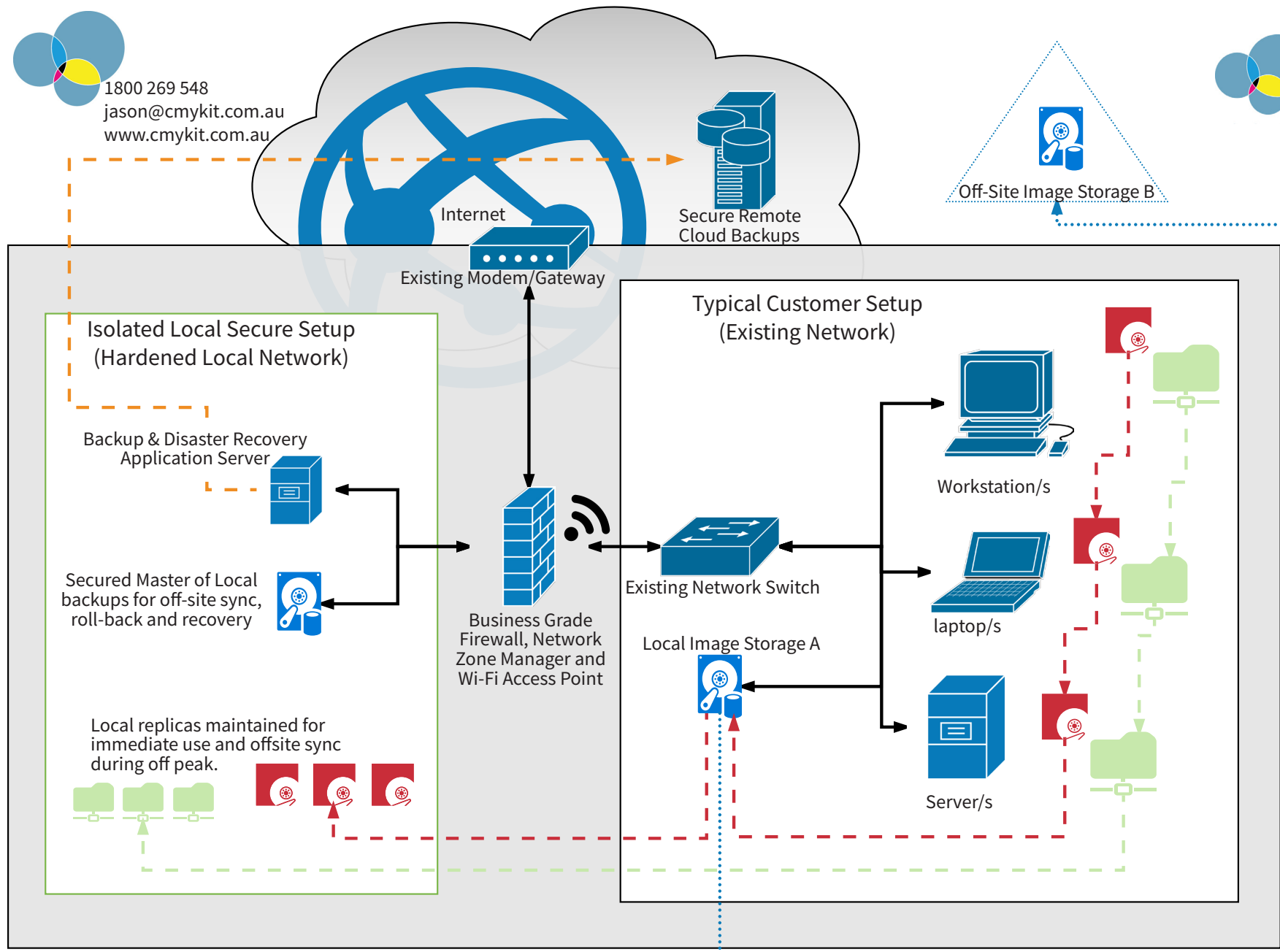


1800 269 548  
 jason@cmykit.com.au  
 www.cmykit.com.au



SME CyberSecurity that provides *peace of mind, convenience and value for money.*

The CMYKit BDR solution has been specifically designed to be a *flexible, affordable and managed solution to a complex and evolving problem.*

*Effective* defense is achievable with a clever *combination* of hardware, software, configuration and maintenance.

