

*SMBs Face the Same
Regulations as Large Enterprises
for Data Protection*



SMBs Realize Significant Costs Savings and Superior Security with Self-Encrypting Drives (SEDs)

To better compete in a global economy, small and medium-sized businesses (SMBs) are incorporating mobile technologies — like laptop computers — across their organizations. While those technologies improve productivity and lower IT costs, storing more sensitive data off secure networks also increases the risk of accidental and intentional data loss.

SMBs are stewards of their customers' sensitive financial, health and personal data, all of which are prime targets of identity theft and other cyber crimes — despite many SMB owners' misconception that they are too small for thieves to notice. In January 2011, a National Retail Federation (NRF) survey found that more than one million small businesses nationwide had been victims of data-breach related fraud in 2010.¹ The most common type of fraud was from cyber attacks on stored data. Those breaches can be devastating. Other recent research found the average cost of a lost or stolen record is \$214. Further, this study revealed, organizations on average lost approximately 16,000 records from a data breach. This translates to a cost of about \$3.4 million for each incident.²

Growing political, public and industry pressure have strengthened commercial and government requirements to notify breach victims and regulators. SMBs must comply with these regulations just as enterprises do — even though SMBs lack equivalent IT security expertise and financial and personnel resources to implement it. Nonetheless, they face the same negative public reaction, government and commercial scrutiny, lawsuits and hefty fines. When even one breach — whether by loss, theft or cyber attack on a laptop — could spell disaster or even bankruptcy, SMBs must mitigate the chances as much as possible.

Three key-related challenges are listed at the right:

Key SMB Data Breach Mitigation Challenges

State Regulatory Compliance

Forty-six states and the District of Columbia have data breach notification laws mandating public disclosure of breaches that may compromise customers' personal information. Two states, Massachusetts and Nevada, mandate encryption of sensitive data.

Federal and Commercial Regulatory Compliance

Federal regulations include the Graham-Leach-Bliley Act (GLBA) and the Health Information Portability and Accountability Act (HIPAA). Commercial regulations, especially the Payment Card Industry Data Security Standard (PCI DSS), also carry great weight. Failure to comply with PCI can forbid violators from performing online credit card transactions, which can severely damage both profitability and customer trust.

Bigger Needs, Smaller Budgets

Increased use of mobile technology has exacerbated the need for secure laptop storage but SMBs' IT budgets remain extremely tight. To safeguard their data, SMBs need proven protection that meets government and commercial standards, works across platforms and has known acquisition and operational costs. Automated, low-cost IT solutions are ideal because they enable SMBs to focus their limited resources on doing business, not protecting it.

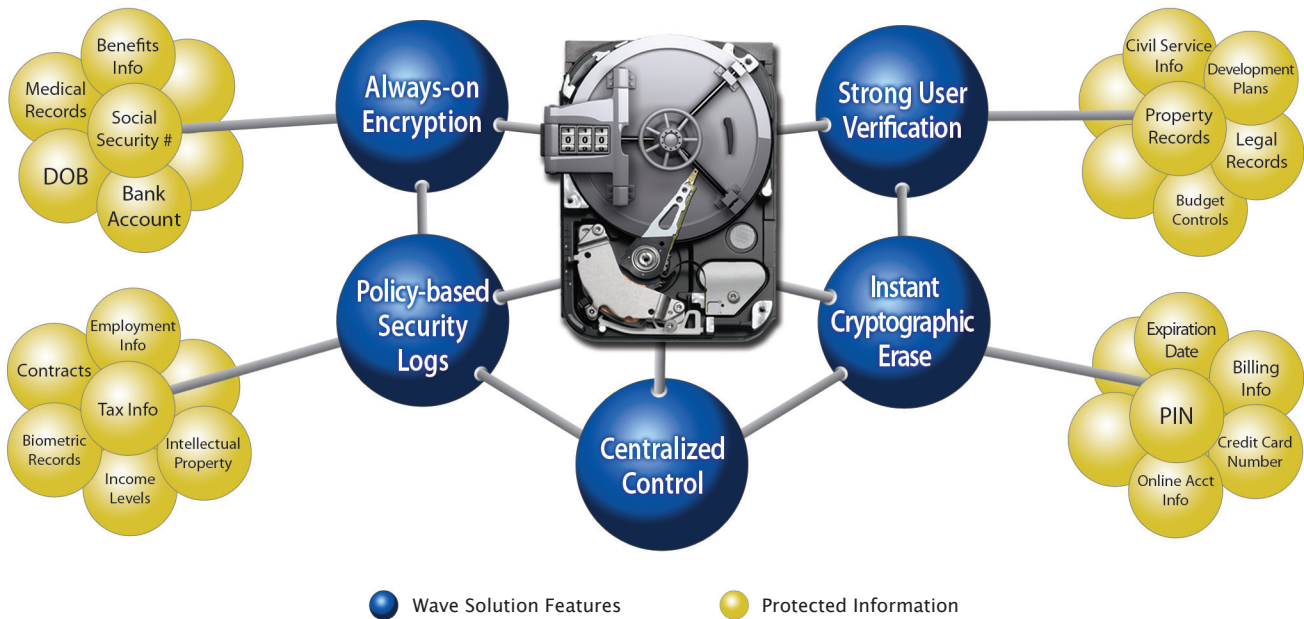
Self-Encrypting Drives and Wave's EMBASSY® Software Protect SMB Data

Options abound for protecting sensitive data but many experts consider full-disk encryption (FDE) the best because it encrypts everything on a hard drive, eliminating many vulnerabilities attackers can exploit to gain unauthorized access to data. Unfortunately, software-based FDE, the most common form of FDE, has exploitable weaknesses, meaning it can't guarantee that lost data is unreadable. This fact leaves SMBs at continued risk of costly and catastrophic breaches.

To overcome these hurdles and comply with regulations, more SMBs are turning to SEDs. SEDs offer an alternative hardware-based FDE approach, making them more secure and less expensive to implement and maintain. SEDs house all encryption processes and keys in a protected hardware boundary impervious to traditional software attacks. Further, they cost only slightly more than unencrypted hard drives, need little IT overhead and are transparent to end users.

Wave Systems, a pioneer in hardware-based laptop security, has partnered with leading hard drive manufacturers Hitachi, Samsung and Seagate to provide enterprise security management for their SEDs. Through partnerships with Seagate, Data Management, Inc. and other trusted IT providers, Wave serves a growing number of SMB customers.

SEDs are a proven IT security solution; for instance, Seagate has shipped more than one million SEDs, many of which use Wave's EMBASSY software.³ Further, given the status of computer equipment manufacturers Gartner believes that, within five years, all hard disk drives (HDD) will be shipped pre-loaded with some kind of industry-standard FDE technology. EMBASSY transforms SEDs into a complete managed enterprise encryption solution: one that centrally provisions security policies limits access to only authorized users and — perhaps, most importantly — proves whether or not sensitive information stored on a laptop was encrypted at the time it went missing.



¹ "First Data and NRF Release Results of SMB Data Security Study," Press Release, First Data Corporation, Jan 12, 2011 http://www.firstdata.com/en_us/about-first-data/media/press-releases/01_12_11

² 2009 Annual Study: U.S. Cost of a Data Breach, The Ponemon Institute, January 2010

³ Press release, Seagate, 2/14/11 http://www.wave.com/news/press_archive/11/110214_RSA_Announcement-Seagate.pdf