Protect your data

Intellectual property (IP) is one of your company’s most valuable assets, yet it is transmitted daily across networks and devices that are vulnerable to unauthorised access. By Alison Job

Security printing is an industry term referring to the safe transfer of data specific to the output of that information. With a company’s IP flying across networks every day all day, it is the chief information officer’s job to ensure that it is kept secure. According to Andrew Griffith, product manager for office products at Konica Minolta South Africa, the transmission, storage and output of data need to be properly secured in order to minimise the threat of IP theft.

This threat is taken so seriously that there is an ISO standard that can be applied to devices that properly safeguard the information they process. Konica Minolta is one of very few companies worldwide to have attained the ISO EAL Level 3 grade for its multifunctional systems, which covers the transmission, storage and output of information. Griffith explains, ‘We’ve had this authentication for more than three years and believe that our systems are the most secure in the industry.’

Nowadays, all data is digital and IP theft is a very real possibility across all industries. In fact, data security is a huge industry in and of itself. ‘If you store your company information on one of our devices, the hard drive has an embedded firewall, requires a 20-digit alphanumeric password and the data is encrypted using a 128-bit algorithm, which can be upgraded to 256-bit algorithm should the customer require it. In addition, if the information is deleted, there is no residual ghost image on the hard drive,’ says Griffith, underlining his company’s commitment to keeping its customers IP secure at all stages during its transmission.

Obsolete office equipment is sold on with little thought about the data that could remain on a hard drive even after that information is deleted. This is of particular concern to government departments, for example. In South Africa, where identity theft is prevalent, there is much concern about what happens at a system’s end of life, what type of information can still be retrieved from that hard drive?

Another safeguard on Konica Minolta SA’s systems is PDF encryption, a standard feature on output devices. If the PDF is intercepted, the data can’t be seen. Griffith points out that companies are often lax on the document distribution side and don’t realise that this is where their IP is at its most vulnerable. This is especially true when it comes to education, where there is a need to protect the output, distribution and storage of examination papers. While the cyber crime statistics for South Africa are unknown, one only has to read the newspapers at the end of each year to find countless reports of leaked exam questions. Copy protection is also available, where if an unauthorised person gets hold of a piece of paper and tries to copy it, the machine recognises the document as secure and prints ‘invalid’ across the page.

On all Konica Minolta SA devices, the RAM is partitioned into volatile and non-volatile sections. Anything processed in the volatile RAM is deleted instantly if the machine is switched off, which prevents a user from accessing it illegally. They also feature user identification technology such as finger-vein biometric authentication, where an infra-red scan detects unique finger vein impressions. ‘This is the most secure authentication method available today,’ says Griffith. ‘There are several installations in South Africa, including one of the country’s leading financial institutions.’

‘This level of security is increasingly becoming a factor when making a purchasing decision and we encourage our customers to go this route sooner rather than later,’ emphasises Griffith. ‘Cyber crime happens every day, the business world is a highly competitive environment and every time data is transmitted across a fibre optic cable it is at risk. It’s our job to help our customers minimise that risk!’