

Companies Fail to Take Precautions to Secure the Weakest Link in their Information Infrastructure - Paper **NewsPortal.com**

Recent well documented stories in the media have shown how easy it is to cause breaches in security by careless handling of paper documents. IT managers need to understand that not all attacks are malicious, and employees can inadvertently be involved in accidental data loss.

While millions of pounds have been spent by corporations on security networks to ensure that data entering and leaving cannot be accessed by anyone without permission, many companies still fail to take any precautions to secure perhaps the weakest link in their information infrastructure – paper.

With Chief Security Officers under increasing commercial and regulatory pressure to implement watertight data security systems to protect their businesses, Helen Berentzen, office solutions marketing manager at Ricoh, says that the focus should not only be on digital information. The potentially most embarrassing data, or compliance, breach could be paper-based.

Investing in firewalls and anti-virus software has become second nature for businesses to ensure that their sensitive information is not stolen and does not fall into the wrong hands. The same cannot be said for technologies that ensure the security of hard copy documents.

According to research by Info Trends, 30 per cent of business documents are still paper based yet the majority of companies are failing to ensure that they have taken adequate precautions to ensure that paper does not become the weakest link in their information and document management strategies.

Increased regulatory compliance and legislative requirements to protect data mean companies need to treat paper documents with the same degree of security attributed to digital data.

IT managers need to look at the threats and demand that their paper-based information is as secure as that contained on corporate networks. Complete document security cannot be achieved without considering paper documents. Technology already exists to achieve these standards without inconveniencing everyday life but before you can implement it you need to fully understand your needs.

When data is shared by many users across a network, new threats to security can arise continuously, simply as a result of human nature. Mistakes are made and information can be leaked simply by people accidentally looking in the wrong file on a network, or by printing out a document that is inadvertently picked up by someone else. What one person doesn't consider sensitive data, may become extremely sensitive in the hands of the wrong person.

These may sound obvious but what would be the impact on staff morale if, for example, details of the pay-roll or disciplinary proceedings were left lying around the printer, or if they were picked up by the wrong person in error? Alternatively, what

would be the impact on the business if your sales orders were typically received by fax and a large order comes in this way and is misplaced? The customer will never receive their goods, valuable business is lost and goodwill is put at risk.

When developing information and document management strategies it is important to consider the whole of the document lifecycle. The sensitivity of information – both internal and external - needs careful evaluation. All aspects from access control, scan, copy, print and even fax need to have clear guidelines within an organisation to ensure devices linked to the IT network cannot compromise information security.

Threats that organisations need to consider when looking at documents include:

- Document creation – who is opening and viewing soft copy documents; when are they being scanned and saved onto the network?
- Scan to email – without an audit trail it is impossible to monitor if someone has distributed confidential data to a wrongful destination, or to track who has received it?
- Unauthorised access to archived documents.
- Can documents be copied or viewed by passers by once printed?

How can these be resolved?

Each log-in point on the network, such as multifunctional devices (MFDs), printers, scanners, copiers and mobile devices, etc should require user access just like a PC. As part of a standard security programme IT managers can implement authentication solutions which require staff to input their log-in details and password before accessing these devices, just as they would to access their PC or the corporate network.

Smartcards ensure that access to MFDs is restricted and print jobs can only be released by the authorised users. This means that documents can only be scanned, emailed and faxed directly from these devices by staff members with authority to do so.

In more complex environments, the latest security technologies can provide up to four different layers of administration and supervisor rights for enterprises, including managing permission for machine default settings, network default settings, access to stored files and managed local address books.

As with any form of network traffic, unprotected print jobs are vulnerable when they transfer from the desktop to the output device, so it is now possible to encrypt this traffic in order to restrict the ability of hackers (internal or external) to access this data in transit. Other uses of encryption on an MFD include; data in the local address book, print job authentication and encrypted passwords when using PDF direct print functions.

With documents only being printed when the user actually goes to the device, the system has the benefit of reducing the environmental impact of energy and paper consumption. It stops people sending print jobs to the printer

and then not collecting them, saving paper and energy. If a print run isn't collected at the device within a pre-defined time period, then the device simply deletes the job from the queue.

Looking to the future

While smartcards and encryption technologies are already available to businesses, biometrics is fast becoming the next step in authentication with enterprise ready solutions. According to Matia Grossi, Frost & Sullivan's industry analyst, "the market for biometrics products is going to almost triple in value between 2008 and 2012."

This will address demand for an enhanced, secure identification and personal verification technology. Fingerprint technology is the most established way of doing this, with the main advantages being that it is the most economical biometric technology, its small form factor, reduced power requirements and resistive nature to temperature and background lighting. It also provides added convenience to the user who doesn't have to remember a user ID PIN and reduces the risk of lost cards.

This technology is being developed for a range of devices and will allow the release of documents only when an authorized fingerprint is read at the device, providing users with added security, control and convenience. Biometric applications will also eliminate the security and cost implications every time an authentication card is lost. This is an issue which has been highlighted in technology savvy schools that spend a small fortune replacing the authentication cards that students lose.

In the not so distant future this could be extended even further with devices having the ability to scan retinas or even DNA before releasing documents.

Realising the potential for abuse and security weaknesses isn't new, but building some or all of these security measures into an information security strategy will help ensure that paper-based information is as unlikely to fall into the wrong hands as its digital compatriot.