## Home page

Mark Ellis

Cyber Security Consultant

Citrix Consultant

Architecture optimised for security.

### Services I offer:

I have a Masters Degree in Cyber Security, over 50% of a Computer Science Degree (ongoing study), Citrix and Microsoft qualifications, and 30 years’ experience working as a Systems Engineer.

* I can deliver a military grade solution to keep your most secure data and communications safe.
* Review of security architecture. I have experience at a senior level in very high security environments.
* Cyber Security audit using the [NIST](https://www.nist.gov/cyberframework) framework.
* Identify security weaknesses and points of risk.
* Cost optimisation. I can review your current operations and advise on removing waste, inefficiency and duplication of effort or software.
* Set up systems monitoring to collect the data to make data backed decisions.
* Manage projects. I can get people moving and get results. Technical skill and experience can make a big difference when managing a project. I am not afraid to have “*difficult conversations*” if required.
* Microsoft Server Security Hardening. Remove unused software and disable unused services and features. This reduces the attack surface of servers. There is nothing to buy or add and yet so few people attempt it.
* Use Microsoft AppLocker, a feature you already own, to do whitelisting of your Microsoft servers.
* Create AD Policy to deploy a set of Microsoft Firewall rules that blocks data collection by well-known offenders.
* Optimise profile management, including browser cache and OneDrive behaviour.
* Network printer optimisation.
  + Optimise drivers. A single bad driver can damage your whole printing system.
  + Minimise print job “*tromboneing*” where print jobs traverse the WAN more than they should. It is really common for a user in a branch office print to a printer across the room but the print job goes via the WAN to the corporate print server and back out to the branch office. (You double your network traffic charges if it goes into the cloud.)
* I can fix all your **Citrix** or **Remote Desktop Services** problems. I am really good at Citrix.
  + Citrix & RDP Printing,
  + Fix applications that won’t run on Citrix or Remote Desktop Services.
  + PVS and MCS
  + Citrix & Remote Desktop Services Profile and cache management.
* Write or update security policies.
* Design and deliver Cyber Security training to staff.
* Studies have found 65% of hacking attempts are internal. Whether this is a departing employee wanting to take a client list with them to a new employer, to an employee wanting to harm your company due to *‘ideological differences’.*

I am based near Cessnock in the NSW Hunter Valley. I normally travel to site anywhere in Australia, spend time on-site collecting information, then return home to write up reports or deliver agreed work remotely.

### Attackers have first mover advantage

**Attackers have first mover advantage**. In defence you are always playing catch-up.

Your network and computer systems are a contested space.

Convenience is the opposite of security and it is up to you to determine the balance that is right for your company.

* USB flash drives can walk data in and out. (How the Stuxnet virus got into the Iranian nuclear program.)
* BYO Device. Popular among younger employees.
* Take home laptops. I once worked for a power company that had a serious incident because an employee took home his company issued laptop, connected to the Internet via a home router, was infected with a worm, then he came back to work plugging it into the company network. That worm had a zero day exploit in it and every server in the company was infected.
* Another company I worked for allowed employees to surf the web at home with their work laptops then come back to work and plug them into the SCADA network. What could possible go wrong with this? This is not just some quaint little company. I am limited in what I can say about this…

### Someone hacking your company?

Since I have been doing this I have been surprised how much cyber warfare is going between rivals in small and medium companies. The most common threats to your company are:

* Insiders, like the salesman who leaves and takes your customer list with him/her.
* Clicking on the wrong link. The email might be claiming to be from MyGov or the ATO with some alarming demand for payment attached.
* Software you have installed you thought was safe but steals you data, with your permission; or didn’t your read page 271 of the End User Agreement?
* Many well know cloud storage services and email services look through your data and sell it to marketers. Google and Microsoft don’t even make a secret of this. Edward Snowden disclosed it is also government agencies looking through your data.

### Passwords

One of the most common mistakes is overly simple passwords on web sites and email accounts. 91% of people use one of the 1,000 most popular passwords and 98% of people use one of the 10,000 most common passwords. Consider this: If an adversary tries just 5 passwords per day they will have cracked 91% or their target’s accounts within 200 days.

The reuse of passwords is a major problem. If one site on which you have an account on has poor security that results in a data breach it could leak your user name (often the email address) and your password with weak encryption. If the same password is used across a series of cloud services and web sites the attacker now has a valid username and password for a large number of sites.

Check out: <https://haveibeenpwned.com/> too see how often you have been compromised.

It is shocking how much data is lost via poor practices with passwords. This is particularly vulnerable when a company uses a large number of cloud services and SaaS where poor password practices by any one employee could be the source of a data leak.

Solutions to the password problem may include:

* Always use long complex passwords.
* Use password management software like **KeePass** or **Password Safe** <https://www.pwsafe.org/> so you are not trying to remember dozens of different passwords.
* Use Multi-Factor Authentication (MFA)

A list of the 1,000 most common passwords can be found here: <https://lucidar.me/en/security/list-of-1000-most-common-passwords/> There is software that can cycle through this list very quickly adding common numeric substitutions and numbers at the end.

The 10th most common password is **dragon** but **Dr@g0n951** is not much better as it will be quickly guessed by password cracking software. Computers are fast and can run millions of variations on the common list in minutes. According to Bitwarden at: <https://bitwarden.com/password-strength/> **Dr@g0n951** would take 3 minutes to crack. Go to the site and test out some of your favourite passwords.

