

**COMPUTERWORLD**

**SNIA**

OCTOBER  
**11-14**  
2010

# SNW

**The Gaylord Texan, Dallas, Texas**

SNIA



**SNW**  
COMPUTERWORLD

October 11-14, 2010  
The Gaylord Texan  
Dallas, Texas

# Industry Perspective: Compliance and Self- Encrypting Drives

Robert Thibadeau, Ph.D.

Senior Vice President and Chief Scientist

Wave Systems, Inc.



# Agenda

- Self-encrypting drives
  - Characteristics
  - Market Drivers
- TCG
- Shadow MBR and Self Healing Demo
- Controller SP and Intel's CPU Conversion

# Self-Encrypting Drives



**Transforming the way  
you protect your  
business information**

SNIA



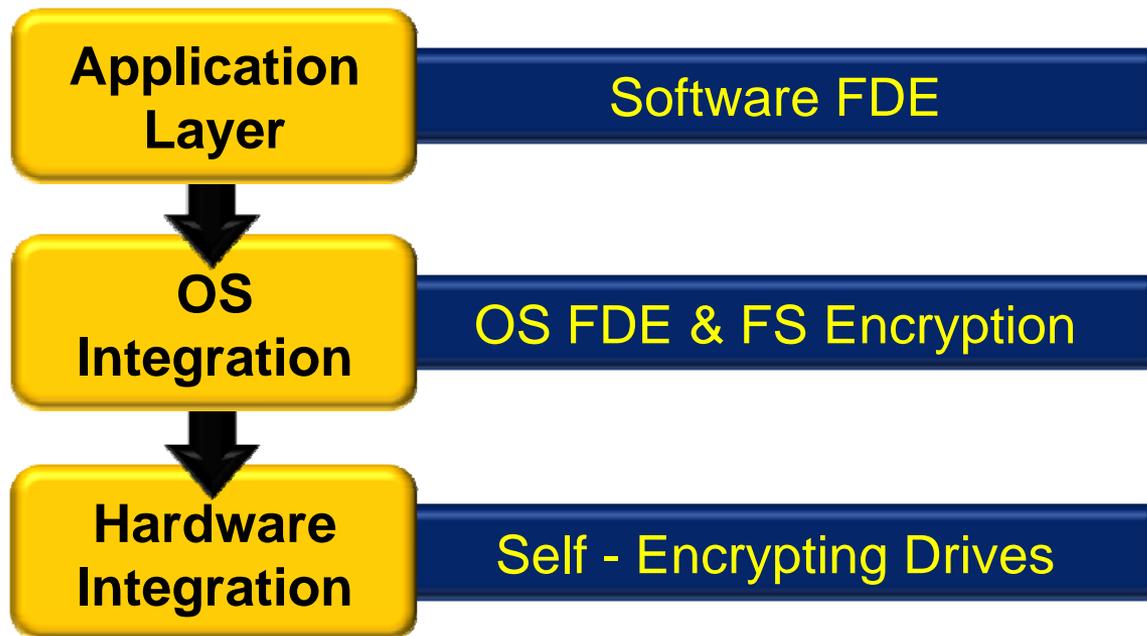
**SNW**

COMPUTERWORLD

October 11-14, 2010  
The Gaylord Texan  
Dallas, Texas

# Evolution of Data Protection Solutions

## *Migration to Hardware*



**Faster, Simpler, Lower Cost!**

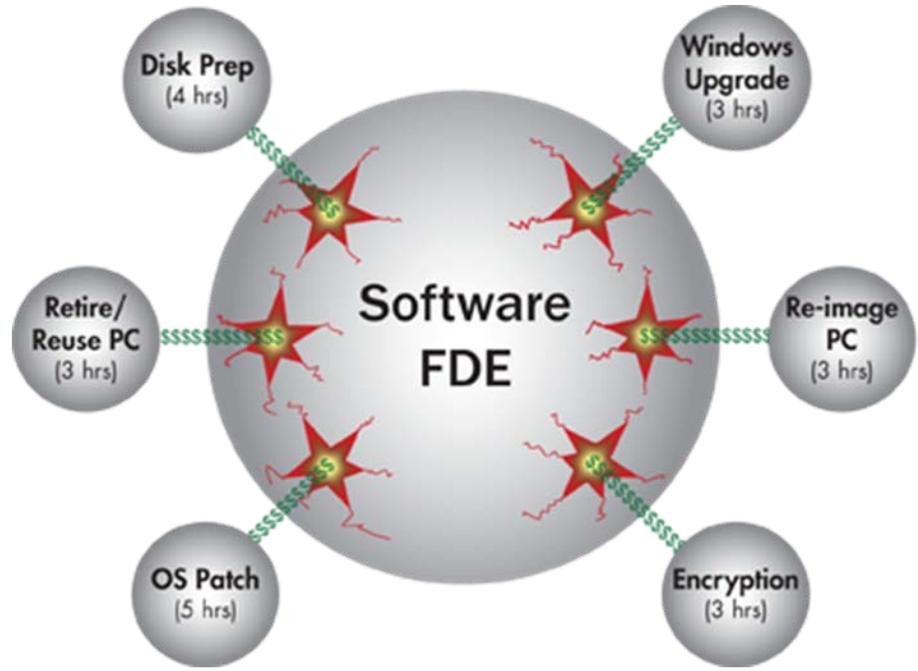
October 11-14, 2010  
The Gaylord Texan  
Dallas, Texas



