Essentials of a security policy

Cyber Fact sheet

Why it Matters

Every company that uses computers, email, the internet and software on a daily basis should have information security (IS) policies in place. It is important for employees to know what is expected and required of them when using the technology provided by their employer, and it is critical for a company to protect itself by having policies to govern areas such software and hardware inventory and data. With upcoming legislative changes around areas like data protection, you will need a policy to help you comply with your legal duties.

It's important to differentiate between an IT Security policy – which concerns itself largely with the technology in use in the business – and an information security policy - which addresses all the security risks associated with information flowing through and stored with the wider business. This includes how security risks are addressed with vital service providers and suppliers.

Key Takeaways

- You need an information security policy as part of your cyber risk management.

Getting the Basics Right

Policy - As with any business activity, in cyber security it's crucial to identify what must be done and who will do it. Overall responsibility should rest with a senior manager who has a broad view of all the risks and how to tackle them. The policy should cover responsibilities, technical and user requirements. An example is provided below.

Policy Scope – the policy should cover the systems, people and business processes that make up your business's information systems. This includes all executives, employees, contractual third parties and agents of the organisation who have access to your information systems. The policy should include the following:

1. Information will be protected against any unauthorized access;
2. Confidentiality of information will be assured;
3. Integrity of information will be maintained;
4. Availability of information for business processes will be maintained;
5. Legislative and regulatory requirements will met;
6. Business continuity plans will be developed, maintained and tested
7. Information security training will be available for all employees;
8. All actual or suspected information security breaches will be reported to appropriate manager.