




LESSONS from the FIELD



Observations of an IT expert

By Franco Di Dio



The advent of cheap computers and an abundance of software choices mean that almost every legal practice uses this technology every day. Most remain blissfully unaware of the potential risks of poor choices and how to avoid them, with consequences that unfortunately become clear only after disaster strikes.

Remember, the most important 'law' belongs to Murphy – whatever can go wrong, will go wrong, and will do so at the worst possible moment.

Applying some simple rules can reduce your law firm's exposure to risk. In this article, I endeavour to offer some advice on how to make cost-effective and common sense decisions about computer technology, including choosing the right hardware, the importance of backups, virus

protection, passwords and wifi security. It is very important to spend a little time going through how dependent you are on the technology used in your practice in order to make a good risk assessment.

First, look at the real value of the computer on your desk by asking yourself the question 'could my practice survive if for some reason I lost access to my computer for a week?'

What about for a month, or for a year?

Like an onion, technology has a number of layers, starting

with the 'outer' hardware of the computer itself. Most people can cope with the idea of being without a computer for a day or two, but for any longer the obvious answer would simply be to buy a new one.

A cheap computer from a discount store can cost as little as \$800; add some basic software for word processing and email for \$800, and perhaps another \$800 for a dictaphone, monitor and other software packages. This makes a rough total purchase price of \$2,400 for a reasonably capable computer.

LIFECYCLES AND SHELF-LIVES

The first recommendation is not to buy the latest or newly released technology unless you are willing to play the role of guinea pig for the computer manufacturers.

Software and hardware change so fast, it is now a common practice for manufacturers to treat customers as 'beta-testers' of their products. Avoid being on what is known as the 'bleeding edge' of technology, as it is known in the industry. The best time to buy is in the middle of model's lifecycle, before a new model supersedes it.

Determining this time for computers can get a little tricky as they are produced in different classes, each with a different lifecycle. Computers produced for home-users and computer gamers are usually manufactured to a price and have a lifecycle of about six months. During the production run, the outside case of a computer may not change, but the internals can be changed – and often are –without notice.

Machines for business-users have a lifecycle of about 18 months. In that time, the hardware components may have only minor changes. All of which is exactly what large companies who want to roll out batches of computers in a standard operating environment need. Most businesses keep their computers for between three to four years because of what is known as 'planned obsolescence', something which can already be seen in the mobile phone market.

Mobile phones are really designed to last for the length of the longest contract, which is about 24 months. I still have a Nokia 5500 which, despite being the size of a house brick and more than 20 years old, still powers up and all the buttons still work. Meanwhile, a mobile purchased three years ago turns off after five minutes and only half a dozen of its buttons still work.

The lesson to be learned from 'planned obsolescence' is that holding on to a computer for more than four years becomes an increasingly unreliable prospect, moving into the future.

It is very likely that a part of the computer system will fail just when you need it most. I would pass these machines on to the children or donate them to one of the charities that rebuild these machines and gives them to disadvantaged families. After three years, don't rely on a computer as your primary machine, unless you accept the risk of potential failure and the loss of information.

More than hardware and even software, the most important part of the story is the information stored on the computer. Consider the effort that goes into creating your documents. Assuming that you spend as little as a quarter

of a work day creating documents, the information stored on a computer can cost about 30 to 100 times that of a computer's hardware and software. That rough calculation doesn't even include the costs associated with recreating that information following a computer failure, or the less tangible – but possibly more serious – costs to reputation or potential liability concerns.

Protecting your data

It is easy to see that information stored in a computer is a very expensive and valuable commodity which needs to be preserved and protected. There are steps that can be taken to reduce systematically your risk if things go south on the morning of a big court appearance.

One of the most important steps is to do regular backups. For as little as \$100, an external USB hard drive can provide storage for 750 gigabytes of data, and copies of files can be transferred to this device at the end of each day.

For lucky Mac users, Apple has provided a wonderful program called 'Time-Machine', which can enable copies of changes made to any part of the computer to be recorded on an external hard drive. The program takes a snap shot of the data and stores it away. Then, at any time the program allows the restoration of a computer to the way it was on a certain day. This application has saved a number of clients, especially when recently installed programs have corrupted the computer.

