CYBER Security magazine

Optimized for tablets

CYBER SECURITY MAGAZINE

Pre Attack Stratigies

Software Assets
Hard Ware Assets
Backup & Storage
User Training

Anti Virus Software

Paid or free anti virus programs

Email Security

Web Site Security

Post Attack Strategies

Ransom Ware
Malware
Virus

DIY Cyber Security

A range of strategies & techniques for small businesses & sole traders

Cyber Security

Cyber Security can be expensive or simple depending on how you set up your digital assets like software, hardware and internet services.

We have provided Cyber Security for our clients for the past 10 years

In this digital magazine we will look at how you can protect yourself against Cyber Attacks and how you can recover if you do get attacked.

Obviously if you are a large company your Cyber Security requirements are a lot different to home based and small to medium business.

This magazine is mainly for this later group because there is little support or information for them. They also don't usually have enough resources to be able to implement a high level security plans so we look at what you can do.

The key suggestion is **always make sure your Operating Software has the latest updates.**

Cyber Security has been part of our products and training system for our business for quite a while now and hope that you can get some simple strategies you can implement now.

Quentin Brown

Digital Training Products

Step 1 - Software Assets

One of the most important parts of any Cyber Security project is to be able to get back up and running in the shortest time possible. Not everything can be cleaned.

These can be divided into two categories:

a) System software: These are things like Windows or Apple software that help your computer systems run. They are the core of your business and should be kept up to date. If you're going to spend money this is what you should spend it on first.

b) Application software: This is all the add on software like accounting software, word processors etc. Much of this is online today which makes it a lot easier to retain access in all situations. Things like 365 Office, Xero etc

So the first step is to make sure you have copies of all the software that is not online that you use. So for example Windows or Mac OS software. Unfortunately, most OS software these days does not come on a CD/DVD so you should save the product key usually or access key to be able to download

Your vendor like Dell, Acer etc. will send you a copy of your OS with all the various drivers so order yours today. Alternatively download one from Microsoft site. If you don't have a legal version buy one. If you have a legal copy then list the code in a safe space next to an id for each computer. For Apple you can use recover.

For Apple computers After starting up from macOS Recovery, decide whether to erase your startup disk or begin reinstalling macOS.

What ever method you decide on get it organized today as an insurance policy. Some companies are now using Linux with Ubuntu or similar as a lot easier to recover from and less likely to get hacked.

Software Assets (cont)

Now you have your operating system covered it is time to do the same with the general software.

Save all Product codes & versions

To open the **Add/Remove Programs** tool on a computer that is running Windows 7-10 click **Start**, click **Control Panel**, and then click **Programs**.

In Windows XP, click **Start**, click **Control Panel**, and then click **Programs and Features**.

If you have a Mac you can find this information under Finder and applications.

Report Templates
Several templates are available for your inventory reports:

Software Inventory Report Template – Use this report to document the programs you find on computers in your organization.

Software Inventory Summary Report Template – Use this report to consolidate individual software titles.

To gather this information, you can do it manually or use some simple software. We actually use a system called **Manage Engine**

Office Software

Again, make sure you have the dvd or installation software and product key however, if you don't now is the time to buy. We quite often come across companies that use illegal software and can be the access point for hackers.

There is so much great free software around in this area today. Try it out now before you have a problem.

There are both online solutions like Google apps and offline like Open office

Free Office
Libre Office
WPS Office Free
Open Office

Accounting Software

Many businesses have started to use online accounting software and most accounting software has an online version.

Programs like Xero, MYOB and Quickbooks can be great alternatives however if you have software on your commuters then again make sure you have the disks and latest copies.

Once you have all the physical products installed and updated the next thing is to make a copy on a new hard drive so if anything happens you simply change the hard drives and your up and running again in no time.

PC Mag has a great article on how to do it for windows and Mac. This is probably the best Cyber Security for any small business.

Step 2 - Hardware Assets

Hardware is any physical equipment your have in your business. Computers, copiers, scanners, telephones, tablets, phones etc.

Just like the software we want to register all this hardware with any serial numbers, makes and model numbers.

Computers

When checking out the computer(s) we are checking for a few things.