### Don’t have faith your internal network is secure

I was doing a Citrix project at one of the Universities in Sydney when the G:\ drive, containing a large number of documents, was suddenly encrypted. One of the administrative staff had clicked on a link in an email and triggered a ransomware attack.

It was responded to quickly:

* Her computer was taken off line
* Her computer was reimaged
* The G:\ drive was restored from the nightly backup tape with some data loss.
* The employee was given some training about clicking on unknown links.

She did the same thing the next day with exactly the same result. Often the social engineering is more powerful than the training.

Two things went wrong here:

* This employee had more access than she needed.
* The employee was doing email and surfing the web, two inherently insure applications, on the same network as valuable data.

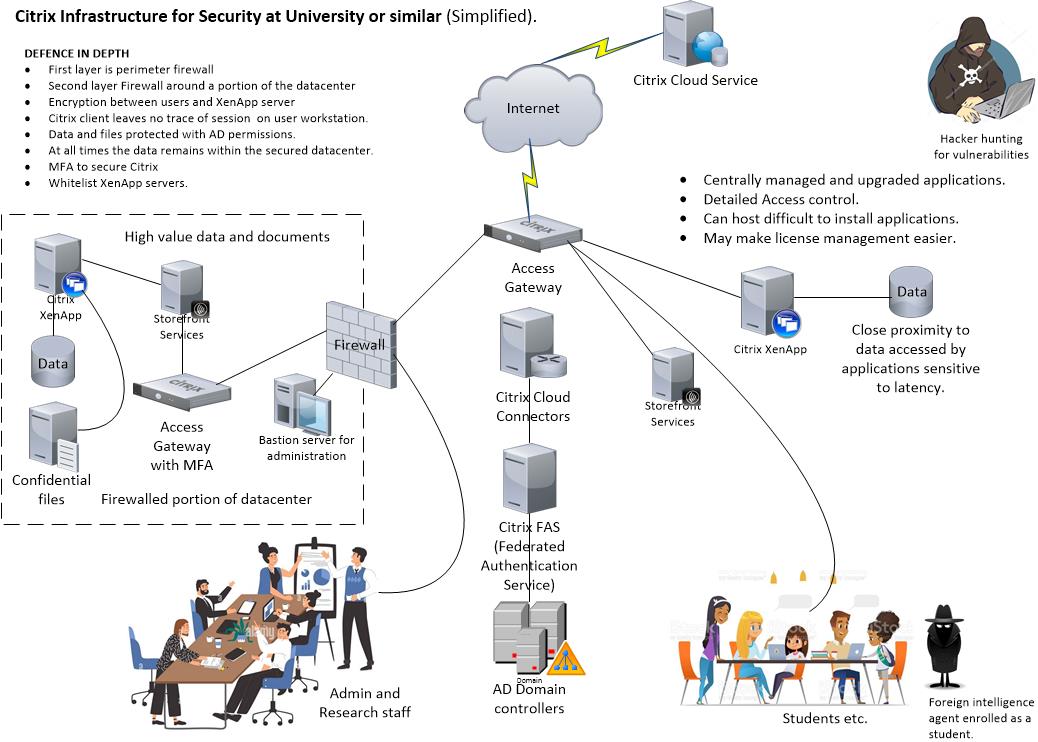
Gone are the days when a good firewall and an antivirus program will provide adequate protection.

General administrative users should not be doing email, web surfing, using BYO devices, or other risky activities on the same network you have your sensitive data and valuable intellectual property stored. It can easily be argued that there should be no path between sensitive data and the Internet.

There are a number of strategies on how to separate the administrative network from the network containing sensitive data and intellectual property.

## Citrix & Microsoft Remote Desktop Services (DRS)

The Citrix XenApp and XenDesktop products or Microsoft RDS have some inherent qualities that make them ideal in a high security environment.



## Citrix Printing

I have seen more problems with Citrix printing than any other feature. Get it right and it works fine, get it wrong and you will face dozens of spooler crashes per day.

If you have Citrix printing problems I can fix them.



## Network Security

Two rules of network security:

1. You can never prove you are secure. However, you can reduce risk.
2. Security is always a balance between convenience and security.

### Server hardening

This is about reducing the attack surface on each server so find an article from a reputable source on server hardening and follow it. Use intelligence, decision and testing in applying the hardening. Remove any roles or features not needed by the server for its job. Disable any services that are not required, for example the print spooler service is not required on most application servers. Don’t install any software that is not actually needed, like management tools when they are managed from a jump box or install utilities *“because we put them on all our servers”.* Be very aware that some software agents are a little too much like the spyware of *“big data”* for my comfort.

This reduces the attack surface on the server leaving the malware less to work with.

You might want to use WireShark on machines every so often just to see where they are sending data. Uninstall it when you finish your investigation.

### How private is Microsoft software?

Microsoft’s business model has moved from a business that sells software to one that also sells user data. To reduce Microsoft surveillance, and you don’t want to transition to Linux, then have a look at these web sites to reduce the Microsoft surveillance.

<https://github.com/hagezi/dns-blocklists#native>

<https://cdn.jsdelivr.net/gh/hagezi/dns-blocklists@latest/hosts/native.winoffice.txt>

<https://www.oo-software.com/en/shutup10>

### Whitelisting of servers

What is whitelisting and is it better than anti-virus? Think of anti-virus like a night club where any member of the public can enter except know trouble makers. The doorman has a blacklist and all others are given the benefit of the doubt. You only find out about a previously unknown troublemaker when they get rowdy inside.

