



# Data Security

What's the worst that can happen?

Paul Godden

1<sup>st</sup> Year MEd

22<sup>nd</sup> Year IT Consultant

[www.paulgodden.com](http://www.paulgodden.com)



# What are the risks?

## Historically: Just the three F's...

Fire – Disasters in any shape or form

Fault – Failing equipment

Human Error – Always check the nut behind the keyboard

## But now...

Malware – viruses, trojans, worms and key-loggers: through pop-up windows, IM, e-mail and web page scripts, file attachments

Spyware – a class of malware that collects personal information and transmits it elsewhere (adware and system monitors)

Human Error – Always check the nut behind the keyboard



# What's the worst that can happen?

- Pass on the infection
- Slow system performance by using up capacity, possibly shutting down an entire network
- Capture and transmit confidential information, such as credit card numbers, user names and passwords, or sensitive information about research or business
- Change data
- Erase files
- Change software configurations
- Give the attacker a connection to your computer for further attacks
- Botnets “a collection of internet-connected computers whose security defenses have been breached and control ceded to a third party”



# Malware protection

- Internet security suites—Macs are NOT immune!

These don't have to be expensive, and some of the best are also the cheapest...

Windows/PC Protection	Mac Protection
<a href="#"><u>ESET CyberSecurity Pro</u></a>	<a href="#"><u>Sophos Anti-Virus for Mac Home Edition</u></a> – IT'S FREE!!!!!!!!!!
<a href="#"><u>Avast! Internet Security</u></a>	<a href="#"><u>Avast! Free anti-virus for Mac</u></a>
<a href="#"><u>F-Secure Internet Security</u></a>	<a href="#"><u>F-Secure Anti-Virus for Mac</u></a>
<a href="#"><u>Kaspersky Internet Security</u></a>	<a href="#"><u>ESET CyberSecurity Pro for Mac</u></a>
	<a href="#"><u>Kaspersky Security for Mac</u></a>
Other vendors such as Norton/Symantec and McAfee produce packages that will protect your system just as well—but I won't recommend them.	



# Patches and software updates

- Windows and Mac computers allow for automatic updating. This has problems on both platforms, but the pros outweigh the cons.
- Third party applications need updating too...
  - Adobe
  - Internet browsers
  - Java
  - Office suites
  - Hardware drivers
- Internet security software is only as good as it's last update



# What if you've lost your data?

- You have got backups haven't you?
- When was your last backup?
- Was it a complete backup or just incremental?
- Do you know it's going to restore OK? You do test your restores occasionally don't you?
- Have you got a backup backup?



# Your backup strategy?

- What can you afford to lose?
- How much data have you got? Do you know what a petabyte is?

Capacity	Description	Price
500 GB	WD Elements Portable WDBUZG5000ABK - hard drive - 500 GB - USB 3.0. CDW #: 3114328	\$79.99
500 GB	Seagate Slim for Mac STCF500102 - hard drive - 500 GB - USB 3.0. CDW #: 3080039	\$88.99
750 GB	WD Elements SE Portable WDBPCK7500ABK - hard drive - 750 GB - USB 3.0. CDW#: 2623195	\$89.99
1 TB	WD Elements Portable WDBUZG0010BBK - hard drive - 1 TB - USB 3.0. CDW #: 3199285	\$94.99
2 TB	Toshiba Canvio Connect - hard drive - 2 TB - USB 3.0. CDW Part: 3273132.	\$147.99
Supplier: CDW Canada (List Updated July 26, 2014) - <a href="http://www.cdw.ca/">http://www.cdw.ca/</a>		



# If you're running a Mac

- Use Time Machine, it works
- Apple have a Mac 101 tutorial to help - <http://support.apple.com/kb/ht1427>
- From OS X Mountain Lion (upgrade from previous OS X for <\$20.00), you can use more than one disk drive

Time Machine settings allow you to select a disk and configure two backup regimes.

Restoration is simple, but test it every now and then.