1. Is the operating system up to date, all new patches applied etc.
2. Does it have antivirus software?
3. Is there a backup system?
4. Unused software
5. Password to access.
6. Amount of Ram, access points, CD, usb.

This is not really a point but if possible I like to look at the back of the computer to see if the fans are clogged up with dust and if so recommend a local IT person to clean them.

Any means by which code can be introduced to a computer is inherently a hardware vulnerability.

That means that when a user installs software, moves files such as CD/DVD ROMs or plugs in flash drives those items can all be thought of as hardware vulnerabilities. A

Securing physical access by locking any rooms, cabinets and cases housing computer equipment protects against this type of vulnerability.

You can buy locks from most computer stores.

Step 3 - Storage

Saving files on individual computers etc. can be hazardous for many reasons so we use a NAS which stands for Network Attached Storage.

Basically, it is like a mini server where you can save all your work and files for sharing for a fraction of the cost of a full server. It also has software to help the process of backing up.

The reason we use a NAS over just an external drive is that it usually has at least 2 drives which copy each other so if one goes down you have a spare. Just add another drive and it should auto all copies of files.

NAS systems start for as cheap as $200 and go up in price depending on configuration and software.

They are usually only used to store work files, photos and graphics. You can then allow access to specific users.

Here is a comparison of some of the best NAS Hardware. Always try and get something local so you have support for your critical files.

Simply look up on Google for the Best reviews of NAS hardware for this year in your area.

Docking Station

If you are only a small home business you could use a Docking Station. In fact all businesses should have one as they are a great backup solution.

The other day a customers HD crashed and we replaced it with a new HD and attached our docking station and put in the old HD and were able to copy all the files off it to the new one.

You can use it for other storage media as well.

Multi Function Docking Station

Step 4 - Backup

Now you have your NAS storage set up you can backup any files not being shared on the NAS.

A NAS can also protect the data stored on it by being configured to **Redundant Array of Independent Disks** (RAID). A RAID setup is essentially two or more hard drives connected to add extra redundancy (storing data concurrently on all of the drives) and to act as a failover in case one of the hard drives fails.

What about a Robbery or Fire

Your NAS will be **password protected** how this does not help in a fire or flood, so we like to organize a cloud storage solution as well. We personally use Amazon S3 for a storage solution as you only pay for what you use.

https://aws.amazon.com/s3/

There are lots of tutorials and software on how to set this up. Because all your files are now all on your NAS you can simply back it up to Amazon. You could also use the docking station to make a copy and take home or store offsite.

Setting up Time Machine for Mac

Automatically back up all your files with Time Machine, which is built into your Mac, or choose another backup method. You can also use the NAS or docking station.

Setting Up For PC

For the PC user, CloudBerry Backup ($US29.99, Windows) is more of a traditional backup tool for this job or you can even do it for free via FTP backup.
You can use both software program in Auto mode and organize to replace changed files or add new ones.

Step 5 - Train Your Users

Training Your Employees

Training employees is a critical element of security. They need to understand the value of protecting customer and colleague information and their role in keeping it safe. They also need a basic grounding in other risks and how to make good judgments online.

Most importantly, they need to know the policies and practices you expect them to follow in the workplace regarding Internet safety.

One of the sites we use to provide resources to our Customers is called **Stay Safe Online**

Its important to control what happens with your computers and what staff can do.

Make sure you have laid them out clearly so for example:

We don't let staff use their own hardware in the office like USB's, mobiles etc.
We don't let them access their own email accounts as this is where most trouble starts. Have good passwords etc. And so on.

Videos

Learn how to protect yourself online.
Click here to open the Youtube video
Learn how to protect yourself online while on the go.
Click here to open the Youtube video
Learn how to protect yourself online while at home.
Click here to open the Youtube video
Learn how to protect yourself online while playing video and online games.
Click here to open the Youtube video

Step 6 - Anti Virus Software

From our interaction with small businesses we found most small businesses are using free antivirus software and many do not keep it up to date.

Virtually none are using malware blockers and we have only found one using any end point blocking software.

Most are all individually entered and on many of the computers the staff had disabled or failed to keep it updated. The beauty of upgrading your operating system to the latest version is that both **Mac and PC have internal Virus Software**.