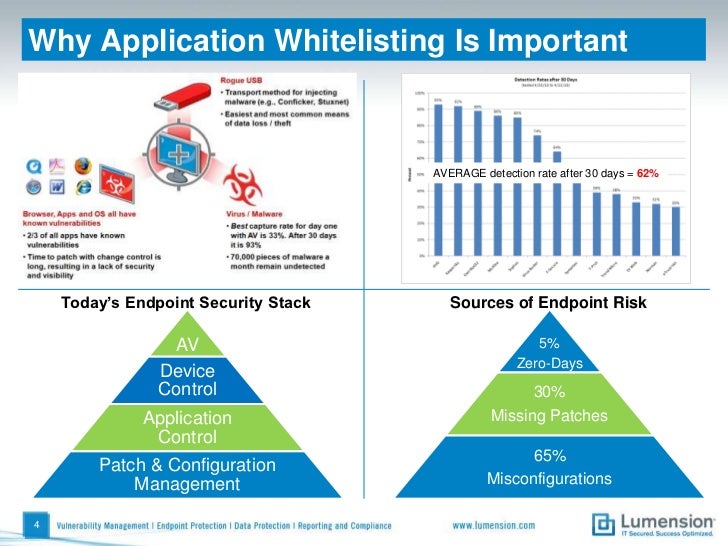
Whitelisting entry is via invitation only. You are on the guest list of know good people or you don’t get in.

On a tightly whitelisted server only verified software is allowed to run. If a piece of malware finds it way on and tries to execute, the whitelisting software shuts the process down immediately and logs the event.

Whitelisting desktop computers can have its challenges with use expectations, but your server room is a much more controlled and I recommend tightly whitelisting all servers.

Whitelisting software you might want to evaluate include:

* Microsoft AppLocker (a free included feature with Windows server.)
* McAfee Application Control
* VMware Carbon Black application Control
* Symantec Endpoint Protection Whitelisting.



### Web application firewalls

Here is a really well written description of a Web Application Firewall by Crowdstrike:

*“A Web Application Firewall (WAF) is a security device designed to protect organizations at the application level by filtering, monitoring and analysing hypertext transfer protocol (HTTP) and hypertext transfer protocol secure (HTTPS) traffic between the web application and the internet.*

*A WAF acts as a reverse proxy, shielding the application from malicious requests before they reach the user or web application. Part of a comprehensive cybersecurity strategy, a WAF helps protect the organization from a variety of application layer attacks, including Cross Site Scripting (XSS), SQL injection, Zero Day attacks, and Denial of Service (DoS)/Distributed Denial of Service (DDoS) attacks.*

*A WAF differs from a network firewall in terms of the type of protection it provides and how that security is applied. Put simply, a WAF protects the organization at the application level by analysing all HTTP/HTTPS communication, whereas the network firewall acts as a barrier that prevents unauthorized access to the network on a whole.*

*On a technical level, the key difference between a WAF and a traditional firewall pertains to where the operational layer of security is applied as defined by the Open Systems Interconnection (OSI) model. WAFs protect from attacks at OSI model Layer 7, or the application level. Network firewalls operate at OSI model Layers 3 and 4, which focus on data transfer and network traffic.”*

