Cybersecurity for start-ups

You have developed the next great thing.

It is going to make Google, Facebook and Amazon look like they were not even trying.

You have spoken to an accountant and you have legally protected your business, your family and your self.

You have spoken to a solicitor to ensure all of your Intellectual property is protected.

You have pitched to your investors and they have opened they cheque books for a small slice of the pie.

So you are all ready to go.

Are you?

I can guarantee that your ball tearing idea is sitting on some sort of digital platform, either yours or someone else's.

That digital platform is the realm of the cyber criminal, the accidental cyber terrorist or the budding script kiddy.

They are the greatest danger to your new endeavor.

Before you go any further I suggest you have a quick read of this

---

Passwords, passcodes and passphrases

Your passport to your digital world. Protect them accordingly.
Complex, unique and more that 12 characters long. No personal information.
No easily discovered information.
Do not write them down in a password protected file on your computer

Too hard, use a Password manager

There are a number of password managers available now and they all do roughly the same thing.
If you need additional people to access a system then you will need a corporate one.

Implement 2 Factor and Multi Factor Aujtentication

Something you are, something you know and something you have is the best security available
Username (are), Password (know) and a third one associated with your smart device (have)
That third one can be an SMS or an authentication app.
NEVER GIVE THE CODE AWAY—NEVER

Use and install the latest business and security software.

No Free stuff
Goes to all Software—no free stuff.
Free stuff makes you the product and it is really hard to secure the data

Use anti virus / anti malware on all devices

Get it
No matter what always pay for it.
Nothing for free

Implement the essential 8 strategies where possible

These are simple but effective strategies that you need to apply to your organization.
These strategies include patching, backups, two factor authentication, white listing, hardening, script and macro management and minimizing of your exposure by reducing the number of administrators.

Develop a culture of security (security is everyone's job)

There is no such thing as security is someone else's job.
It is everyone's job not just the job of ICT

CareMIT Pty Ltd. Unit 3,116—118 Wollongong Street, Fyshwick, ACT ,2609. Email: directors@caremit.com.au Phone: 612 62577792

Understand your risks and mitigate them in the right way

Throw away all previously conceived ideas about risk and risk management.

Create a new list of risks not constrained by costs, capability or time.

Use that list to focus your mitigation requirements and start to reduce the risks with standard mitigation and control requirements

Awareness training starts at the start

Everyone needs to be aware of the issues associated with the digital realm.

Implement awareness training from the start, with everyone included and do it regularly (at least once a month)

Identify your crown jewels and protect them appropriately

You need to know what is your most important asset.

That can include people, reputation, intellectual property, information and property.

Once identified put in security requirements to protect it.

Use defence in depth

When it comes to security a single point of failure is to be avoided at all costs.

Use the combination of people, technology and process to ensure that all protective requirements have a fallback system in place.

Proactive not reactive

The worst place you can be is reacting to a cyber event without a trusted and tested plan.

The only way to have a trusted and tested plan to have thought about the situation and have contingencies in place to secure the organisation.

When it comes to plans, do not let the first failure be the test of the system—IT WILL FAIL.

Everything that is connected to the internet uses TLS security

Websites, cloud based systems, everything that is internet facing needs to b secured.

They need to be secured with your unique key.

Get one and use it, but also protect it well

Cloud based systems—where is your data

The implementation of cloud technology and cloud services has been embraced by every business in the world.

The questions to ask are—where is my data, who has access to it, does anyone else have access to it and who has sovereignty over it.

You need to measure your suppliers supply chain security

If someone else has a need to have access to my information you need to do your due diligence and understand a little bit about their business.

You are allowing others access to your systems and data—how much access are they going to have and what can they do with that access.

Implement security policies around your business

The best solution for policies is to ensure that the already in place business policies now include your required security.

Your team are already versed in you policy, adding to them ensured they will be followed and adhered to.

Trust no one

Trust has to be constantly check to ensure nothing untoward is happening.

Send people on leave, train everyone to do most jobs, swap people around—this way no one has the ability to cause issues

Social media—best friend / worst enemy—your choice

It is up to you what you and your organisation does on social media.

Make sure that no personal, staff related or intellectual property information is posted.

Please back it up

If you do not have a back up of all critical data you need to implement the 3,2,1 rule.

3 copies of all information, in 2 different location and one of those location has to be out of band and isolated.

Remote wipe capability

All devices and systems need to be able to have all information removed remotely

CareMIT Pty Ltd. Unit 3,116—118 Wollongong Street, Fyshwick, ACT ,2609. Email: directors@caremit.com.au Phone: 612 62577792