Antivirus: free or paid for?

Our tests focus on paid-for and free AV products. Paid-for AV products usually offer better technical support and more comprehensive protection features than free programs. Internet security suites go further still, offering firewalls, parental controls, identity theft protection and more. They are also managed from one computer rather than separately.

We mainly suggest the paid small business solutions because they have great additional features. Some of these are central admin, password protection, financial data security, Internet protection, policy management, regulate or block employee access to games, leisure websites, control social networking site access, limit IM communications and general data protection

Our Suggestions for both free and paid Antivirus Software.

Our current antivirus recommendation is **Kaspersky Internet Security** – which has a 99.8% detection rate, lowest processor payload & lowest false positive detection. It has personal up to full business versions which give the owner full control over his digital assets. **Kaspersky Anti-Virus**

Avast or **AVG** are definitely the better of the free AV software which should only be used for personal or one computer businesses. These both have mobile, PC and Mac versions.

Step 7 - Email Security

Most cyber security problems for most businesses will happen because someone clicks on an email link.

Email security is a priority for all businesses, with the growing threat of hackers, viruses spam, phishing and identity theft, as well as the need to secure business information.

Email security is mainly a manual thing. Antivirus software will highlight most of the viruses etc. however the phishing and ransom ware comes in through what seems to be an official email so very hard for most software to detect.

Most people dealing with email everyday in business will notice differences or things out of the ordinary. Lets face it no banks, financial institutions, Govt dept etc will ever send you an email asking you to login from the email or ask for a password.

Here are some warning signs (Youtube Video) of possible scamming links:

The Link is a Shortened Link

Obviously, if a link is shortened, you can’t tell whether it’s bad or good just by looking at it, but there are tools to allow you to view the true destination of a short link without actually clicking it. Check out our article on the Dangers of Short Links for details on how to view a short link’s destination.

The Link Came to You in an Unsolicited Email

If you received an unsolicited email that is supposedly from your bank asking you to “verify your information” then you are probably the target of a phishing attack.

The Link has a Bunch of Strange Characters in it

Oftentimes, hackers and malware distributors will try to conceal the destination of malware or phishing sites by using what is known as URL encoding. For example, the letter “A” that has been URL-encoded would translate to “%41”.

Using encoding, hackers and malware distributors can mask destinations, commands, and other nasty stuff within a link so that you can’t read it (unless you have a URL decoding tool or translation table handy). Bottom line: if you see a bunch of “%” symbols in the URL, beware.

Step 8 – Website Security

Take control of the assets

One thing we have noticed over the last year of implementing cyber security for small businesses is when it comes to their website, they have no idea who owns their domain, How to update their own website and have never added any new content let alone check if it is secure.

Stay up to date

Even the simplest websites rely on software which was not authored by you. Since software is created by people it is inherently flawed and contains errors or bugs. You should know the components your website relies on to operate, and keep tabs on the known issues, and releases of updates and patches. This is why we love wordpress as it is easy to keep up to date and has simple plugins to help secure your site.

Use strong passwords

You need a username and password to place files on your web server or to update content. Make sure you're not using the default password and chose a password which is difficult to guess.

SSL Certificate

These days more and more specialists are suggesting we use SSL certificates on our websites especially if we have any type of payment system. Many devices wont open pages if they do not have ssl encryption which will be https:// for the url.

SSL Certificates are small data files that digitally bind a cryptographic key to an organization's details. When installed on a web server, it activates the padlock and the https protocol and allows secure connections from a web server to a browser.

Post Attack Strategies

Step 9 – Ransome and Hacking

In your business your going to get three main attacks. Viruses and malware, hacking and Ransome ware.

Viruses and Malware

If you have kept your software up to date and installed good anti virus and malware software then all of these will be handled automatically. For those that are super nasty see the ransome ware solution.

Hacking

We see it in the news all the time now and basically there is very little you can do. If companies with millions and a IT dept cant stop them then we have little chance.

Unless you have a lot of money or something they really want the chances are pretty slim. The best way to deter them is by using strong passwords and keeping good backups.