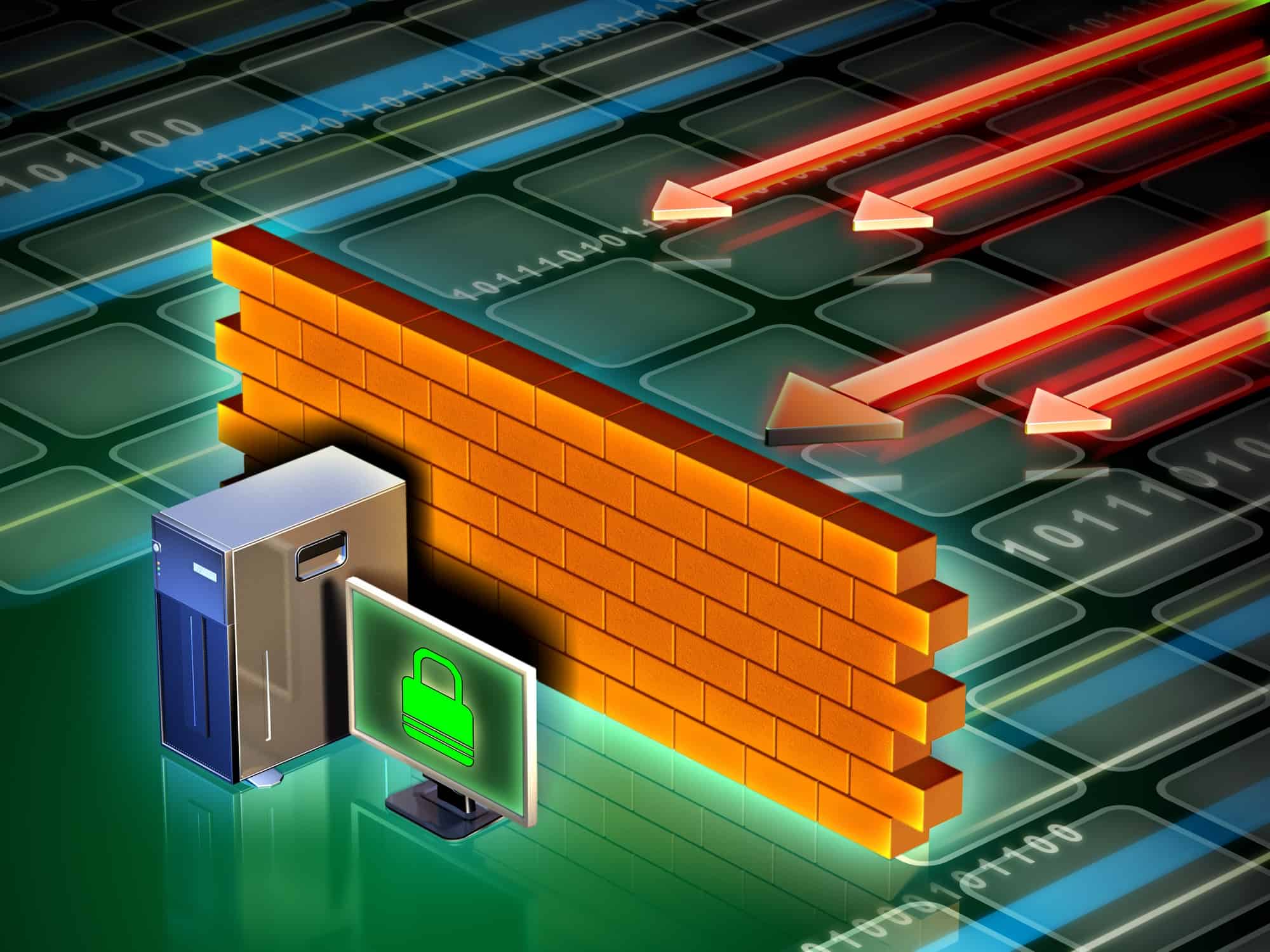
From Crowdstrike: <https://www.crowdstrike.com/cybersecurity-101/web-application-firewall/>

I was checking the price on some Web Application Firewalls for a design. Some are horrendously expensive so if you are doing architecture **check the prices** before making your recommendations.

### Monitor your firewall

How many times have I seen firewalls with **any-to-any rules** enabled on them? *“But I needed that to make some-program work.”* All too common. Firewalls have to be monitored regularly for suspicious behaviour. What is all this FTP traffic to Russia?

You need people who really know what they are doing to configure and monitor these things.

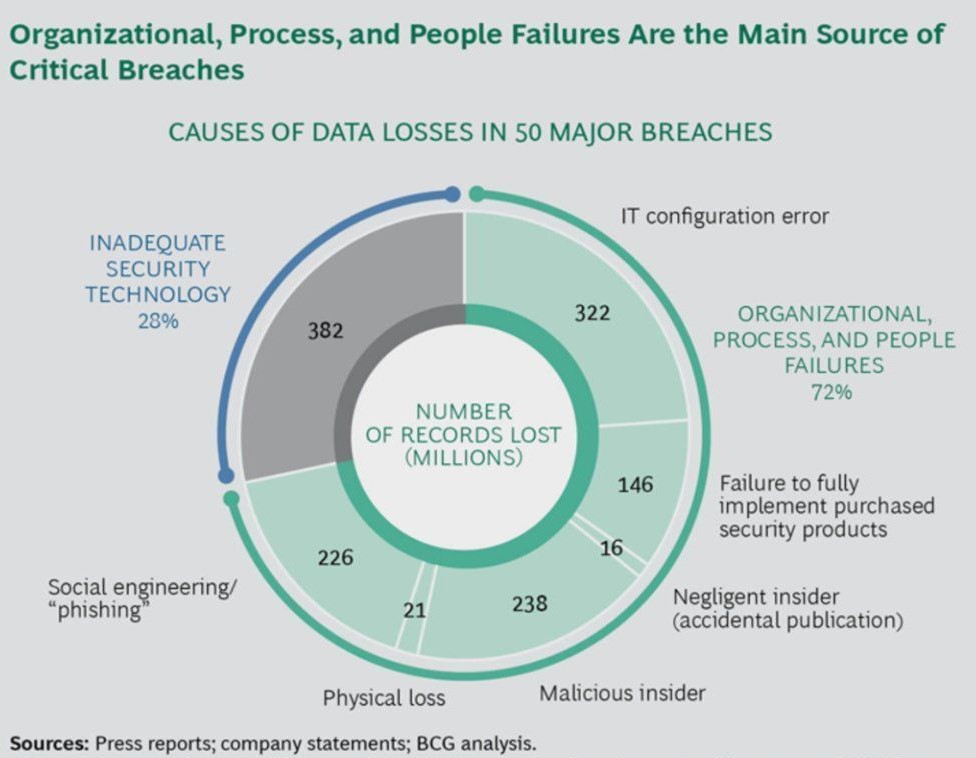


### Segment your network and firewall your datacentre

Think about your user base. Some of them are *“brave”* clicking on links in emails from unknown sources (or a spoofed e-mail from a manager to them), installing software they have downloaded from the Internet and clicking yes to run a macro any time a document asks for it. Some user want to connect their own devices and you have no idea what is installed. Any of these actions open the door to malware resulting in the loss of intellectual property, personal information on your customers, or destruction of data. In the worst case it could bring fines and loss of reputation against the company, even criminal charges against directors.

