

How safe is
your Corporate
Information?



June 2008

www.williamslea.com



For all modern corporations, whether in the banking, telecoms or legal sector, Corporate Information has become one of the most important intangible assets – and one of the most at risk. Michael Vorel, Chief Technology Architect at Williams Lea, explores the latest trends in hard disk drive security and considers how safe information is in today's corporate world?

Background

Information security has become an increasingly hot topic for businesses and consumers alike, after a rising number of scare stories about corporate data loss and consumer identity theft. The information we store on hard drives at home and work or on mobile devices such as Blackberries and flash storage devices, can give away vital and sensitive details about who we are as an individual or an organisation.

Corporate Information

Corporate Information can contain highly sensitive data about customers and employees, corporate strategy and financial strength, patent applications and even litigation. Highly secret information about corporate strategy, deals and disputes is now at risk of being captured or duplicated indiscriminately thanks to the growth of digital copy and communication equipment present throughout every business. So why is it that so many companies are still struggling with information security and what are the latest products that can help minimise the risks involved when storing commercially sensitive documents and files?

When it comes to looking after the future of a business, protecting intellectual property, technical data and customer information is paramount. The only thing that has matched the burgeoning growth of Corporate Information is the increasing number of ways in which it can be lost. Personal information and bank details have been lost repeatedly when disks have been misplaced or sent to the wrong address. Laptop computers containing gigabytes of unencrypted personal and corporate information have been lost or stolen on numerous occasions, and recently HSBC lost an entire server containing the address details of hundreds of thousands of its Hong Kong customers.

But these are just the cases we hear about, in part thanks to legislation adopted by a growing number of US states and EU countries to force companies and governments to tell the public when they lose data. Far less visibly, the growth of multifunctional devices (MFDs) offering copying, faxing and scanning throughout

Many of the world's leading multifunctional device manufacturers have taken significant steps to boost hard drive security.

offices around the world has resulted in a hidden epidemic of unsecured and duplicated information. The lack of security on these devices has resulted in the "worst of times" for businesses around the world.

Until recently, information copied, faxed or printed from these devices would reside on the device's hard drive disk (HDD) until it was over written or removed. This meant that most of the data remained non-secure, vulnerable and open to theft or manipulation. Such non-secure information is accessible to people within an organisation who should not have access to it, making Corporate Information vulnerable to espionage from something as simple as a routine maintenance check. While there is little hard evidence to back it up, there are anecdotal tales of technicians contracted to repair equipment replacing a functional hard drive and selling the unit on the street.

Is Corporate Information really secure?

Corporate Information stored on hard drives is not as secure as company bosses would like to think, and with the type of data stored ranging from audit and employee details to highly confidential merger and acquisition information, they could be leaving themselves open to future legal actions, as the laws surrounding information storage, transfer and dissemination are tightened.

To protect customers from these vulnerabilities, many of the world's leading MFD manufacturers such as Sharp, Canon, Xerox and Ricoh have all taken significant steps to boost hard drive security, but the first steps towards standardisation were taken twenty or more years ago.

Standardization

Throughout the 1980s, various standards emerged, until in 1990, the International Organization for Standardization began to develop a set of international standard evaluation criteria for general use. These new criteria resulted in a standard security evaluation across the global IT market, establishing a "Common Criteria". This has now been adopted by 14 nations and is recognised worldwide as the primary measurement for IT security. It is partly as a result of this regulation that there are the advanced security options in place on the more advanced MFDs used by companies around the world.

In today's corporate environment, the need for standards has grown in line with the explosion in the number of MFDs, mobile devices and flash drives in the market. The problems faced have been enhanced by the blurring of the boundaries between home and work brought about by flexible working.

The emergence of super-databases of interconnected and duplicated information shared between doctors, lawyers, shops, banks and credit card companies, and employers, not to mention credit, security, immigration, police and government

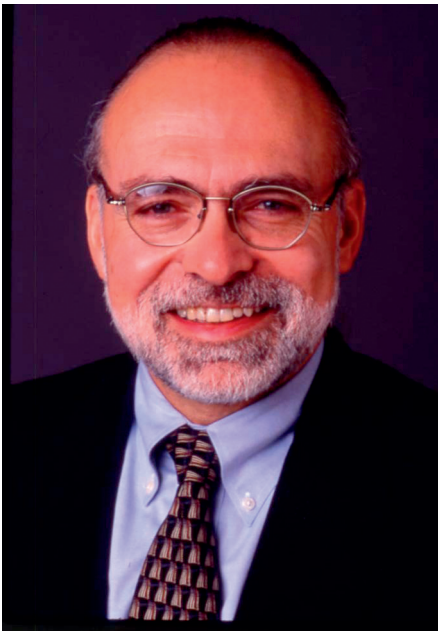


International Organization for Standardization is responsible for the ISO 9000, ISO 14000, ISO 27000, ISO 22000 and other international management standards. www.iso.org

agencies, has meant protecting Corporate Information has become hugely complex multi-agency task. For all the benefits brought about by the interoperation of devices and web-based data transfer, they have come at the expense of information security.

On multifunctional and mobile devices, simple but essential measures such as password security and enabling protocols have enhanced network security protecting information from sophisticated hackers. In addition, some of the latest MFDs come with image-overwrite technology, useful for research and development (R&D) departments and businesses working with high volumes of secure information such as financial services companies and many business process outsourcing organisations.

As with most major business issues, prevention is better than cure. As Corporate Information has become at once highly valuable and at ever increased risk of loss or mismanagement, most information-rich companies have elected to work with experts to ensure they have given consideration to the risks they face. In many cases, risk management raises potential savings through better information performance, reducing duplication, improving access by authorised personnel, and reducing information at risk.



Michael Vorel is Chief Technology Architect at Williams Lea, working with many of the world's leading banking, legal, retail and telecoms organisations to improve information performance and security.

Confidentiality Statement

The contents of this document together with all other information, data, materials, specifications or other related documents provided by Williams Lea ("WL") (together "materials") shall be treated at all times by the recipient as the confidential and proprietary information of WL. The recipient shall not disclose any such materials to any third parties without the express, prior written approval of WL. Where such express approval is granted by WL, the recipient shall ensure that all third parties to whom disclosure is made shall keep any such materials confidential and shall not disclose them or any part of them to any other person. All intellectual property rights in the materials shall remain the property of WL, or its third party licensors, and are protected by copyright. © 2008 Williams Lea Group

Disclaimer

This document may be incomplete without reference to any oral briefing provided by WL, reflects current conditions and WL's views as of this date and is subject to correction or change at any time. Although the information contained in this document is believed to be accurate in all material respects, neither WL nor any of WL's advisers, agents, officers or employees accepts responsibility or liability for or makes any promise, representation, statement or expression of opinion or warranty, express or implied, with respect to the accuracy or completeness of the content of this document (to the extent permissible by law) unless and save to the extent that such promise, representation, statement or expression of opinion or warranty is later expressly incorporated into a legally binding contract.