COMPUTERWORLD

October 11-14, 2010  
The Gaylord Texan  
Dallas, Texas

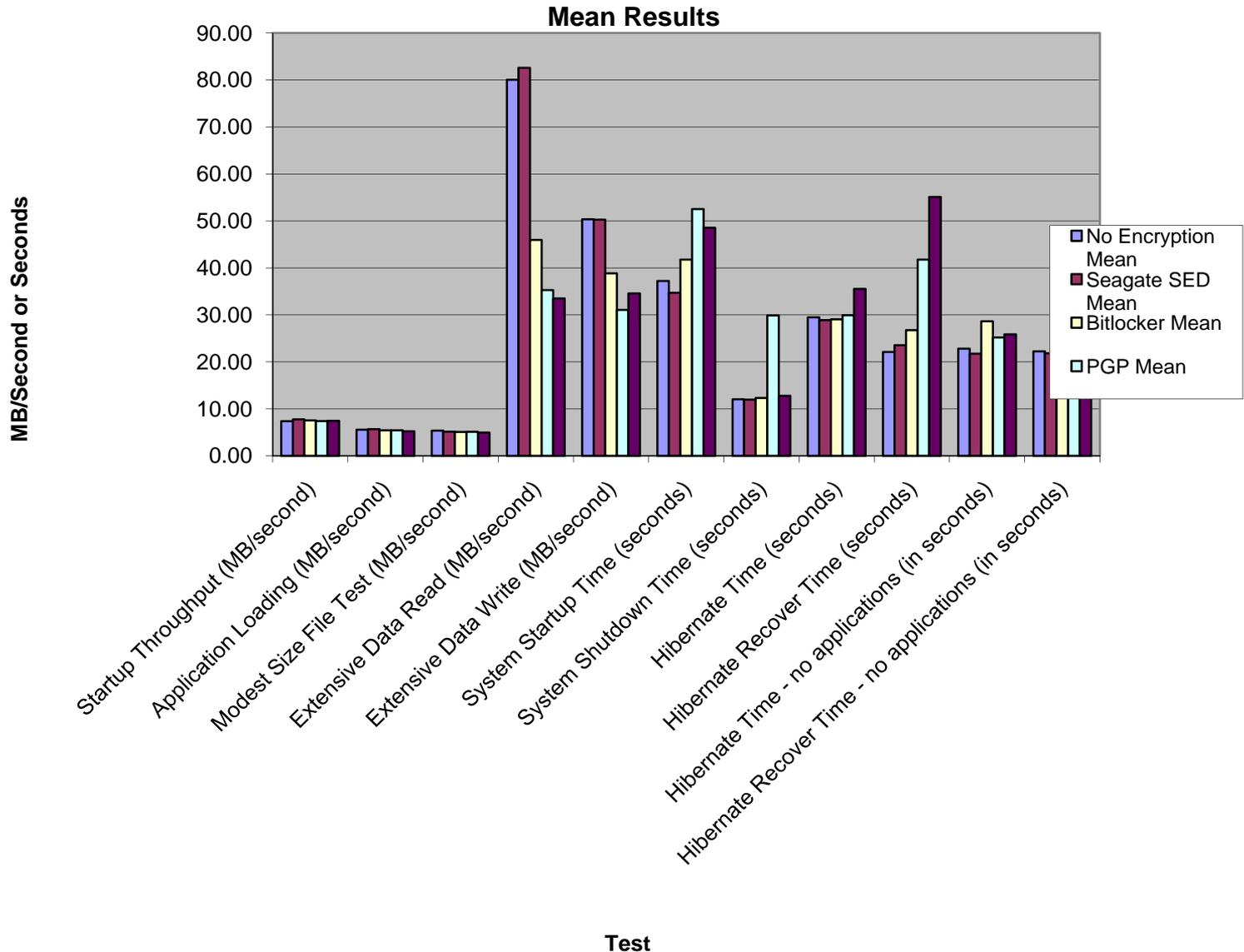
# FDE Deployment Considerations



Set it ...  
**Self-Encrypting Drive**  
... and forget it



# SED vs. SW FDE



# Data Breach Headlines

Welcome Guest | [Log In](#) | [Register](#) | [Membership Benefits](#)

**InformationWeek Healthcare**  
InformationWeek Healthcare Newsletter  
SIGN UP HERE

Powered By  
**InformationWeek BUSINESS TECHNOLOGY NETWORK**

RSS FEEDS  
SUBSCRIBE  
EVENTS  
DIGITAL LIBRARY

Home News Blogs Software Security Hardware Mobility Windows Internet Global CIO Government **Healthcare** Financial

- Administration Systems
- Clinical Information Systems
- CPOE
- Electronic Medical Records
- Healthcare Blogs
- Healthcare Stories
- Interoperability
- Leadership
- Mobile & Wireless
- The Patient
- Policy & Regulation
- Security & Privacy

E-mail | Print | BOOKMARK | Take Us With You | Buzz up!

## 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 15, 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.

**More Security Insights**  
**Whitepapers**

- The ROI and TCO Benefits of Data Deduplication for Data Protection in the Enterprise
- 7 Ways to Reduce IT Costs with Master Data Management

There were about 732,000 practicing physicians in the U.S. at the end of 2007, according to a spokesperson for the American Medical Association.

The BCBSA, which represents various Blue Cross health groups across the U.S., did not immediately respond to a request for comment.

A spokesperson for the American Medical Association confirmed

**Organization:**  
Blue Cross  
Blue Shield

**Breach Type:**  
Stolen Laptop

**No of Records:**  
850,000

**Date:**  
October 6, 2009

**The Latest Security News**

- Google Launches Music Search
- Verizon Drops iPhones Phone
- Google's 'Gov Cloud' Wins \$7.2 Million Los Angeles Contract