It is a really good idea to segment your LAN with VLANs and put your datacentre behind a firewall. Treat your user’s computers as nothing more than semi-trusted.

I don’t know how accurate the chart below is but it rings true to my experience. Look at how many of the data breaches were preventable through good procedure and properly trained people.



Source: <https://aristininja.com/causes-data-loss/>

### Timely patching

So often I see product managers unwilling to patch computers because the patch “*might break something*”. It is certainly true there are potential risks but it is a balancing of risks. Once a vulnerability is exposed it alerts the potential attackers of something they can exploit and the risks start rising rapidly.

It is essential to have a timely testing and roll out of new patches. And remember all security patches need to be installed. Don’t let administrators become selective about what patches get installed.

## Designing an appropriate level of security

Secure design and practices are inconsistent with easy access and convenience so each organisation must decide where they are comfortable on the security, convenience spectrum.

At one extreme data can be shielded from EMP and TEMPEST attack by a Faraday cage. Guards and gateways that include biometric authentication to access the datacentre. Once logged on you have minimum necessary rights to do your job. You would have redundant cooling and electrical power. Any outside data links are via high encryption, failover and backup are to a similar datacentre far enough away not to be caught in the same nuclear blast, tsunami, earthquake etc.

At the other extreme everything is in the cloud using SaaS, Microsoft 365 from home computers and end point device including employees phones and tablets. Add low levels of password complexity and lack of multifactor authentication and your data is accessible by any government agency or competent hacker.

## Complexity

Never buy technical infrastructure that is beyond your ability to support competently. Don’t be that organisation that *‘solves’* every problem with a new product.

Might sound obvious, but I have seen way to often organisations have been sold too many complex solutions that are above the skill levels of their staff to get anything more than basic functionally out of. The extra un-configured feature set is just left as a larger attack surface for a cyber-attacker.

SAN infrastructure is complex and expensive. Do you really need a SAN? Would you be better off buying 2 unit rack mount servers and using local disk? Also, local disk access is often faster than SAN disk access that can introduce bottlenecks.

### One group has no understanding on their impact on other systems.

At a certain well-known bank the VMware guys were moving virtual machines around that had been created by the Citrix PVS servers. The VMware guys were using VMware tools, the database behind the PVS server had no record of the new location. Teams didn’t communicate. Months were spent trying to fix the *“Citrix problem”.* Too many silos acting without the understanding of the many other complex systems, no cross training. The total system was too complex for every team member to have a conceptual understanding of the many different components.

This bank had contractors that passed all communication with the client via Customer Delivery Managers who didn’t understand the subject matter.

### Over-buying on your one shot cap-ex.

So often I see rack after rack of servers running at less than 5% of CPU. A project is proposed and scoped. The proposal and business case, complete with all costing, goes to management for approval; and it is a one shot approval. If you go back and say we need some more hardware or software licenses that is considered a failure and a cost overrun. So you spec everything big, from the start. A lot of solutions are difficult to right size until you see how your users are using them.

Educate your managers that every solution will be specified on *‘just enough to do the job’* but may need more resources if the project is successful and is heavily used. A successful system will be heavily used by the staff and having to come back for more hardware resource should be seen as a sign of success.

Change your business culture so you don’t have this one shot at a cap-ex with its incentive to over specify and over order.

It is not just hardware costs but 24 x 7 power costs, air-conditioning costs, maintenance contracts, software costs for backup and antivirus, patching and upgrades, lifecycle management etc. The total cost of ownership of every server is remarkably high.

### Leasing computer hardware

You have to be very careful about leasing server infrastructure often servers sill performing essential roles 7 years after installation. Leasing companies make a lot of money on *“lease inertia”* where are lease was intended to run for 3 years runs on for say 5 years. I have seen computer racks on 3 year leases when the useful life expectancy of the rack in the company could be 50 years.

### The Cloud first solution

Cloud is not necessarily the solution to the hardware problem as I have seen systems over specified in the cloud. Cloud companies make a substantial profit on these services. Most of Amazon’s profit comes from their AWS division. While cloud companies have economies of scale, and a level of discipline in their range of offferings, they make a fat profit margin on the services they sell. Once you reach a certain size most companies will find self-hosted hardware is better value for money.

I have seen emergency migration out of the cloud due to unexpected costs. If a company is using micro-services in a serverless design there is a risk of endless loops. Programming mistakes can become VERY EXPENSIVE learning experiences.

### Five tools to do the same job

I have been involved in software audits and it is not uncommon for an enterprise to have multiple tools, sometimes each with full site licenses to do the same job. It is common to see 2,000 or 3,000 different applications across an enterprise. Every new application is a risk. Every application may contain spyware, *“No that is not spyware, it is telemetry so we can better server you.”* Every time that software company changes ownership the next *‘upgrade’* may be spyware.

Rationalise your applications, centralise buying, and make sure every software product is **Common Criteria certified**. There are many software products that exist because of their ability to harvest data, not because they do what the advertised function claims.

### Single vendor technology stack

I have encountered real problems with server hardware, Host Bus Adapters (HBA) drivers and firmware, SAN firmware and management software, and Hypervisor compatibility. When it comes time to do upgrades the **compatibility matrix** overlayed from different vendors can make life *“interesting”,* in the way you might find the **Nine Circles of Hell** interesting.

