Cyber Security is a Business Imperative

Risk Management is defined as the identification, evaluation and prioritisation of risks and the impact of unfortunate risks on the business.

Senior Executives (C Level, Board Directors, Owner/ Managers) need to be prepared to drive and visibly support their organisations develop and implement a robust cyber security program.

The misalignment between senior executives' expectations and reality of the IT's function ability to deliver results against them constitute one of the most prevalent cyber security dangers

The foundation of risk management is knowledge of the factors which may cause loss. *Cyber Security is no different.*

Information Technology (IT) systems are capable of providing businesses with numerous competitive advantages in today's world, in the way they enable business to engage with their customers to sell and support their products and services, those same IT systems need to be protected by a robust security program.

Unfortunately IT systems provide a number of different Threat Vectors, via Networks, Websites, Applications and Databases for the hackers to attack, so any security program needs to ensure that all these threat vectors are secure

The impact of a successful data breach can have a devastating effect on businesses for example:

- Loss of Revenue.
- Loss of Intellectual Property.
- Corruption/loss of critical digital information
- Brand Name Damage – loss of reputation
- Financial Penalties – under new government regulations (Notifiable Breaches xxxxxx) any organisation with a turnover of $3 million that experiences a data breach where personal information is lost or subject to unauthorised access or disclosure can face fines of up to $1.8 million.

Or Even resulting in the total collapse of a successful business.

According to a 2018 Telstra report **60% of Australian businesses were interrupted by a security breach in the last 12 months and a recent report and a report in the Gartner 2018 Cybersecurity report, 95% of CIO's interviewed expect cyber-threats to increase over the next 3 years.**

As data breaches become more and more common, businesses and their customers are becoming increasingly concerned about the loss of confidential and personnel information.

Due to the impact of a successful breach, decisions on "How to develop and Implement a Robust Security Program" *need to involve all the key stakeholders in the business*", not just IT management.

In relation to Cyber Security the IT manager's role is similar to a Risk Manager, they are the tactical advisors to the business for the practical tasks of identification and mitigation.

As with other key assets in your business you need to access and manage the risks to your Digital Information, a valuable asset to your business

Where to start – Similar to Risk Mitigation you need to identifiy vulnerabilities, evaluate, prioritise and remediate.

A simple way to establish a credible understanding of your Cyber Risk would be a Vulnerability Scan, with the option of an ongoing monitoring service.

The Vulnerability Assessment scans all digital assets, identifies ALL vulnerabilities and delivers a remediation report.

Each scan delivers a single Remediation Report – provides the ranking of the discovered risks and step by step recommendations to fix each risk.

A Vulnerability scan is an effective way for ALL organisations form SME's to Enterprise of identifying and fixing the vulnerabilities that could result in a successful cyber breach.