**AirWave OnDemand**  
It's everything the IT Guy needs, to be the hero every organization wants.

October 11-14, 2010  
The Gaylord Texan  
Dallas, Texas

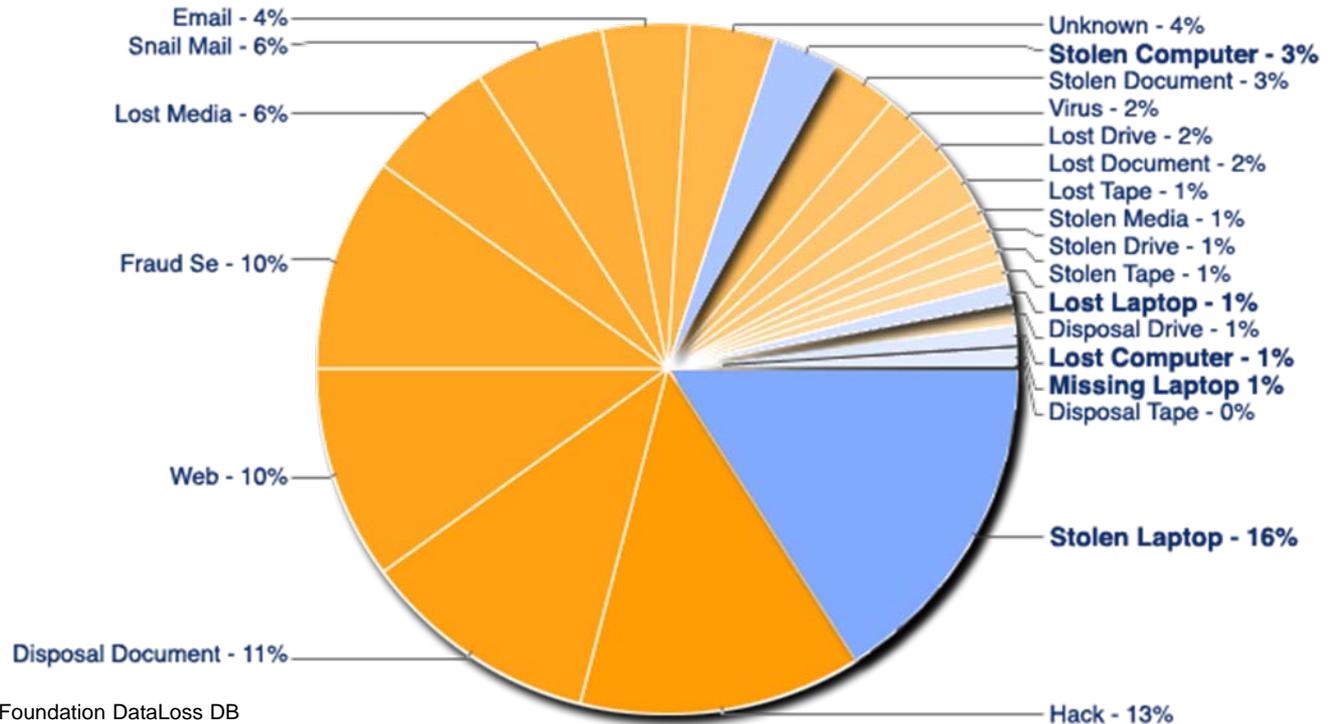
SNIA



**SNW**  
COMPUTERWORLD

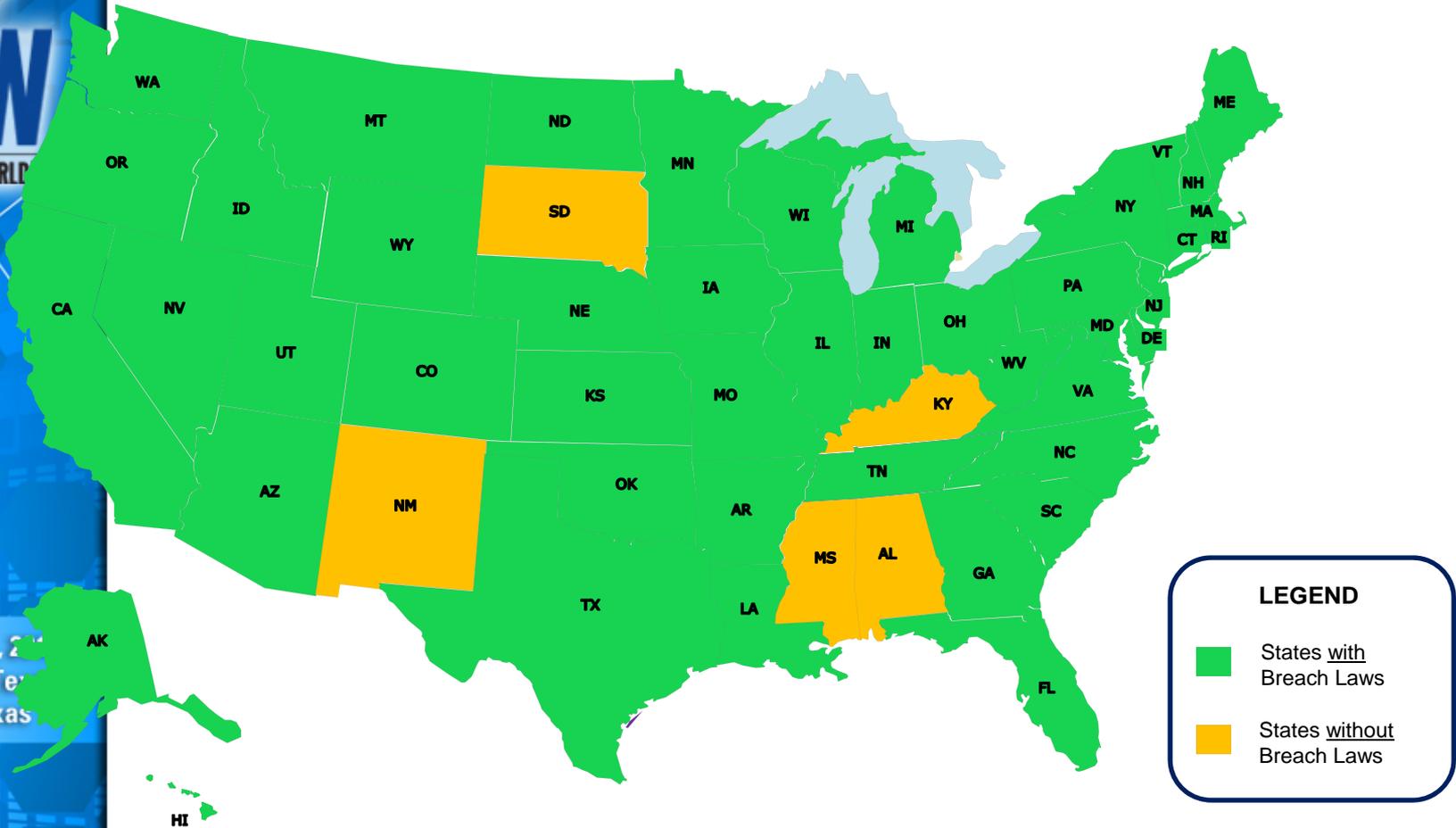
# Stolen or Lost Computers are The #1 Cause of Data Breaches

