

fact sheet

How do I manage my e-security when the service is outsourced?

Many small businesses choose to outsource their information technology requirements so they can concentrate on their main business objectives. This approach can be successfully extended to e-security, especially if an outside company is used to host your business website.

Outsourced e-security services are often referred to as secure managed services, and are usually provided for a fixed monthly fee. Secure managed services can also be an effective way of implementing technologies such as firewalls and anti-virus packages.

The main benefit of secure managed services is that small- and medium-sized companies do not need to invest heavily in e-security technologies or training. However, the business is still responsible for ensuring e-security is adequate. Any arrangement with a secure managed services provider should be based on a well-developed Service Level Agreement (SLA) that outlines the quality and type of service required and includes penalties for failure to deliver.

You should also make sure that you have an internal policy for overall business security, and that the secure managed services provided are consistent with these. The policies that have been developed must be clear, concise and effectively cover all relevant security issues. You should also review security policies on a regular basis, and discuss any concerns with your provider.

Staff education is also important. No matter how effective the service provided to you, it can be compromised if staff are not aware of security policies on issues such as creating and protecting passwords, sending email securely and carrying out transactions online.

Terms you should know

Outsourcing - Paying an outside company to provide services such as information technology management, rather than employing internal staff.

Firewalls - Software or hardware systems to protect PCs and networks from unauthorised access.

Viruses - Malicious pieces of computer code which make unauthorised changes to your PCs, causing them to malfunction or deleting data. They often distribute themselves via the Internet or email. Well-known recent examples include Melissa and the Love Bug. They can be prevented with anti-virus software.

Hackers - Someone who attempts to gain unauthorised access to a computer system, often for fraudulent purposes.