Self-Encrypting HDDs and SSDs

Robert Thibadeau, Ph.D.
Wave Systems Corp.
Self-Encrypting Drives

Transforming the way you protect your business information
Evolution of Data Protection Solutions
Migration to Hardware

Application Layer
- Software FDE

OS Integration
- Vista® BitLocker™ / EFS

Hardware Integration
- Self-Encrypting Drives

Faster, Simpler, Lower Cost!
FDE Deployment Considerations

- Disk Prep (4 hrs)
- Windows Upgrade (3 hrs)
- Retire/Reuse PC (3 hrs)
- Re-image PC (3 hrs)
- OS Patch (5 hrs)
- Encryption (3 hrs)

Software FDE

Set it...
Self-Encrypting Drive
...and forget it
Self-Protecting Self-Encrypting Drives

Definition?
How do they work

- KEK not MEK
- Opal: Shadow MBR and Preboot
  - Self-Healing MBR & Hypervisor Demo
Data Breach Headlines

- Organization: Blue Cross Blue Shield
- Breach Type: Stolen Laptop
- No of Records: 850,000
- Date: October 6, 2009

Laptop Theft Nets Data On 800,000 Doctors

The stolen laptop contained personal data on nearly every physician in the country.

By Thomas Claburn
InformationWeek
October 16, 2009 03:47 PM

The theft of a laptop belonging to an employee of an insurance trade group has put hundreds of thousands of physician around the country at risk of identity theft.

The laptop, belonging to an employee of the Blue Cross and Blue Shield Association (BCBSA), was stolen from a car in late August, according to reports in the Boston Globe and the Chicago Tribune. It contained a database listing the business and personal information of about 800,000 doctors.
Stolen or Lost Computers are The #1 Cause of Data Breaches

Source: Open Security Foundation DataLoss DB
45 States and the District of Columbia Have Notice of Breach Laws

LEGEND
- States with Breach Laws
- States without Breach Laws
Must Meet NIST SP 800-111

June 2010: Now even if a contractor loses PII, you are blamed unless he meets SP 800-111
Completing the Data-at-Rest Security Puzzle

- 800-111 Access control, centralized mgmt and reporting are required