Incidents by Breach Type — 2009



Source: Open Security Foundation DataLoss DB

# 45 States and the District of Columbia Have Notice of Breach Laws



October 11-14, 2011  
The Gaylord Texaco  
Dallas, Texas



# HITECH

- Safe Harbor for Data Breach Notification Laws
- Amendment to HIPAA Effective Law Feb 17, 2010
- Requires NIST 800-111 for Data At Rest
  - Requires IT Managed Full Disk Encryption Solutions



## Feb 17, 2010 : Safe Harbor

- 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

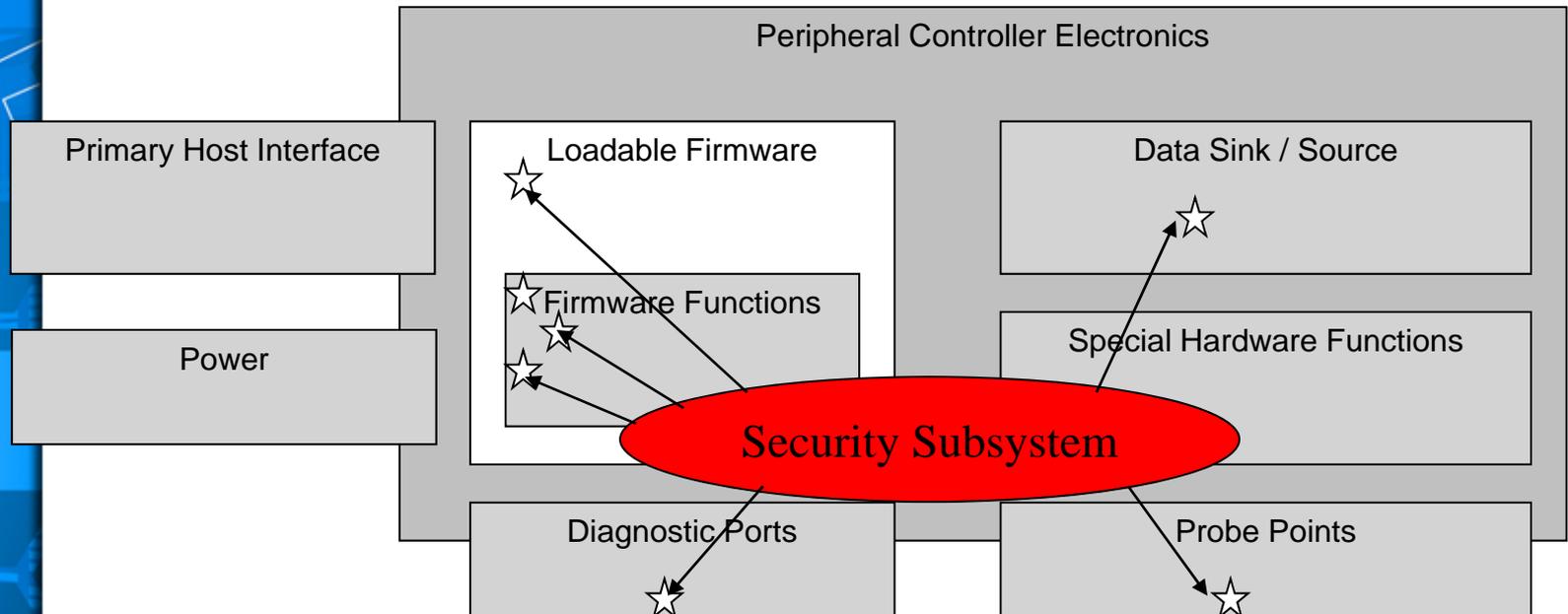


- 800-111 Access control, centralized mgmt and reporting are required

October 11-14, 2010  
The Gaylord Texan  
Dallas, Texas

# Storage Devices are full scale computers (CPU(s), RAM, ROM, Flash, and lots of secured NV Memory) that are SLAVES with limited commands.

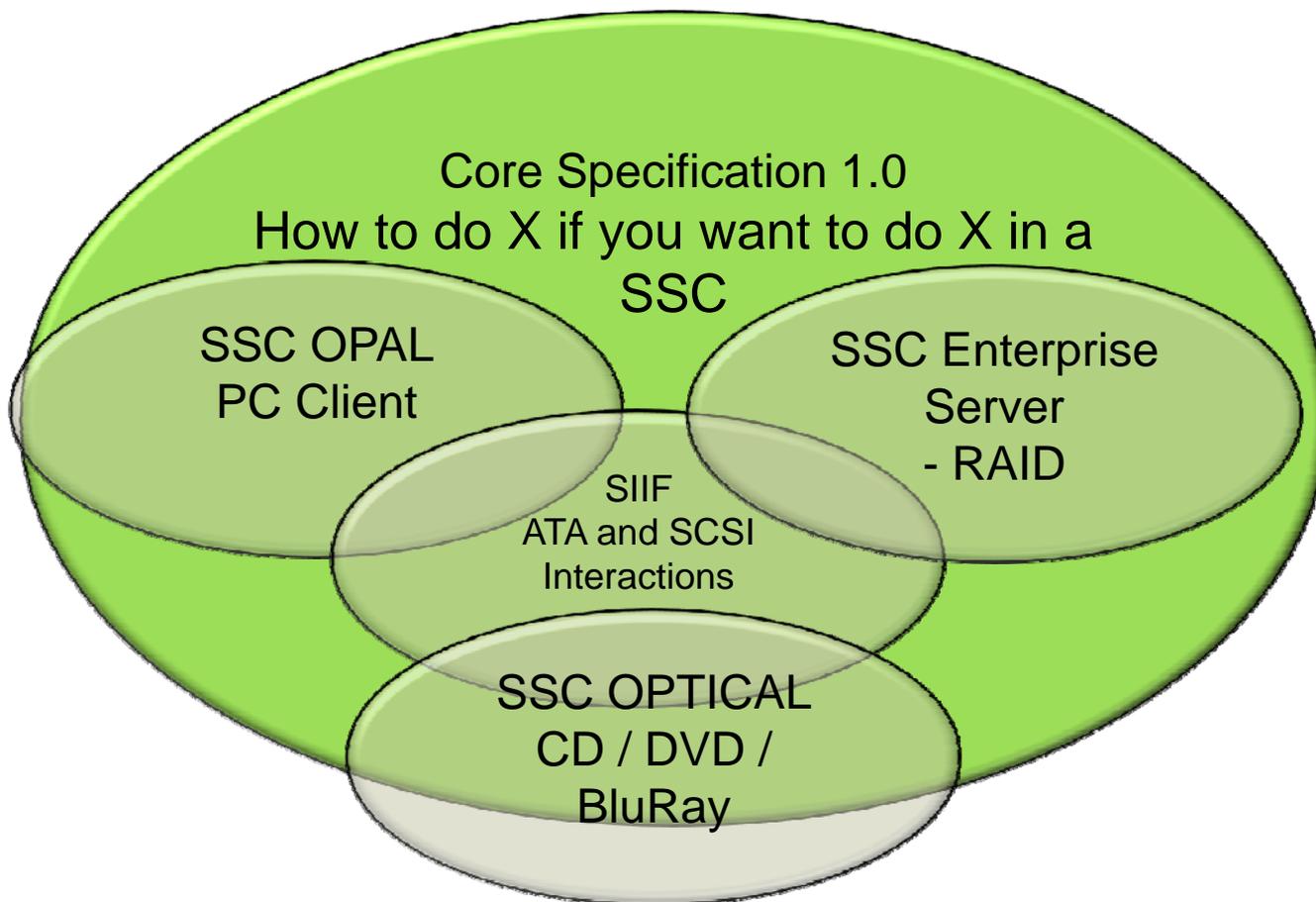
- Only two ATA and SCSI command sets, TCG adds security subsystem commands that tunnel through ATA and SCSI.