In combination we *custom build* you a:  
**Proactively Maintained and Monitored, High Availability, OnSite / OffSite, Disaster Recovery & Backup Solution;**

**Secure WiFi Protected zones = INSURANCE and ASSURANCE!**

Data and Files stored in Folders available on network either locally stored on workstations, shared from servers or other network attached storage.

A complete image of the Operating System, Programs, Folders, Files and Data taken at a specific moment in time. A known good "restore-point".

A File and Data Storage Point. Either portable for swapping out off-site backups or local RAID (hardware failure protected backup storage).

--- Dashed lines show logical connections, solid lines represent physical connections

## > **CMYKit provide the latest combination of technologies and techniques to fight CyberAttacks**

CMYKit handles cybersecurity breaches of all kinds for our clients on a daily basis. The headlines of the 'WannaCry' ransomware though have been a global wake-up call.

We have been providing the latest technologies in defense against malicious software (malware) including viruses, worms, ransomware and intrusion for years.

We regularly remind our valued clients of the importance of having more than an ad-hoc approach to the several important aspects of defending their vital commercial data. In fact a strategy that includes carefully thinking about what would happen if a disaster or compromise occurred that made local backups unusable. This could be ransomware or a building fire.

**>Often, small businesses believe they are too small, too insignificant to be targeted by organised criminal cyberattacks.**

**>Nothing could be further from the truth.**

Small and medium sized enterprises hold confidential and commercially sensitive data on behalf of their clients and vendors, as well as financial and accounting records that are very valuable to cybercriminals. Not only that, but they are perceived (usually correctly) as "soft targets" because of this very attitude and the lack of resources, planning and investment in a robust, comprehensive cybersecurity solution. They have relatively *much more at stake* too.

Worse still, the recent worldwide news stories about massive ransomware infections of computers show that criminals can indiscriminately launch attacks that have no interest in the data they hijack other than to extort the person to whom it is invaluable.

Ransoms, even if paid, do not always result in restoring the data that has been locked. Furthermore, paying a ransom frequently leads to further attacks as a dangerous precedent has been set.

If ransomware is able to access and compromise local backups (and there is no other off-site/ remote and effectively protected instance of the files) there may be no possible way to get it back, other than to hope that by paying the ransom the key to unlock it will indeed be provided.

The ransom is typically in an anonymous currency like Bitcoin and an amount that is attractive enough to compell anyone facing complete loss of their documents, images and other data to pay it. Recent, highly publicised ransoms, have been 1.5BTC which is currently over \$3,000AUD! Add to this the costs of downtime and reputation damage even if the data is restored and the obvious solution is to take every practical measure to prevent such an incident!

**> Speak to us now, before your current systems are tested by state-of-the-art cyberthreats.  
> The threat is real and only a click away! So is the solution - call or email CMYKit today!**

**> The solution shown on the other side of this page is an example of a solution designed for SMEs by CMYKit.**

We have been aware of the changing nature of malware and increasing ineffectiveness of conventional Anti-Virus Products and the firewalls provided in standard commercial operating systems, modems and routers.

You might think you're protected but if they can get into your mailboxes they are only an ill-chosen click away from extorting you.

Even these solutions need to be updated, managed and correctly configured if an incident isn't to turn into a major disruption to your business, or worse.

Therefore a comprehensive design for SME Cyber-Security is what we now strongly urge our clients to deploy and allow us to manage it in a proactive and best-practice way.

This solution is tailored to your business needs, the size of your network, amount of data you store and need immediate access to in order to carry out your business.

**The main features are:**

- **Business Continuity Protection**
- **Comprehensive Malware Protection**
- **High Availability of Files and Data**
- **Protected Roll-Back of File**
- **Local and Remote Disaster Recovery**
- **Local and Remote Compressed Backups**
- **The Insurance & Assurance you need.**