Better Encryption for a Safer Government

Protecting Federal Agencies — and the Public — from Data Breaches

To better succeed at their missions, federal agencies 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.

The Advanced Persistent Threat (APT), cybercrime and even independent organizations are to blame for the many breach attempts against federal agencies. The White House stated in March 2010 that the number of cyber attacks directed against it increased exponentially between 2008 and 2010.[1]

Data breaches can hurt not just federal agencies but thousands, or even millions, of the people they serve; one of the worst breaches was a 2006 Veterans Administration breach that affected 26.5 million patients. Recent research found that U.S. data breaches averaged $7 million apiece and over $200 per compromised data record[2] — meaning the costs associated with a federal agency breach could be in the millions for taxpayers.

Protecting the federal agencies from data breaches and cyber attacks has thus become a critical priority for both the U.S. government and its partners. Four key related challenges are listed at the right:

[1] http://www.politico.com/news/stories/0310/33987.html

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

Key Federal Agency Data Breach Mitigation Challenges

IT Security

The Federal Information Security Management Act of 2002 (FISMA) mandates IT security and compliance requirements for federal agencies and their partners. These organizations must implement policies and equipment that comply with FISMA and protect critical assets from cyber attacks launched by either outside or inside threats.

Logistics

Many federal agencies — the Internal Revenue Service, the U.S. Department of State, the U.S. Postal Service and others — rely on online payment systems to reduce operating costs and improve the quality of their services. (Note: Federal agencies must comply with Payment Card Industry (PCI). Any organization that holds, processes, or exchanges cardholder information from any of the five major card brands must follow them.) To meet their enterprise-wide needs, federal agencies need protection that is proven, meets government standards, works across platforms and has known acquisition and operational costs.

Business and Government Compliance

Federal agencies want the advantages of online payment and other capabilities. They thus must comply with commercial regulations, such as 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

Federal agencies must comply with federal legislation with data protection provisions, including the Health Information Portability and Accountability Act (HIPAA). Congress is debating a national data breach notification law similar to those in 46 states and the District of Columbia. Disclosure often brings negative public reaction, government scrutiny and costly notification, mitigation and other damage control measures.

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

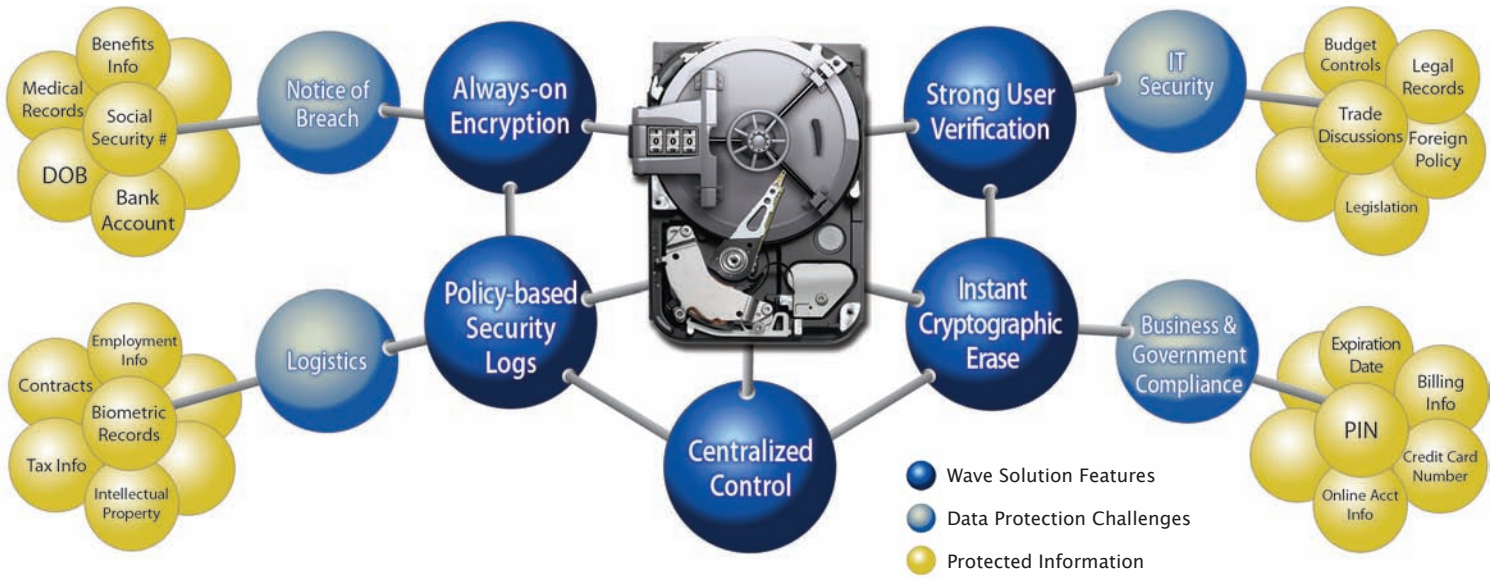
Options abound for protecting sensitive data but many experts consider full-disk encryption (FDE) the best because it encrypts everything on a hard drive, eliminating many vulnerabilities that attackers can exploit to gain unauthorized access to data. Unfortunately, software-based FDE, the most common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

To overcome these hurdles and comply with regulations, more organizations 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 federal agencies 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.



03-000285/ version 1.02

Wave Systems Corp.
480 Pleasant Street, Lee, MA 01238
(877) 228-WAVE • fax (413) 243-0045
www.wave.com

wave®
Simplifying Encryption and Authentication