Ransome Ware and Nasties

We have had a few new clients in this situation and quotes to fix and repair have been exceptionally high from Cyber professionals.

Our main solution is to remove the hard drive and install a new one. Reloading the operating software and programs we recommended previously so you end up with a clean system.

You can use the docking station to access the old drive externally. Run a check on it first however Ransome ware usually just places a file on the hard drive.

If you are just a home business and you only have programs on your computer and save everything externally then you could also reformat however HD are so much cheaper these days.

I only have programs these days.

WMFP AUSTRALIA

WEBSITES FOR $300 +GST

Includes Hosting and SSL Security

Your Website will be built on the Wordpress CMS and will include Yoast SEO, WP Cache and Woo-Commerce shopping cart. It will be developed on the very popular Divi responsive theme. It will be hosted on an Australian cloud server for speed and includes a SSL security. You can have un-limited pages, graphics, posts and products

wmfp.com.au

Get A Website For

$300 + GST

Includes compiling your website, hosting for 12 months and then $99 per year hosting and support.

Fast Hosting With SSL

Fast Australian based hosting with FREE SSL security on every account provided for 1 year then $99 per year after that.

WordPress & WooCommerce

Wordpress loaded with WooCommerce. You can add unlimited pages, images and products. We will fully manage or you can self manage or a mix of both.

Responsive

Your site will be fully responsive so can be viewed on all devices. Over 70% of views these days are on mobiles. Visitors can view and buy products on their phone.

FIND US:

Brisbane, Australia
+61 481269620
quentin@wmfp.com.au

Videos

Hacking 101: Frank Heidt at TEDxMidwest

Watch Here Online

"Hacking 101"! Frank Heidt, one of the world's foremost authorities on cyber security, gives the audience the gift of "straight talk" regarding how companies and people get hacked every day and how to avoid becoming a victim.

James Lyne: Everyday cybercrime -- and what you can do about it

James Lyne: Everyday cybercrime – and what you can do about it

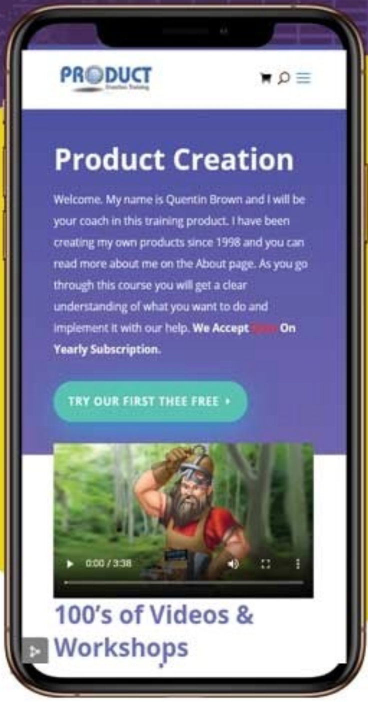
Watch Here Online

PRODUCT
Creation Training

CREATE YOUR OWN PRODUCTS

PRODUCTCREATION.COM.AU

Discover how to create your own digital products and sell online with these easy to follow video and workshop tutorials.



PRODUCT

Product Creation

Welcome. My name is Quentin Brown and I will be your coach in this training product. I have been creating my own products since 1998 and you can read more about me on the About page. As you go through this course you will get a clear understanding of what you want to do and implement it with our help. **We Accept Qoin On Yearly Subscription.**

TRY OUR FIRST THEE FREE ›

0:00 / 3:38

100's of Videos & Workshops

WHO WE ARE?

We have been creating products and services since 1998 and helped hundreds of people do the same

VIDEO TRAINING

A growing number of video tutrials for different industries with workshops.

ZOOM MEETINGS

We use ZOOM for live Q & A plus additional training and support when required.

GROWING RANGE

We are adding new product creation courses regularily and keep you updated on new courses

BUSINESS PROGRESS

We help on the business side also with website, eCommerce and marketing tutorials and advice.

MONTHLY $10 AUD
10 MONTHS THEN FREE

ONE TIME $80 AUD
NO MORE TO PAY

GET IN TOUCH
+61 481269620

Macgregor, Queensland
Australia 4109

Qoin
Accepted Here