Then you have to manage license renewals that can occur at different times. They won’t be synchronised and they are designed to be financially inefficient for you.

**Nutanix** with **VMware** can offer a fabulous and flexible solution, but do you really need all the features? Have you compared **Red Hat Hyperconverged Infrastructure Software** to Nutanix? Have a look at: <https://www.gartner.com/reviews/market/hyperconverged-infrastructure-software/compare/nutanix-vs-red_hat>

Consider commodity I and 2 unit rack mount servers such as **Dell servers** with plenty of disk running **Hyper-V** (or **Red Hat KVM**) as a hypervisor. It can be a simple cost effective solution. Hyper-V can be free with your Microsoft licensing and installs on commodity servers. Not the full feature set of VMware, but will Hyper-V fulfil your requirements?

Look through the marketing hype and the latest bells and whistles. Most hardware is set up once, Operating Systems installed and applications installed. Then application owners don’t want to touch them until they are forced to. Many of the ‘*bells-and-whistles’* with expensive products are never used.

Efforts should be made to reduce complexity at the expense of features because the more complex it is, the more likely you are to have mistakes. Try to keep the technology stack with a single vendor. All too often vendors point at the other company’s product and blame them for the problem.

A small hint on hardware, many Defence and Intelligence agencies won’t use servers manufactured in China. How can you know the full function of every chip on the motherboard?

## Disaster recovery

What is a realistic level of disaster are you facing? Disasters can include:

* Power outages, possibly for days or weeks. Remind me how renewables are backed up on windless nights and how often do wind droughts occur? Work it out here: <https://anero.id/energy>
* Flooding from either outside the building or pluming problems inside.
* Severe weather events - storms, floods, bush fires etc.
* Loss of WAN connectivity, eg. building works cutting the data cable.
* Disk, server, switch or router failure.
* Mistakes by IT staff. This is a very common cause of outages and data loss and is often followed by the blame game. New staff and contractors usually lose the blame game.
* Malware, virus, worm, cryptolocker etc.
* Damage by hackers: Pranksters, competitors, cyber activism (not woke enough, or too woke, or the social media post that has inflamed activists) or state actors.
* Civil unrest after a controversial election result.
* Say and employee was running an illegal Dark Web site from your data centre and the police turned up and seized all the servers? Servers on the TOR network are easier to set up than you might think.
* There is the risk of another pandemic, maybe the next one is more deadly?
* The risk of war should not be underestimated. There are plenty of conflicts simmering in the world. Middle East, Ukraine, Taiwan etc. Remember that this could include the cutting of undersea cables to isolate Australia from the world Internet and this could affect SaaS products, cloud computing and software that needs to dial home regularly to reauthorise its license.
* War can include cyberwar, terrorism, regional warfare not involving Australia, regional war involving Australia, an EMP attack, through to a World War with nuclear weapons.
* Sabotage of equipment or data theft by a disgruntled employee. Data theft is very common by staff going to a job with a competitive employer.

If you had been told in mid-2019 that you needed a robust pandemic plan you probably would have thought it was unrealistically improbable? That there was a risk of an illegal bioweapon escaping from a Chinese weapons research facility that would kill millions of people, sounds more like science fiction, or a plot from a B Grade spy movie.

## Secret email

Email was never designed to be secret. Think of it like sending a postcard, the message is written on the back for all who handle it to see. The major free email providers like Gmail and Outlook make no secret of them looking through your email to collect marketing data, map your contact networks, and then share it all with thousands of marketing companies and the US intelligence agencies. Even your on premises corporate email is exposed to viewing by tech companies once it goes out to third parties.

### My recommendations for improved security and privacy

Set up a laptop computer as a dual boot system with your normal Windows 10 in on one partition and Linux Mint on another partition. Generate and store your private documents in the Linux Mint partition. Linux can read documents from your Windows partition (if it is not encrypted), but not the other way around. You might want to set up a small partition with FAT32 (or use an SD RAM card if your laptop has a port for it) that either Windows and Linux can read and write to.

Install Libre Office as part of your default Linux Mint install. (I have no confidence at all in the privacy and security of Microsoft 365.)

Do email, calendar etc. using the German based **Tuta** which provides the privacy assurance of the GDPR privacy regulations. See: <https://tuta.com/> You can set up your own domain name on Tuta.

Install **Password Safe** <https://www.pwsafe.org/>

### HOW TO USE IT

It is only secure while you are dealing with other people in the Tuta or you attached a pre-shared password.

Both ProtonMail and Tutanota claim to offer end-to-end no knowledge encryption, and maybe they do, but I want to add another layer of encryption on top of that.

Create your secret message in FreeOffice and encrypt it with a long, complex password. Save your documents and attach it to the email in ProtonMail sending your message as an attachment.

Save your passwords in Password Safe so you can copy and paste passwords. Passwords are a weak link as simple ones can be cracked by machines fairly easily.

You have to share these long and complex passwords with your colleagues. Put them in a text file, save them on to a USB flash drive, and hand deliver them to your colleague.

NEVER be tempted to starting surfing the Web or getting on to Facebook on your Linux partition. Web browsers are too vulnerable to malware to totally trust them.

Any highly component computer technician should be able to set this up and provide training on how to use it. You can also employ me to do it.

Just remember any email you send outside the ProtonMail (or Tutanota) environment loses the end-to-end encryption. The message that was encrypted with FreeOffice will still be encrypted but you have lost a layer of encryption and are starting to leave visible meta data.

