Services Provider (MSP) in Australia to deliver a daily and cost-effective computer management service for small business. A recent Telstra Business Awards state finalist, listed in AFR's "25 Rising Stars" and winner of "Business Excellence" and "Innovation" awards, TechOnline focuses on proactively "managing" computers rather than reactively "fixing" them with a daily and fully automated service of:

- security and monitoring
- offsite backup
- disaster recovery, and
- 24 x 7 helpdesk to provide technical advice and resolve (fix) problems.

Don't wait for your next computer incident. Protect your business now.