



*Does Your State,  
County or City Encrypt  
Its Data Effectively?*

## Helping State and Local Governments Keep Sensitive Data Safe

To better succeed at their missions, state and local governments are incorporating enterprise applications and mobile technologies — especially laptops — across their organizations. While those technologies help improve services and productivity and lower taxpayer costs, storing an ever-growing amount of sensitive agency data on mobile devices also increases the risk of accidental and intentional data loss.

Data breaches can hurt not just state and local governments but thousands, or even millions, of the people they serve. Recent research<sup>1</sup> found that U.S. data breaches averaged \$7 million apiece and over \$200 per compromised data record — meaning state and local government data breaches can quickly reach budget-busting costs. Additionally, lost or stolen laptops accounted for more than one-third of data breaches in 2009, making securing information on these devices an essential element of these governments' security and compliance strategies.

Protecting themselves from data breaches and cyber attacks has thus become a critical priority for both state and local governments and their partners. Four key related challenges are listed at the right:

### Key State and Local Data Breach Mitigation Challenges

#### IT Security

All state governments and some local governments have IT security and compliance requirements for their own operations and those of their partners. These organizations must implement policies and equipment that protect critical assets from cyber attacks launched by either outside or inside threats.

#### Logistics

Increased use of mobile technology has exacerbated the need for secure laptop storage but state and local IT budgets remain incredibly tight. These requirements help protect personal and sensitive data and the PCs, laptops, networks and other equipment that contain that data. In addition to defending vital systems and information, these requirements also must not impede the transparency, cost-effectiveness and accessibility of government services.

#### Business and Government Compliance

State and local governments want the advantages of online payment and other e-commerce capabilities. Therefore, they must comply with commercial regulations, such as Payment Card Industry (PCI) requirements and federal laws such as Sarbanes-Oxley (SOX). Failure to comply can forbid violators from performing online credit card transactions, which can severely damage both profitability and customer trust.

#### Notice of Breach

State and local governments must comply with federal legislation with data protection provisions, including the Health Information Portability and Accountability Act (HIPAA), as well as state data breach notification laws mandating public disclosure of breaches that may compromise taxpayers' personal information. Forty-six states and the District of Columbia now have such laws and Congress is debating a national law. Disclosure often brings negative public reaction, government scrutiny and costly notification, mitigation and other damage control measures.

<sup>1</sup> 2009 Annual Study: U.S. Cost of a Data Breach, The Ponemon Institute, January 2010

Self-Encrypting Drives and Wave’s EMBASSY® Software Protect State and Local Government 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 that attackers can exploit to gain unauthorized access to data. Unfortunately, software-based FDE, the most common form of FDE, has exploitable weaknesses — which means it can’t guarantee that lost data is unreadable. This fact leaves state and local governments at continued risk for costly and catastrophic breaches.

To overcome these hurdles and comply with regulations, more government and commercial enterprises are turning to self-encrypting drives (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 software attacks. Further, they cost only marginally more than non-encrypted hard drives, require minimal 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. Wave’s EMBASSY software transforms these self-encrypting drives into a complete managed enterprise encryption solution: one that centrally provisions security policies,

limits access to only authorized users and – perhaps most importantly — provides foolproof assurance that sensitive information stored on an SED remains safe.

Through its partnerships with Seagate, Data Management, Inc. and other trusted government IT providers, Wave’s software has been installed on more than 70 million PCs worldwide. Most importantly, Wave is the leading ISV for managing the security of Seagate Momentus Self-Encrypting Drives, the first SEDs to be certified under the Federal Information Processing Standard 140-2 (FIPS 140-2) set by the National Institute for Standards and Technology (NIST). The certification means that these drives meet data protection standards that all U.S. and Canadian federal, state and local government agencies and regulated industries, such as defense, healthcare and finance must use to protect sensitive information on their computers and networks.

Because state and local governments often have IT infrastructure that mixes new and existing technology, Wave understands the need to protect information on PCs that do not have self-encrypting hard drives. For those agencies that are adopting Windows 7, Wave software provides a comprehensive set of tools to automate and secure the configuration and administration of Microsoft BitLocker drive encryption. So whether you have decided to use the latest in hardware-based encryption, or the latest integrated OS FDE application, we’ve got you covered.

