Roger's Cybersecurity check list

"The basics of business security" was a book I wrote 12 years ago and most of the information in it is still relevant.

Some of the information is outdated but the underlying principles that I discussed are still an integral part of an organisations ability to protect their critical assets

I also believe that the best way to protect an organisation is to be proactive.

This create contingencies and plans that allow an organisation to react in a specific, managed and understood way.

☐ Software patching and updates.

Patching and updates are the best and only way to ensure that the cybercriminal will not gain the all important foot hold of a cyber attack.

Operating systems and applications all have an update system. Apply the updates in a timely manner

☐ Remove old software and operating systems.

There is an underlying human reaction to digital components and that is that if they are still working then you do not need to replace them.

Anything in the digital world that is consumer based is obsolete after 4 years and a business network should never have

☐ Back up and test it all.

Use the 3,2,1 rule. Three copies of all data and systems, in two different locations and one of those locations has to be off site and disconnected from the system. Includes cloud based data. Regularly restore.

☐ Encryption.

All data that is under your control needs to be encrypted in some way. Websites have TLS certificates and backups are encrypted using the similar systems. Cloud based systems should be using your certificates not the vendors.

☐ 2FA and multi factor authentication.

Use multi factor authentication especially for all cloud based systems. Multi factor authentication relies on username, password and some other input from the person.

☐ End points

All end points (computers, smart devices and cloud based systems) should have some level of protection as an initial indicator that something is wrong.

☐ Firewall

That firewall that you were given when you joined an ISP is not protecting your organisation. A second generation firewall is needed in todays business world.

☐ Passwords

All passwords need to be unique, complex and more than 12 characters. Get a password manager and check you password on sites like https://haveibeenpwned.com/

☐ Email filtering

Cloud based systems have a rudimentary scanning system in place but because most cyber attacks come through email it is a good idea to invest in better protection at that level. Gmail and office 365 have a paid additional capability.

☐ Awareness training

Your troops, your team are the vanguard of your organisation. Invest in educating them in the cybersecurity space with awareness training. Not a set and forget process I recommend that there is something done every month.

☐ Additional policies, process, procedures and plans

Disaster Recovery, Business continuity, resilience and the 2 people rule for accounts are all ways that can be utilised to increase security around the organisation. Use sparingly, get everyone on board as why they are needed and then get sign off from everyone involved including management.

☐ Other requirements

To be truly secure you need additional systems including access management, log management, forensic capabilities, threat management and intrusion detection capabilities.

This checklist is just to take you from the truly vulnerable to a little higher up the security ladder.

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