October 11-14, 2010  
The Gaylord Texan  
Dallas, Texas

# Spec Organization – VENN Diagram

SSC = Security Subsystem Class



SNIA



**SNW**

COMPUTERWORLD

October 11-14, 2010  
The Gaylord Texan  
Dallas, Texas

SNIA



**SNW**  
COMPUTERWORLD

October 11-14, 2010  
The Gaylord Texan  
Dallas, Texas

# How do they work

- KEK not MEK
- Opal and Enterprise: Multiple Bands (Match FS Partitions)
- Opal: Shadow MBR and Preboot
  - Self-Healing MBR & Hypervisor Demo

# SED is Secure for Data at Rest

BOOT HYPERVISOR / OS

320 GIGABYTE DRIVE

**UNLOCKED!**

**POWER UP!**

October 11-14, 2010  
The Gaylord Texan  
Dallas, Texas

SNIA



**SNW**  
COMPUTERWORLD

October 11-14, 2010  
The Gaylord Texan  
Dallas, Texas

## Kleissner Return from Hibernate Attack

- Hiberfil.sys for rapid 'winresume' restart of Windows
  - Changes everytime – not great for TPM measurement!
  - Winresume cannot and does not check programs frozen in hiberfil.sys
  - Hack hiberfil.sys and you can load unsigned code into Windows in returning from hibernation.
- Write malicious MBR to disk via normal application using raw sector access
- Modify hiberfil.sys with MBR record and now the user will unknowingly inject malicious unsigned code into Windows (or, similarly, any OS/hypervisor)

**the attack**

SNIA



**SNW**  
COMPUTERWORLD

October 11-14, 2010  
The Gaylord Texan  
Dallas, Texas

# Kleissner Return from Hibernate Attack

Foiled by measuring MBR in preboot

Problem: Do you stop booting?

