

SME Information Security

As most Small to Medium sized Enterprises develop, time and budget is often not afforded to the security of business information. Take a moment to consider the following points and information:



- Are you in complete control of who gains access to your information?
- Would anyone outside your business be interested in information on your systems?
- Are you confident that your business information can only be accessed by people you want to access it?
- Does your business make regular backups of business information & store securely?
- Are you confident you comply with the IT and information standards, regulations & laws that apply to your business?
- Do you have a plan to minimise impact to business in the event of serious incident i.e. fire or malicious employee/adversary attack on your systems?
- Can you continue business as usual if you can't access your business information?

If any of our points concern you then we can advise & implement security

Our Security Services

Confidentiality

A key factor in maintaining confidentiality is to ensure information access mimics business process and authoritative arrangement.

Basic Examples:

- Server access granularly controlled through accounts
- Lock down on local ability to transfer information away
- Construction of coherent data storage structure
- Policy documentation with contractual usage terms
- Forced password policies
- Secure disposal of business data & equipment

Availability

Availability encompasses all factors relating to systems and business information being accessible to authorised persons.

Basic Examples:

- Backup of business information & systems
- Offsite recovery depositories
- Disaster recovery plans
- Recovery testing to ensure continuity
- Firewall & ISP security
- Physical security

Integrity

Integrity of systems and data is the objective that such resources be protected from unauthorised, unanticipated or unintentional modification/damage.

Basic Examples:

- Automated virus protection
- Automated malicious software protection
- System vulnerabilities patching
- Auditing system to enable accountability
- Documented security training & new employee packs
- Least access practice applied to information

Service Levels

Levels

- Ad hoc consultancy services
- Packaged solutions
- Contractual arrangements

Please call to discuss further

The information objectives of businesses should consistently be: confidentiality, integrity and availability . . .