>>

arw
australian
rehabworks

OCCUPATIONAL THERAPISTS
CATASTROPHIC INJURY SPECIALISTS

- ◆ ADULT AND PAEDIATRIC BRAIN INJURY
- ◆ SPINAL CORD INJURY
- ◆ COMPLEX ORTHOPAEDIC INJURIES
- ◆ MEDICAL NEGLIGENCE
- ◆ MULTI-DISCIPLINARY CAPABILITY

WE PROVIDE COST OF CARE REPORTS

Anna Castle-Burton
5/181 High Street, Willoughby NSW 2068

PHONE: 02 9958 6410

For Microsoft Windows users, software for backups is not as integrated as for the Mac product. However, there are applications that will do automated and scheduled backups that can be set and run in the background.

Whatever the case, all backups need to be checked and tested regularly, or at the very least log files need to be checked to ensure that backups have been completed without errors. Unfortunately, waiting until you need your backups to check that the information has been successfully preserved is just a recipe for a heart attack. One easy way to test if backups are working properly is to create a file in a special directory and then, once a month, delete it and try to restore it from a backup.

VIRUS PROTECTION

Another layer in the basic metaphorical 'technological onion' is virus protection. The most common way that viruses enter computer networks is by exploiting the social aspect of users' lives. When people open files from friends or someone they think they know, or visit websites that interest them, this provides the opportunity that most of those propagating viruses use to enter machines.

Never open an attachment unless you are certain you know who it came from and, like all scams, remember that if something seems too good to be true, it probably is. When it comes to websites, those with a good reputation will not ask you to provide bank details via email; nor will they ever ask you to email your user name or password to them. Any who do should have their security seriously questioned, as they are likely to be a fraud target either from within or externally.

When asked for personal information by any website, especially bank details, consider very carefully what information you are disclosing and to whom.

For computers running Microsoft Windows, virus protection is absolutely essential.

Unfortunately, Windows was never designed to be a fully secure computer environment and, from its roots in the computer operating system of DOS in the 1980s, it retains the legacy of an immature security model. Microsoft has spent a considerable amount of time, money and energy over the past few years trying to plug its security holes. However, the company remains trapped in a technology arms race where 'black hat' hackers try to exploit security issues and Microsoft tries to stop them.

I recommend that Windows users buy an anti-virus product from a respectable software maker or, at the very least, install Microsoft's free Windows Defender Anti-Virus package, which can be downloaded from the Microsoft website. Additionally, install software updates provided by Microsoft. These updates provide fixes for security holes that viruses use. Some clients like to install free anti-virus products, but these are intended only to entice you into buying the full version, and can be poorly written.

As a Unix-based operating system, the environment for Mac users is somewhat different, but there are still viruses out there trying to get a foothold, even for Apple products. Unix is an operating system that has its roots in the late 70s,

when computers were very expensive and needed to be shared with many people to utilise every hour of the day and night to recoup their huge costs. A byproduct was the extensive development of security as a fundamental part of the operating system. The achilles heel of Unix and the Apple operating system is what is called the 'root' user. This user has access to all parts of the system and can control the installation of programs. For an Apple system, this is what the virus-makers are trying to get hold of; once they have this, they can control your machine.

PASSWORDS

Another layer to the computer technology onion is passwords. They are also a major cause of teeth-gnashing among IT professionals. The number one rule here is that your name is NOT a password, nor is the name of a significant other, child or much-loved pet. The next most common password is the address of your business or home. Another common security problem is when users choose the same password for everything. The risk here is that a cyber criminal only has to break one password and suddenly everything is wide open. If you wouldn't use the same key for your house, car, gym locker, office and safely deposit box, why use the same password for every website or application? In the real world, different types of locks are used depending on the level of security we need, and that is a good analogy when considering passwords. Getting access to online banking should be long and complicated but accessing a newspaper website should be relatively easy.

For anyone saying 'but I can't remember passwords, so how do I make a complicated password I can remember', there are solutions. One easy way is to use a dictionary and grab words that are equal or longer than four letters and string them together, using a minimum of three unrelated words, for example MoonSnailSailing.

This sort of password offers reasonably good security. The words are not related to one other and its absurd nature can make it easy to remember.

Hackers trying to beat the password will take longer to crack this type of password and the more words you string together the longer it takes to break. Each additional word can double the time involved, although there is always the possibility of a secret government super computer or a fluke getting the right words in the right order in a shorter time.