Need a Self-Healing Solution to the Kleissner Attack

# Demo: Why SED can Provide MBR Boot Integrity

RESUME HYPERVISOR/OS

320 GIGABYTE DRIVE

**UNLOCKED!**

MALICIOUS MBR

VALID MBR

SNIA



SNW

October 11-14, 2010  
The Gaylord Texan  
Dallas, Texas

**Table 223 LockingInfo Table Description**

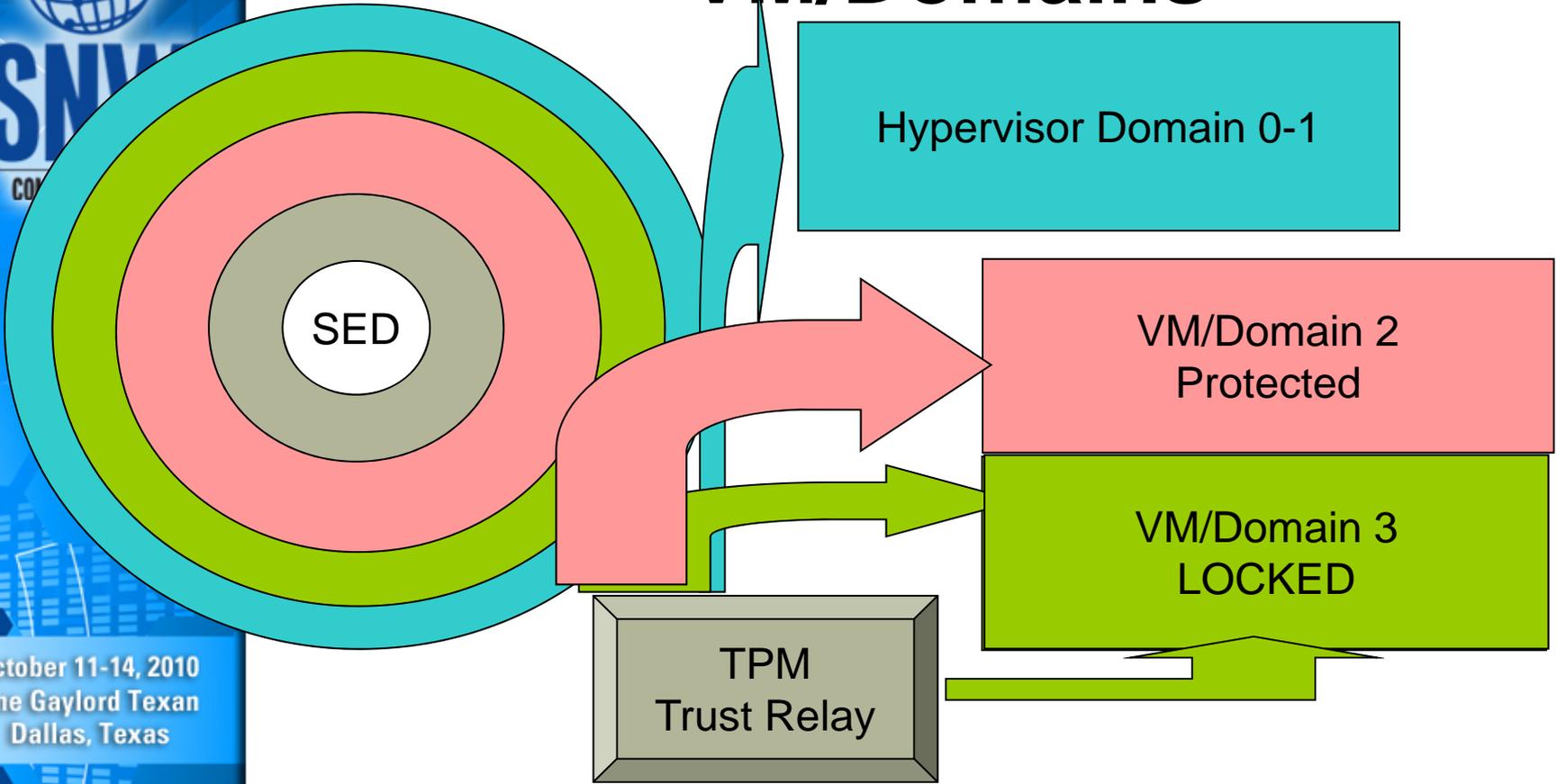
Column Number	Column Name	IsUnique	Column Type
0x00	UID		uid
0x01	Name		name
0x02	Version		integer_4
0x03	EncryptSupport		enc_supported
0x04	MaxRanges		integer_4
0x05	MaxReEncryptions		integer_4
0x06	KeysAvailableCfg		keys_avail_conds



**Table 224 Locking Table Description**

Column Number	Column Name	IsUnique	Column Type
0x00	UID		uid
0x01	Name		name
0x02	CommonName		name
0x03	RangeStart		uinteger_8
0x04	RangeLength		uinteger_8
0x05	ReadLockEnabled		boolean
0x06	WriteLockEnabled		boolean
0x07	ReadLocked		boolean
0x08	WriteLocked		boolean
0x09	LockOnReset		reset_types
0x0A	ActiveKey		mediakey_object_uidref
0x0B	NextKey		mediakey_object_uidref
0x0C	ReEncryptState		reencrypt_state
0x0D	ReEncryptRequest		reencrypt_request
0x0E	AdvKeyMode		adv_key_mode
0x0F	VerifyMode		verify_mode
0x10	ContOnReset		reset_types
0x11	LastReEncryptLBA		uinteger_8
0x12	LastReEncStat		last_reenc_stat
0x13	GeneralStatus		gen_status

# Multi-band and HAP VM/Domains



October 11-14, 2010  
The Gaylord Texan  
Dallas, Texas

TCG Opal is minimum of 4 bands

SNIA



**SNW**  
COMPUTERWORLD

October 11-14, 2010  
The Gaylord Texan  
Dallas, Texas

# Controller SP

- Recent announcement of post sales CPU performance upgrade
- Controller SP – Methods for configuring drive personalities under cryptographically strong activation / deactivation.

SNIA



**SNW**

COMPUTERWORLD

October 11-14, 2010  
The Gaylord Texan  
Dallas, Texas

**Thanks!**

**See Technical Article  
Steven Teppler on  
Current Compliance Laws**