

Finding a Balance between Security and Convenience

Financial institutions cannot exist without customer trust, and as identity theft becomes increasingly common, clearly customer trust cannot exist without rock-solid data security. Although technological advances such as remote account access provide customers with real-time services not previously available, extending the network beyond the confines of the office has made it increasingly difficult for IT departments to protect company/customer information stored on computer hard drives (“data at rest”).

With the Computer Security Institute (CSI) and Federal Bureau of Investigation (FBI) 2006 Computer Crime and Security Survey stating that 52 percent of the 313 organizations surveyed had experienced unauthorized access to company data in the previous year, it is hardly surprising that customer trust is increasingly linked to data security.

Worldwide regulations, including the Personal Information Protection and Electronic Documents Act, the European Union Privacy Directive, and Sarbanes-Oxley attempt to drive strong data security adoption. Security breaches must be disclosed, and penalties include fines and/or criminal/civil action. But, the severity of these penalties is inconsequential when compared to the negative impact bad publicity can have on customer trust and company profits.

In a recent example, Ameriprise Financial Inc., made an agreement with the Commonwealth of Massachusetts to hire a consultant to review its laptop policies after the embarrassing theft of one of its computers exposed the personal data of more than 150,000 clients. Although the laptop was recovered without undue harm resulting from the data breach, Ameriprise agreed to pay \$25,000 to the state of Massachusetts to cover the cost of an investigation.

Most regulations, such as California Senate Bill 1386, acknowledge that data is only secure if encrypted. So, if encryption is the best method of protecting “data at rest”, why is it not installed on every device? The simple answer is that increased security usually negates the right-now convenience of today’s online financial services. That means the ideal solution must encrypt all data without inconveniencing administrators or customers.

WinMagic’s SecureDoc full-disk encryption exactly meets these requirements. SecureDoc provides the strong data security required by encrypting all data on the entire drive, including often-unprotected temp, paging, clear text, and hibernation files. SecureDoc’s preboot design also makes it simple to integrate encryption with multi-factor authentication, such as smart cards, tokens, biometric devices, and PKI authentication technologies before the operating system brings up the logon screen – ensuring data cannot be accessed via a lost or stolen device, or via a retired hard drive.

User- and administrator-friendly, SecureDoc encrypts the entire hard drive automatically so as not to burden users with encrypting files individually. In fact, a SecureDoc-protected disk acts exactly as it did before encryption – eliminating the help-desk costs associated with installing new software. Administrators are further assisted by the fact that SecureDoc encrypts a hard drive faster than any other solution, and does not require bad sectors to be fixed or defragmentation of the drive before installation.

By enabling banks to supply the remote, real-time services customers want without compromising the data protection customers need, SecureDoc provides the rock-solid security necessary to foster the customer trust on which banks are built. A SecureDoc/financial industry case study is available at <http://www.winmagic.com/cuinfosecurity>.



Joseph Belsanti
Director of Marketing

Joseph Belsanti is Director of Marketing at WinMagic and is responsible for developing marketing strategy, including public relations, analyst relations, and corporate positioning for WinMagic’s SecureDoc full-disk encryption product suite. Belsanti’s career includes a solid background in direct and channels sales having sold software and hardware solutions in Canada, the United States and South East Asia. Belsanti has worked with influential organizations affecting enterprise applications including Pitney Bowes, Hewlett-Packard (Canada) Co., Hummingbird Communications, and Xerox. In past roles, he has held various progressive sales and marketing leadership roles in the fields of E-services, software connectivity solutions, IT hardware products and test and measurement equipment.



WINMAGIC
DATA SECURITY

Contact Info:

<http://www.winmagic.com>