

With organisations of every size, from SMEs to global companies, moving to cloud-based services, there has been understandable concern about security. The potential in the cloud for exposure of sensitive and valuable information is at odds with legislation requiring organisations to know where information is stored and to demonstrate how it is protected.

However, there is potential for a silver lining. Cloud service providers who respond to these concerns intelligently can provide additional security controls rather than undermining the status quo. This is particularly true for SME cloud users. Where smaller organisations may have inadequate or insecure backups for example, a cloud-based backup service that incorporates strong encryption can ensure regular backups and provide assurance of confidentiality. Firms that outsource their email service can also benefit from a cloud provider's anti-spam and anti-virus facilities with little effort.

In addition, my experience (and that of many security experts) is that the majority of security breaches and data losses occur because of weaknesses in internal networks. Properly configured cloud services can reduce the risk of accidental exposure on corporate networks, but the emphasis must be on "properly configured". It remains essential to conduct a thorough review of the provider's security to ensure good governance. This means inspecting their information security policy and procedures against proven standards such as ISO 27001, and ensuring that the relevant controls are embedded in your contract and service level agreement.

Security providers are also moving to enhance the security of cloud offerings or use the cloud to offer enterprise-quality controls. For example, Sourcefire has a cloud-based intrusion prevention service using the Amazon Web Services cloud platform, which allows users to monitor network activity for malicious behaviour. WatchGuard's Reputation Enabled Defense provides SMEs with protection against malware, botnets and other web-based threats via a cloud-based reputation lookup that scores URLs as good, bad or unknown.

There is no doubt that cloud computing is still in its infancy and many offerings remain insecure or poorly documented. However, the extensive press coverage of security concerns about the cloud model is resulting in a response from providers who see a way to differentiate their offerings and add value to customers of all shapes and sizes. Security providers are also seeing a market opportunity to add cloud-based services to their traditional on-premise products, both to enhance the security of cloud services and to reach a new audience via their own cloud-based security solutions.

Peter Wood is CEO at First Base Technologies, an ethical hacking firm based in the UK, and a member of the ISACA conference committee. Peter founded First Base in 1989 and has hands-on technical involvement in the firm on a daily basis, working in areas as diverse as social engineering, network penetration testing and skills transfer. Peter is also a world-renowned speaker and security evangelist.

Peter Wood
peterw@firstbase.co.uk
www.firstbase.co.uk
www.white-hats.co.uk
www.peterwood.com