# If you're running a proper computer

- Windows backup is awful
- Windows 8.x has a Time Machine rip-off that's quite good
- Windows 7 is great, Windows 8 is awful... 8.1 is slightly better... Windows 9 looks fine
- SyncBack from 2BrightSparks  
<http://www.2brightsparks.com/syncback/syncback-hub.html>  
is pretty good. SyncBack Pro or SE are about \$60.00, and there is a freeware version.
  - Full Backup (or Reference Backup): all the selected files and folders on the drive are backed up
  - Incremental Backup: files that have changed or are new since the last incremental backup
  - Differential Backup: files that have changed since a full backup was performed



# The backup regime - generations

- Keep more than one backup
- Businesses use a generation scheme...
  - A backup of the days' work would be made at the end of each day for three weeks (requiring fifteen disks – one for each working day).
  - At the end of the third week, the 'grandfather' (1<sup>st</sup> generation) media are re-used, over-writing the three-week-old data and turning these backups into the latest generation.
  - For added security, media can be removed from each week at random, and replaced with new, blank media, whilst what was removed is sent off to be stored securely at another location.
- Nobody's suggesting you buy 15 disks, but just two will ensure you always have a backup of a backup... and the more, the merrier.



# Disk imaging (I)

Most backup software requires you to have a working computer from which to run your software and restore the system. What if your main system drive just dies, suddenly?

Macs – in most cases, TimeMachine can restore your computer to it's previous state, but sometimes you have to reinstall the Operating System (OS) and restore data from there. Do you know how to do that?

PC's – will need a full system restore, unless you've used “disk imaging” software. Do you know how to do that?

## **Disk Imaging Software**

Takes a “snapshot” of your PC, personalised settings, data, everything and stores it on another drive, allowing you to restore the entire system, just as it was, to a new disk in a couple of hours. And it's easy.



# Disk imaging (II)

## Where can you get this software miracle?

For the Mac – Carbon Copy Cloner (<http://www.bombich.com>) at about \$45.00 (or less with an [educational discount](#)).

Simple and easy to use, excellent value. No other real competitors.

For PC's...

O & O Disk Image – About \$30.00 from O & O Software (<http://www.oo-software.com/en/products/oodiskimage>)



# Disk Encryption

- You want to encrypt data when you don't want anybody but you to read it
- Passwords on operating systems for Macs or PC's discourage at best, and offer a false sense of security at worst
- I can get access to the files on any unencrypted Windows PC in the time it takes to start the PC up from a CD or USB stick
- I can get your e-mail passwords too
- Don't ask
- Encryption can make that *practically* impossible



# Jetico BestCrypt Volume Encryption

In previous versions of this presentation I have recommended a previously highly popular encryption product called TrueCrypt.

If you use it, lose it.

Or rather, migrate to something else (like BestCrypt, just click on the heading above). The old TrueCrypt web site provides some migration instructions (<http://truecrypt.sourceforge.net/>).

In a high profile IT security case, it's been detailed as to how TrueCrypt has a *backdoor* through which U.S. law enforcement has full access to any encrypted data.

Who knows, other products may have the same, despite what they say, but TrueCrypt definitely does.

Don't use it.



# Strong passwords

- Contain at least 8-12 characters
- Contain characters from at least 3 of the following 4 classes:
  - Upper case letters
  - Lower case letters
  - Numerals
  - Non-alphanumeric characters
- Do not contain words in a dictionary and are not name/s
- Do not contain any part of the account name
- Are not based on personal information
- Are known only to the user



## Strong password (cont'd)

- Do not use names, people, or places that are identifiable to you
- Never share your password with others
- Don't write it down, post it near your computer or include it in a data file.
- Don't store passwords in an unencrypted file or send in an unencrypted email
- Don't store passwords in web applications or software

Unique, strong passwords can be difficult to come up with and remember, but you don't need a strong password for *all* of your accounts.





# Strong password (cont'd even more)

The strength of your password should be based on the sensitivity of the data that you are trying to protect. Photo's of the cat don't need much of a password, *other* photo's might.

- Create strong passwords for your most sensitive accounts, such as your network account and personal financial accounts.
- For non-critical accounts you can use a password that is easier to remember.





# Thank you for your time!

If you'd like to contact me  
regarding anything in this  
presentation, please e-mail me at:

[paulg@pauldgodden.com](mailto:paulg@pauldgodden.com)

A copy of this material  
may be located... [\*\*HERE.\*\*](#)