This is inconvenient. You are right. What is important to you? Privacy or Secrecy? The choice is yours.

## Want a top 1% income in IT

In Australia to earn in the top 1% of incomes in 2021 you need to earn at least $351,000 per annum.

If you want to have assets in the top 1% you need to build up a portfolio of over AUD$8,000,000.

On Wall Street a key reason why they make such big incomes is not a very high hourly rate but a good rate and long hours. Wall Street employees are not 9 to 5 people; it is common for them to work 80 hour weeks.

Median income for a Wall Street trader is US$250,000 = A$391,000.

Average income for a Wall Street trader is US$422,000 = A$660,000.

The very high earners make the average MUCH HIGHER than the median.

So you are an Australian IT guy and want to earn over A$350,000 placing you in the top 1% in Australia?

Early in your career build qualifications and experience that will give you string skills in a highly demanded area.

Once you have strong skills get a contract that pays $120 per hour. (Easy enough in IT.) $120 x 40 hours per week x 50 weeks per year = $240,000 per annum. Good but way short of the top 1%. You still need an extra $111,000 per annum.

At $120 per hour you would need to work a total of 58 hour per week. Another 18 hours per week work beyond the 40 hour contract is required. Can you arrange to do overtime on a regular basis? Especially after a colleague leaves? *“Just give me a bit of overtime and I can do his job too.”*

If you are able to work 80 hours per week at $120 per hour that would gross: $120 x 80 hours per week x 50 weeks per year = $480,000 per annum. (80 hours per week would kill me.) Some people can enter into arrangements where they are working two 40 hour per week jobs.

## WHAT TO DO FOR THE EXTRA $111k/ANNUM INCOME?

Investment income is good. Buy 5 lower middle quality apartments each paying a rent of $400 per week will give you $100,000 per annum that will rise over time as rents rise. Of course you will need borrowed money to buy them, but work hard at paying the loans back and once paid off this is clear income.

### Earn some extra cash

*You do not have to be Mark Zuckerberg, he said, to be an entrepreneur. "You can learn basic web development," he said. "You can go to Codeacademy.com, learn the basic skills in three months, then sell them on Freelancer.com, where there are millions of jobs. I know 15-year-olds who are making a few thousand dollars a month."*

**James Altucher**

You might benefit from watching:

**Broke at 50, should you Learn to Code**? <https://youtu.be/2m7Bd6lGxX8>

Do some training:

Professional Certificate in Computer Science for Web Programming

https://www.edx.org/professional-certificate/harvardx-computer-science-for-web-programming?index=product&queryID=98ee5aeb80f152fa234bc0c75fe1e32a&position=1

Good introductory programming course with the CV building Harvard name attached.

Do lots of work and get really good at web programming.

Start your micro business:

So you build yourself a web site to promote your skills. (In my case it has a Cyber Security spin.)

Pimp yourself out on : <https://www.freelancer.com/>

Under these arrangements you can work from home.

Unfortunately, I don’t have the stamina to work a 58+ hour work week. That is 9 hour 40min per day, 6 days per week. Many of us, myself included, could start building the mental and physical stamina by losing weight and getting fit.

In Asia there is something called the **996 work culture**. Work 9am to 9pm 6 days per week which is a 72 hour week less any breaks for lunch etc. <https://en.wikipedia.org/wiki/996_working_hour_system>

Part of being able to work long hours is to manage stress in that time. Having a high level of competency in your chosen area of specialisation is essential to sustaining a high work output. The work has to be in the *Goldilocks zone*, not too hard and not too easy. If you are constantly challenged by work at the outer end of your ability then you will thrive in it. Good managers (they are in short supply) should consider where the edge of the employee’s ability when assigning work. It is important for keeping people engaged.

## GETTING INTO A STATE OF FLOW

Read about this in *“Deep Work: Rules for Focused Success in a Distracted World”* by Cal Newport

You need to choose one goal. Flow takes all your mental energy, deployed deliberately in one direction.

That goal needs to be meaningful to you – you can’t flow into a goal that you don’t care about.

It helps if what you are doing is at the edge of your abilities.

Like all good things training and experience builds competency. This can be built with:

Formal qualifications like degrees and diplomas.

Industry certifications.

Informal study – read relevant books.

This bring me on to my 5 point plan for learning IT but it can be adapted for many things.

## BEING IN THE DAY JOB

Something I learned early in my military career is **don’t take anything to heart**. If something unfair happens to you just get over it. The world is not fair, get used to it. Some days you will be unfairly blamed for something, you will be yelled at, there will be a bad vibe at work. Don’t take it to heart. Find a way to deal with it but working out in the gym, or meditation, or playing guitar is a much better way to deal with stress than alcohol!

Develop the character and emotional maturity to deal with the problems. When a customer or your boss yells at you, don’t feel bad about it, think this a exercising my *emotional robustness* muscle.

When I was in the Army Sergeants would have us stand on parade and shout at individuals an inch from their face things like: *“Private Ellis you look like a bag of shit tied in the middle.”* Once I worked out that they were doing I had to restrain myself from laughing at them.

I was so tempted to reply: *“Sargent, you must have some very good looking bags of shit.”*

An angry person is an undisciplined person and that is their problem, not yours. I have noticed young women have a special fear of people being angry at them. Just learn you don’t take it to heart.