If you do choose a shorter password, substitute upper and lower case letters and add numbers and symbols from the keyboard. While it might make it more difficult to remember your password, it also makes it harder to use a program to break the password. Choose the level of security of the password based on the value of the information to your business and your clients.

Once you have a password the question arises about where to store it.

Until mind-reading scanners are invented, the best place is still inside your head. One place not to store a password is attached to the computer on either a post-it note or on a neatly typed piece of laminated paper. This also applies to writing it on the bottom of a keyboard or mousepad.

A number of programs and applications are available to store passwords securely in encrypted form on either a computer or a smart phone. If you must write them down, it is a good idea not to store them with the item that uses them. For example, don't store your online banking password in your purse or wallet.

WIRELESS CONNECTIONS/INTERNET SECURITY

The final big security issue is wireless connections. Here, the basic rule is that if you are not using it, turn it off. Far too many computer users leave their wifi turned on all the time, meaning that the computer is open and ready to be exploited. When the wifi is on, hacking tools can exploit the computer's vulnerability. The nature of wifi is that you are like a TV station radiating into the environment. You have no control over who can intercept your signal. When you access devices or information through the wifi, you are transmitting the information into the environment, as well as to your devices. As a risk issue, it is one of the highest.

Some clients use either simple or even no passwords on their private wifi. A quick test is to take your laptop or phone, turn its wifi on and walk out of your office. See how far you can go before your device loses connection with your wifi access point. You will find that the wifi travels a fair distance outside. The distance is a radius of a sphere, which gives you an idea of how far the wifi signal is travelling into spaces that you may have no control over. At home, I was surprised to discover that my wifi is available for a radius of just under two blocks. At the office, I can connect to my company's wifi signal in another office building across the road. In both cases, these wifi access points are normal, off-the-shelf devices that are unmodified.

If a hacker accesses your wifi system, they may not simply steal your internet connection, but also mess with your network, crash your devices and access confidential and private information on your desktop computers. Again, it is very important to have a long and complicated password for wifi networks. It is also crucial to ensure that the wifi access point uses some sort of encryption method for transmission. 'WPA2' (Wifi Protection Access 2) is what I would recommend as the minimum secure encryption method that you should use in your wifi system.

CONCLUSION

In everything that we do, some element of risk is involved. In business, we seek to control our risk exposure to ensure that the decisions we make are fully informed. We owe this to ourselves and to our clients. In this article, I have tried to expose some risks that you need to assess in your practice. Don't be paralysed by fear or put off from using technology, however. Instead, be aware and inform yourself of the issues involved, the risks, and how best to minimise them.

Carry out the following, quick risk assessments:

1. Check the age of your hardware – is it more than three or four years old?
2. Is the operating system up to date, with all the service fixes available from the manufacturer?
3. Are you running a virus-checker on your systems?

4. What is the rough value of the information on your desktop computer?
5. Do you have a backup of the information on your desktop computer? Do you back it up regularly?
6. Are your passwords secure?
7. Do you have the same passwords for everything?
8. Is the wifi on permanently? Does it use WPA2 encryption and do you have a very secure password for accessing it?

Computer security is not rocket science, and it doesn't have to be difficult or expensive. As a vital office tool which is used every day, choosing the right computer and ensuring that the information stored on it is safe and secure is worth some time and consideration. For anyone who remains unconvinced, try turning off your computer and running your office for a day or more without it. ■

Franco Di Dio has worked as an IT professional for more than 24 years. In that time, he has worked in legal, commercial, educational and government environments. He has a degree in electronic engineering from Curtin University, and is currently working towards his MSc in astronomy from Swinburne University. He holds certification in Prince 2 project management, and Certificate IV in workplace training. EMAIL francodd@optusnet.com.au.

HELEN L. COLES

**MEDICO-LEGAL
OCCUPATIONAL THERAPIST**
(33 years medico-legal experience)

- Assessment of residual function, rehabilitation potential, employability
- Home visits/work site evaluations
- Recommendation of aids, equipment and services for home and work
- Assessment following work injury, motor vehicle accident, medical negligence, criminal assault, public access injury
- Assessment for family court related to special maintenance needs of former spouse or dependant
- Assessment for administrative appeals
- Availability - local, all states & overseas by negotiation

Watkins Medical Centre
225 Wickham Terrace, Brisbane
Tel: (07) 3832 2630 or (07) 3839 6117
Fax: (07) 3832 3150
Email: hcoles1@bigpond.com