RESOLVE DEFENCE

Cyber Response

Cyber-attacks are now very real in New Zealand. Being “that little country at the bottom of the world in the middle of the ocean” is no longer isolating us from these attacks.

Cyber incident investigation

Knowing exactly the nature of the cyber-attack on a business dictates the level of recovery response required, and who needs to be informed of this cyber breach, from various government departments, the privacy commission, various insurance companies, and lastly clients.

Identifying the method of the cybercriminal access and the activity they undertook once “inside” requires a very specialised IT forensic skill set, and trusted relationships with the Cyber Insurance / Cyber Response companies and assessors.

Resolve Defence have qualified IT Forensic Security personnel, with registered Private Investigation credentials who can analyse the breached services, identify the method of access and then investigate the level of infestation and possible identification of any extracted data.

Armed with all this information and working with your business’s Cyber Response / Cyber Insurance Companies, your business recovery process can proceed.

Contact Resolve Defence to discuss how we can assist you to build your **Cyber Incident Response** business plan now.

Why does the cyber-attacker care about my business?

Cybercrime is a billion-dollar business; over 90% of these cyber-attacks are about money. Cybercriminals having penetrated your business will look around for information to gauge the degree of ransom they can extort from you.

Ransoms can involve crypto locking all your data files, locking out all staff from working, causing lost revenue from data loss and business downtime, or data extraction of files that will cause embarrassment and harm the business’s reputation if released to public viewing.

Businesses that survive have a tested and documented action plan in place. Having pre-organised access to the right professional support organisations is essential, not only to assist in getting their business back online as soon as possible, but also identify exactly what the cyber incident did to their business systems.