

IT Analysis – Securing the print environment

By Louella Fernandes, Principal Analyst, Quocirca Ltd

Corporate secrets and intellectual property falling into the wrong hands rank as one of the highest security breaches for any organisation. It is widely accepted that security threats are on the rise with identity theft, fraud, spyware, and phishing permeating cyberspace. Whilst many organisations go to great lengths to establish a security strategy to safeguard their network and intellectual property, the document production environment is often overlooked.

Multifunction products (MFPs) which print, copy, scan, fax and electronically store and transfer documents are integrated with the corporate network and therefore are an essential component in any organisation's security strategy. Today, MFPs play an integral part of document production in the office, managing vast amounts of data. MFPs have been a real asset to office productivity, offering advanced functionality at a lower operational cost, higher speed and quality than single function print devices.

However the downside to this is that security becomes a major issue. As well as the original problems of papers being left in out trays, under scanner lids or being inadvertently picked up by a third party, we have the electronic threats where image data has to be transferred to the device over the network and stored in memory. Non volatile memory such as flash ROM and hard disk drives are particularly at risk, as these components can be stolen or dumped with the residual data intact. Most importantly, the network connectivity of MFPs increases their exposure to hackers hijacking the image data. Documents are at risk not only on the hard disk, but also in transit to the print server.

But steps can be taken to secure the print environment. This starts with controlling access to both device and documents. Most vendors offer some form of user authentication which ensures that prints are only released on entry of a pin number. Enhanced secure printing also offers proximity or security card identification. Although this does introduce the risk that data is being stored on the printer's hard disk drive, many vendors address this by offering

encryption of the stored data which is erased after usage. The ability to send scanned data through the Internet raises other security concerns. This can be addressed through network authentication which offers an additional means of device control via the network, and is well suited to larger scale installations. This can prevent anonymous scan-to-email access, and some security solutions go further by mirroring a copy of the email for auditing purposes.

Protecting the image data from unauthorised access can be achieved via a number of solutions. MFPs that include 128bit SSL (Secure Sockets Layer) encryption provide added security as encrypted documents cannot easily be deciphered. Some MFPs also offer the ability to program the device with Media Access Control (MAC) addresses or IP filtering so that the device will only communicate with recognised computers specified by the IT department. Data overwrite functionality overwrites files stored on the hard disk following the completion of a print job. Most vendors offer this, but the functionality and charging model varies. Konica Minolta, for example, embeds hard disk overwrite functionality into the firmware of its bizhub devices, whilst other vendors offer this capability as a chargeable option. An additional way to protect hard drives is to use optional removable hard drives offered by most manufacturers which can be removed to prevent access to confidential or proprietary data. The removable hard disk is secured using a key lock system and can only be re-installed using a pass code.

Beyond controlling access and protecting data, an audit trail can be invaluable. Tracking and monitoring every page that is printed or copied is a requirement of certain regulatory regimes. Here manufacturers often offer a mix of proprietary and third party solutions for document accounting; Equitrac Office 4, for example, generates detailed activity reports for auditing purposes and integrates with the majority of MFPs on the market. Using such third party solutions can ensure a consistent approach to securing the document production in a multivendor environment.

Despite all this, the level of security certification for MFPs varies widely. Most manufacturers have obtained some level of National Information Assurance Partnership (NIAP) Common Criteria Certification (CCC). NIAP is a U.S. government initiative created to meet the security testing needs of IT consumers and companies. However the differing Evaluation Assurance Levels (EAL) can create confusion for any organisation assessing CCC for different vendor's MFP devices. Whilst Sharp has obtained an Evaluation Assurance Level Four (EAL4) rating for its AR-FR4/AR-FR-5 data security kit, Ricoh and Canon have achieved EAL3 certification and Xerox has EAL2 certification for its WorkCentre devices.

So is CCC a guarantee of the security capabilities of an MFP? CCC in fact does not stipulate the necessary security functionality, but provides a means to assess the accuracy of a particular security implementation as advertised by a manufacturer. Whilst higher EALs involve more detailed documentation, analysis and testing than lower ones, (and is also more costly), a product with a higher EAL certification is not necessarily more secure than one with a lower EAL. This is because to achieve a particular EAL products must meet specific "assurance requirements", but do not need to fulfil the same functional requirements - this is dependent on the Security Target document tailored for each product's evaluation. So whilst Xerox has certified its products at EAL2 level, it claims to be the only manufacturer to have certified complete products, rather than just kits of subsets of functionality. So, vitally, CCC does not represent what security features a MFP device may, or may not offer.

Due to the lack of a common industry approach, the IEEE p2600 working group is defining a security standard for hardcopy devices, as well as recommendations for security capabilities. The working group has broad industry participation. HP is notable in pursuing an alternative security checklist developed for the National Institute of Standards and Technologies (NIST). NIST is responsible for creating security guidance for the United States Federal Government and currently HP is the only listed MFP vendor with a security checklist.

The lack of security standards for MFP devices can create confusion for organisations in assessing their printing and imaging security requirements, particularly as many organisations operate in a multivendor environment. Quocirca recommends that organisations assess the capabilities of their printing and imaging devices in line with their security needs. Irrespective of security certifications, measures to ensure end-to-end document security need to be easy to implement. IT administrators do not want to be overloaded with additional administrative tasks, and end users must not find using secure print features impedes productivity.

About Quocirca

Quocirca is one of Europe's leading independent industry analyst firms. One of its biggest assets is the core team of highly experienced analysts drawn from both the corporate and the vendor communities. This team prides itself on maintaining a bigger picture view of what's going on in the IT and communications marketplaces. This allows all of Quocirca's activities to be carried out in the context of the real world and avoids distractions with fads, fashions and the nuts and bolts of specific technologies. Quocirca's focus has always been the point of intersection at which IT meets "the business".

Quocirca Services

The insight and experience that comes from working as an industry analyst as well as a practitioner allows the Quocirca team to contribute significantly to IT Vendors, Service Providers and Corporate clients. To this end, it provides a range of consulting and advisory services. Details of these, along with some of Quocirca's latest analysis, may be obtained by visiting <http://www.quocirca.com>

Quocirca's primary research involves the surveying of many thousands of technical and business end users each quarter, analyzing their perceptions of the possible impact of emerging, evolving and maturing technologies on their businesses.