

Data Loss Prevention Software

November 2008

Over the past twelve months the news headlines have been dominated by stories of high profile data security breaches. No sector of the economy has been unaffected by the seemingly unstoppable torrent of bad news.

The consequences of the public interest in security breaches have been dramatic. Among others things, they include the May 2008 amendment of the Data Protection Act that gives the Information Commissioner the power to issue monetary penalties when organisations are found to have acted in breach of the Act. They also include the July 2008 public consultation on the introduction of new inspection and auditing powers for the Information Commissioner, led by the Ministry of Justice.

These events have also drawn attention to the need for organisations to implement "Privacy Enhancing Technologies" (PETs); these technologies are designed to help keep data safe.

There are many different kinds of PETs on the market, with encryption software, firewalls and anti-virus software being obvious examples. However, the market for PETs is much more extensive than these examples and a new form of PET, "Data Loss Prevention" (DLP) software, is starting to emerge as an important consideration for organisations with a mature approach to data security technology. Vendors such as RSA and Symantec are currently leading the way in the DLP field and it is highly likely that they will be joined by many other vendors over time.

What are PETs?

PETs is not a new concept; many academic and trade articles have been written about PETs over the years. It is also important to note that a formal consensus definition of PETs has yet to emerge. However, a common theme within current thinking about PETs is that these technologies are ones that help organisations comply with the data security provisions set out in law, such as the security principle within the Data Protection Act 1998.

In recent times the PETs agenda has been adopted by mainstream lawmakers and regulators. For example, in May 2007 the European Commission published a Communication addressed to the European Parliament and Council titled "on Promoting Data Protection by Privacy Enhancing Technologies (PETs)". This document, which calls upon IT companies to develop PETs, provides the following definition:

"There are a number of definitions of PETs used by the academic community and by pilot projects on this matter. For instance, according to the EC-funded PISA project, PET stands for a coherent system of ICT measures that protects privacy by eliminating or reducing personal data or by preventing unnecessary and/or undesired processing of personal data, all without losing the functionality of the information system. The use of PETs can help to design information and communication systems and services in a way that minimises the collection and use of personal data and facilitate compliance with data protection rules. The Commission in its First Report on the implementation of the Data Protection Directive considers that "...the use of appropriate technological measures is an essential complement to legal means and should be an integral part in any efforts to achieve a sufficient level of privacy protection...". The use of PETs should result in making breaches of certain data protection rules more difficult and/or helping to detect them."

The UK's Information Commissioner, in a Guidance Note published in 2007, gives this definition:

"The Information Commissioner considers that privacy enhancing technologies are not limited to tools that provide a degree of anonymity for individuals but they are also any technology that exists to protect or enhance an individual's privacy, including facilitating individuals' access to their rights under the Data Protection Act 1998."

The Dutch Ministry of the Interior, in a White Paper published in 2004, gives the following definition:

"Privacy Enhancing Technologies (PET) is a collection of information and communication technologies that strengthens the protection of individuals' private life in an information system by preventing unnecessary or unlawful processing of personal data or by offering tools and controls to enhance the individual's control over his/her personal data."

The clear affect of these definitions is that a PET is any technology that helps to protect a person's privacy, particularly by facilitating an organisation's compliance with the "data protection principles" within data protection legislation derived from the EU Data Protection Directive.

Regulation for PETs within the UK

The fact that the UK Information Commissioner has taken the trouble to issue guidance on PETs renders it hardly surprising that he has also adopted a PETs-based regulatory strategy. This is best evidenced by his November 2007 enforcement strategy for laptop computers and portable storage media, titled "Our Approach to Encryption". This strategy teaches the following:

"There have been a number of reports recently of laptop computers, containing personal information which have been stolen from vehicles, dwellings or left in inappropriate places without being protected adequately. The Information Commissioner has formed the view that in future, where such losses occur and where encryption software has not been used to protect the data, enforcement action will be pursued.

The ICO recommends that portable and mobile devices including magnetic media, used to store and transmit personal information, the loss of which could cause damage or distress to individuals, should be protected using approved encryption software which is designed to guard against the compromise of information.

Personal information, which is stored, transmitted or processed in information, communication and technical infrastructures, should also be managed and protected in accordance with the organisation's security policy and using best practice methodologies such as using the International Standard 27001.

Further information can be found at 27001-online.com.

There are a number of different commercial options available to protect stored information on mobile and static devices and in transmission, such as across the internet.

Encryption software uses a complex series of embedded mathematical algorithms to protect and encrypt information. This process hides the data and prevents any inadvertent access or unauthorised disclosure of information. Since encryption standards are always evolving, it is recommended that data controllers ensure that any solution which is

implemented, meets the current standard such as the recommended FIPS 140-2 standard or equivalent."

We can draw many conclusions from the Commissioner's approach to encryption, with an important one being that it is highly likely that the Commissioner will start to regulate for the absence of other PETs. As such, it is possible that the Commissioner will eventually regulate for DLP, once he becomes aware of how DLP can increase an organisation's security rating by a significant order of magnitude when compared to encryption technologies alone.

What is DLP?

As one of the technology analyst companies puts it, a DLP solution consists of "tools to prevent inadvertent or accidental leak or exposure of sensitive enterprise information using content inspection technologies". In general terms DLP software works as follows:

Sensitive information within a network is identified and marked as such. Use and access policies can be attached to this information.

Processing of sensitive information across the network is tracked.

- Where processing of sensitive information is in breach of policy, that processing is blocked.
- A person acting in breach of policy can be notified of their policy violation, as part of an educational programme.
- The data controller is informed of policy violations.

If all of this functionality is distilled down to its essence it will be appreciated that DLP keeps sensitive data within the network; sensitive data can only be moved from the network, whether by TCP/IP protocol or from an endpoint where that movement is in accordance with policy. Consequently, DLP software has the potential to eliminate many of the security risks that might otherwise lead to data loss.

Conclusion

Eventually DLP will be regarded as part of the de facto data security standard, in much the same way as encryption now is.

Contact



Stewart Room

t: +44 (0)20 7861 4850

e: stewart.room@ffw.com

Field Fisher Waterhouse LLP 35 Vine Street London EC3N 2AA
t. +44 (0)20 7861 4000 f. +44 (0)20 7488 0084 info@ffw.com www.ffw.com

This publication is not a substitute for detailed advice on specific transactions and should not be taken as providing legal advice on any of the topics discussed.

© Copyright Field Fisher Waterhouse LLP 2008. All rights reserved.

Field Fisher Waterhouse LLP is a limited liability partnership registered in England and Wales with registered number OC318472, which is regulated by the Solicitors Regulation Authority. A list of members and their professional qualifications is available for inspection at its registered office, 35 Vine Street London EC3N 2AA. We use the word "partner" to refer to a member of Field Fisher Waterhouse LLP, or an employee or consultant with equivalent standing and qualifications.

KPMG and the KPMG logo are registered trademarks of KPMG International, a Swiss cooperative.

Field Fisher Waterhouse LLP is an independent legal entity that is separate from KPMG International and KPMG member firms.