#### Work hard, play hard

I have been to job interviews where I am told we ‘*work hard and play hard’*. This is secret code for – we expect you do a whole lot of unpaid overtime then come out drinking with us. The ‘*work hard, play hard’* statement is a red flag from a potential employer.

The reality is most people can only spend a maximum of 5 hours a day doing top quality work and then spend 3 hours just doing routine process work or socialising, hopefully in a team building manner.

#### Tip for interviews

Towards the end of an interview it is common for interviewers to ask: *“Do you have any questions for us?”* I have found the best response to that is: *“What will be the most challenging part of the role?”* **Listen very carefully to the answer**. You might respond by saying how do you are about that thing, or you might tell them sorry, that job is not for you.

#### Be realistic about what you are good at

Don’t claim to be an expert on everything they ask about. You sound like a liar if you are claiming to be an expert on everything. I have got plenty of contracts where I have said in the interview: *“No, that is not my thing. My expertise is in Citrix and Cyber Security.”* The worst thing that can happen is you start a job working on something they expect you to have way more knowledge than you have. You will end up with a bad reputation and poor references.

#### The company team building weekend

Occasionally you have a real expert who can take a team away for a weekend and challenge the team members by gently pushing the edges of their envelope with activities like abseiling, snorkelling, ball games, escape rooms, debates, problem solving, trivia games etc.

Most times these things are not well run and end up making some team members feel uncomfortable and degenerate into excess drinking sessions. This is especially true when you have people with greatly varying physical capacities, intellectual abilities, and cultural backgrounds. This is especially prone to going wrong when it is run by an outgoing, extraverted senior manager.

One horrendous weekend we were asked to line up according to height. I’m 6’1” and comfortable with my height, but my immediate manager was short and he was standing among all the women. I could tell how uncomfortable he was having his height so publically highlighted. Just thoughtless.

## HOW TO STUDY

#### HOW TO LEARN IT - 5 POINT PLAN

Having done a Masters Degree while working in a full-time job and having a house to maintain, wife, adult daughter and 3 poodles I can offer some suggestions on how to learn IT that may be of use to people:

1. Video lectures from university, Pluralsight or similar sources. <https://pluralsight.com> (Free 10 day trial available).
2. Read a book on it. Read in 45 to 55 minute blocks then take a break and go for a short walk, exercise bike or similar.
3. Play with the technology on a test network. Play in an environment where you have no fear of breaking stuff. I wonder what happens if I try this…? I have test lab based on a mini-tower with 32GB of RAM, quad core CPU and a Broadcom NIC. Use free or trial versions of Hyper-V, VMware or Citrix XenServer and use Microsoft and other evaluation software. (Remember slmgr.vbs to reset the Microsoft trial period.)
4. Make notes from your reading and lectures using the *"Cornell Note-taking Method"* (or an adaption of it) in a notebook and use this as the basis for your daily revision. (Search YouTube for Cornell note taking.)
5. At the start of a study session always do revision of the last session.

#### HOW TO LEARN MATHEMATICS

1. Learning is a noble struggle.
2. Mathematics is a set of skills that must be learned sequentially. Every step is the foundation for the next. If you miss a step then you don’t have the foundations for the next level. Not building strong skills at one level before moving on to the next is the most common reason for failure in mathematics.
3. **Put in the hours**. Sit at your desk and work through the examples in your text book. Just do the work one problem after the next. Do a set of exercises and check the answers. If you are not getting the right answers try to figure out what you are doing wrong.
4. Help can come from your text, other texts, You Tube videos or a teacher.
5. Keep working, grinding through the text books. **Just do the work.**

#### Learning the right skills

How do you know if the skills you are learning will get you the right job? A great example of a spectacular fail in the mismatch of skills with the job market is people who did audio engineering degrees to work at recording studios only to find the professional recording studio industry was contracting and people who had engineered multiple hit records were leaving the industry and getting non-music day jobs. Entry level jobs are almost non-existent.

Another example: People doing degrees in journalism only to find out that the profession of journalism is contracting and there are about 10 graduates for every entry level position.

There are more people studying law at university than there are jobs as lawyers at law firms.

In Australia, at any given time, there are 400 people at university conservatoriums studying flute but there are only 17 full time positions with orchestras in the country. There is spectacular opportunity for disappointment. What are you going to do when you graduate? Became a music teacher and teach more kids to follow in your footsteps of disappointment?

To find out what **skill set** is really required in the job market. Look at jobs advertised in places like <http://seek.com.au> in your competency area and you will see **consistent clusters of skills** that are required in job after job. Build your qualifications and work experience around those areas. Write your resume to highlight your training and experience with those areas.

You have to find out what the world is asking for and build your skills to match. Always do the reality check **before** investing the time and money building the skills.

#### CHEAP OR FREE ONLINE TRAINING

**EDx:** <https://www.edx.org/> This is really good.

Udemy: <https://www.udemy.com/>

Coursera: <https://www.coursera.org/>

Lynda: <https://www.lynda.com/>

Tuts+: <https://tutsplus.com/>

Udacity: <https://www.udacity.com/>

Alison: <https://alison.com/>

Future Learn: <https://www.futurelearn.com/programs>

Open Learn: <http://www.open.edu/openlearn/>

I am not endorsing the quality of any of these and I am sure there are plenty more I have not listed. Find something in you price range that works for you.