The Quick Business Security Checklist

	Item	Done	To Be Done	Date to do	Comment
1	**Have you done the basics?**				
	Created a password policy				
	Anti- virus, anti-spyware and anti-malware applications installed on all applicable systems				
	Are they Updated regularly				
	All systems are updated and patched regularly				
	Changed all of your default access to firewalls, switches, modems and applications				
2	**Have you identified all of the risks within your business?**				
	Have you done a risk analysis on the business				
	Have all discovered risks been mitigated against the business				
3	**Have you created a disaster recovery plan?**				
	Do you have onsite and off site backups				
	Is someone nominated to look after this				
	Do you have a written DR plan				
	Does it include all locations where your critical data is - Onsite, off-site, cloud				
	Have management authorised the DR Plan				
	Has the DR Plan been Tested				
4	**Have you created a business continuity plan?**				
	Have all of the risks been factored into the continuity plan				
	Has the BC Plan been tested				
5	**Have you created a business resilience plan?**				
	Are you developing a resilient culture within your business				
	Is the culture driven by all members of the organisation.				
6	**Do you have systematic security training for all staff?**				
	Do you have security training for your staff				
	Do you keep management informed of upcomeing security problems				
7	**Are your mobile systems safe**				
	Do you have a secure pass phrase for your wireless				
	Is your office wireless on a separate network				
	do you have the highest encryption set on the wireless system				
	Do you have a Bring Your Own Device (BYOD) Policy				
	Has your VPN connection been set up correctly				
	Is your VPN using the latest encryption and autorisation possible				
	Do you ensure that all corporate data on BYOD is saved to the internal system				
	Do you use Remote Desktop Propocol (RDP) for external access				
8	**Lost and stolen hardware!**				
	Can you remote wipe all BYOD components				
	Is all data on external systems encrypted especially laptops				
	Are all settings on external equipment set to **not** remember passwords				

9	**Separate business from family!**				
	Do all systems accessing the corporate network have policies applied to them				
	Do you allow external access to the systems - email, RDP, internal website				
	Is the access secure				
10	**Privacy and security systems on access**				
	Has the payment gateway been checked and tested				
	Has the SSL certificate been applied to all locations that it needs to be - web site, mail, RDP				
11	**If you don't have then expertise on site get it from outsourcing, managed services, or professional support companies**				
	Do you need help or have you the technical expertice on staff				
	If you need help contact us and we will put someone in contact with you.				
	This is only a basic level check list for the security of small and medium business and not for profit organisations. A more indepth course and system will be available shortly.				
	The new system will build into a security framework that will allow a small and medium business and not for profit organisation to understand how, when, where and why the				
	protection of the business data, staff and customer information is critical to the the businesses profitability. There is also more information available on the website but you will				
	need to sign up for the newsletter to access it. Access is free and we will not SPAM you nor will we lend, sell or give away your address.				