

To encrypt or not to encrypt?

IT Columnist, Rupert Kendrick, reports on a recent survey that highlights the inadequate approach that many law firms show towards encryption and looks at a proprietary solution

The fiasco involving the loss of confidential data by HMRC serves as sobering warning of the devastating consequences of handling data casually.

Encryption of e-mail has not been widely adopted by the legal profession. Despite the risks to which e-mail is exposed in the course of transmission, most law firms have been content to take the risk of interception by hackers.

With some justification, they point out that there is no universally applicable system that can conveniently be operated between sender and recipient, which is commercially viable. The system of PKI (Public Key Infrastructure) whereby public and private keys (algorithms) are exchanged and applied to encrypt and decrypt e-mail is generally only commercially viable for large corporate bodies and is not practical for smaller organisations.

Survey

Part of the problem also lies in the apparent failure of the profession to understand exactly what is meant by e-mail security. A recent survey threw up some worrying findings. A telephone survey was conducted by Strategy One to explore attitudes and behaviour towards email confidentiality among law firms and to determine awareness and usage of email security solutions.

It highlighted a widespread and mistaken belief that existing anti-virus and spam prevention solutions provide sufficient email protection and that, as a result, the possibility of interception was being overlooked.

The risk posed by an email security breach was further highlighted by a related survey finding indicating that although most respondents believe email is the least secure method of communication, more than half of a law firm's daily email traffic contains confidential information. Interestingly, 82% of respondents were aware that external emails pass through many places before reaching the intended recipient.

There appears to be a widespread misguided view that the most commonly used anti-virus and anti-spam systems also provide protection against interception. This is not the case.

The research indicates that despite the recommendations contained in the email security guidelines issued by the Law Society, fewer than 10% of UK law firms encrypt email.

Findings

Key findings included:

- on average, more than half the emails sent by law firms contain confidential information;
- email is considered the second least confidential way of communicating information;
- almost half thought that their existing software covered confidentiality, although on further questioning it emerged that well over 90% of these were mistaken in their belief. 20% didn't know whether or not their software covered email confidentiality.

The survey sample comprised of 201 partners and non-partners of law firms across the UK.

The importance of encryption is now high up on the agenda of most corporate bodies in the commercial sector because of the need for corporate governance. More specifically, there is now a more widespread awareness of the provisions of the Data Protection Act 1998 and particularly, one of the eight principles that requires data to be held securely.

This is not confined to data stored on organisations' systems. It includes any confidential data either stored or passing through a system. Therefore it catches confidential data contained in email or any attachments.

A brief examination of any electronic file will reveal that without realising it, a good deal of sensitive information is conveyed and it is transmitted without any form of encoding that will protect it from interference by a third party. This is almost like sending clients' communications on a postcard or in a letter placed inside an unsealed envelope – or even without an envelope!

Emerging solutions

Some are now emerging as potential solutions, but until the tipping point is reached whereby a preponderance of organisations are using the software, there will always be a large number of organisations who are outside the encryption 'loop'.

One solution has recently been developed for professional services firms, particularly for law firms, by Securecoms (www.securecoms.com).

Secure-mail provides a hub, which is placed between the customer's email server and the internet gateway which automatically and seamlessly encrypts emails between the user and other Secure-mail users.

Secure-mail:lite is for those without the Secure-mail hub (i.e. most private clients). A Securecoms user can invite them to download an application that enables them to encrypt and decrypt email communications between themselves and the Securecoms user.

Rupert Kendrick is a solicitor and director of Web4Law Ltd., a risk management consultancy, and he specialises in IT and Internet risk issues. He can be contacted by e-mail at Rupert@web4law.biz or visit www.web4law.biz

"This is substantially drawn from an article that first appeared in Property in Practice - the magazine of the Law Society Property Section (www.propertysection.org.uk)."