Ransomware—You have to do something about it!

Any cyberattack will cause any business (micro to multinational) monumental issues but a random ransomware attack, if not considered will cripple your business.

If you think "we are too small to be a target", "we have nothing worth stealing" or "it will not happen to me" then you are in for a world of hurt.

A ransomware attack can be greatly reduced if you implement the following Before, During and After plan.

Before a ransomware attack

Backup: Identify all critical data and then apply the 3,2,1 Rule. ☐

Three copies of all data (original working data, on site backup and off site backup) in two different locations (on site / off site) and one of those locations is off site and out of band (disconnected from the system).

Use a backup system that encrypts your data for your protection and gives report on success and failure.

Restore: Regularly do a test restore from both onsite and off site backup system. ☐

Do it at least once a month.

Run table top exercises and scenarios with a facilitator that proves that the plans and system will work in a cyber event but also so everyone knows what to do.

Risk management: Understand and identify your digital risks and mitigate them appropriately ☐

Essential 8: implement the essential 8 cybersecurity strategies. ☐

- ⇒ Patch operating systems
- ⇒ Patch applications
- ⇒ Remove unnecessary administrators and the ones that remain do not have an email account
- ⇒ Implement 2 factor authentication (especially for all cloud based systems)
- ⇒ Manage Macros and scripting correctly
- ⇒ Do backups (see above)
- ⇒ Remove all unnecessary software and
- ⇒ Use a white list for applications and websites.

Install a proper firewall: The router / firewall that came from your internet provider or you purchased from a box store no longer has the capability and security required to secure your business and its connection to the internet. ☐

Invest in a second generation firewall and get someone to install it correctly.

Implement End Point Protection: Install anti Virus on all computers and smart devices. ☐

Do not use end point protection that does not have a management console and reporting capability.

Awareness and education training: Old adage "your staff can be your biggest issue or your greatest asset". ☐

Your choice but the difference, teaching them about cybersecurity and what to look for or not know, is important.

CARE MANAGED IT

CareMIT Pty Ltd. Unit 3, 116—118 Wollongong Street, Fyshwick, ACT 2609. Phone:- 0262577792 Email:-directors@caremit.com.au

Before a ransomware attack (continued)

Get your "what if..." team together: In the immediate panic of a cyber attack you will need people that you can trust. ☐

They also need to know what they are doing and are willing to help in resolving a ransomware attack, including negotiation of the ransom, if required otherwise your problems will be compounded.

Cultivate the right connections before it happens and when it does happen, you have your Cavalry ready!

Plans and processes: Most organisations already have a number of plans, processes, procedures, policies and standards. ☐

Make sure all users understand them and are following them.

Proactive and contingencies: The before component in a ransomware attack is all about being a scout—being prepared. ☐

If you have thought about how a ransomware attack could impact your organisations then you are already better prepared.

During a ransomware attack—Do's and Don'ts

Don't search the internet for a solution: The perpetrators of the ransomware are just waiting for you to do something silly like search for a solution.

The criminals know you will search the internet for a solution and have already set up thousands of websites waiting for you to make your issue bigger.

Do initiate and enact your plans and procedures (incident response/breach): Now is the time to reach into your filing cabinet (yes you need a hard copy because all of your files are now encrypted) and slap that plan on the table and say. "Lets do this the same way we have done it in all of the exercises".

Do implement your incidence response plan: Your tested and improved incidence response, breach, disaster recovery and business continuity plans are now enacted.

Follow your plans and checklists, they have been proven to work during all of those scenarios.

Do call in your cavalry: Your trusted resources are now needed. Get them in NOW.

After a ransomware attack

Have we got forensic capabilities: If you have then great, do a forensics investigation.

If not, then see the next point.

All systems that were infected need to be rebuilt—not just cleaned: The big hairy payload from a ransomware attack is the malware that encrypts your data.

The little known result is residual unknown malware that could become an advanced persistent threat and repeat the whole thing again.

Want to know more and get some help with building a secure business environment?

We have three free resources that anyone can use to see where they stand in the security of their organisation:

1. Free business security scorecard—complete the simple 48 questions and get a diagnostic report in your inbox based on your answers (**https://caremit.scoreapp.com**)
2. Free 60 minute webinar—a free webinar we run every Friday at 1030. Find out what you need to do to protect your organisation. (**https://www.eventbrite.com.au/o/roger-smith-7580793679**)
3. Free 30 discovery session— This is all about you. Bring your concerns, problems and issues and we will give you some advice on where you need to focus your resources. Book here (**https://caremit.com.au/30_minute_discovery_program/**)

CareMIT Pty Ltd. Unit 3, 116—118 Wollongong Street, Fyshwick, ACT 2609. Phone:- 0262577792 Email:-directors@caremit.com.au