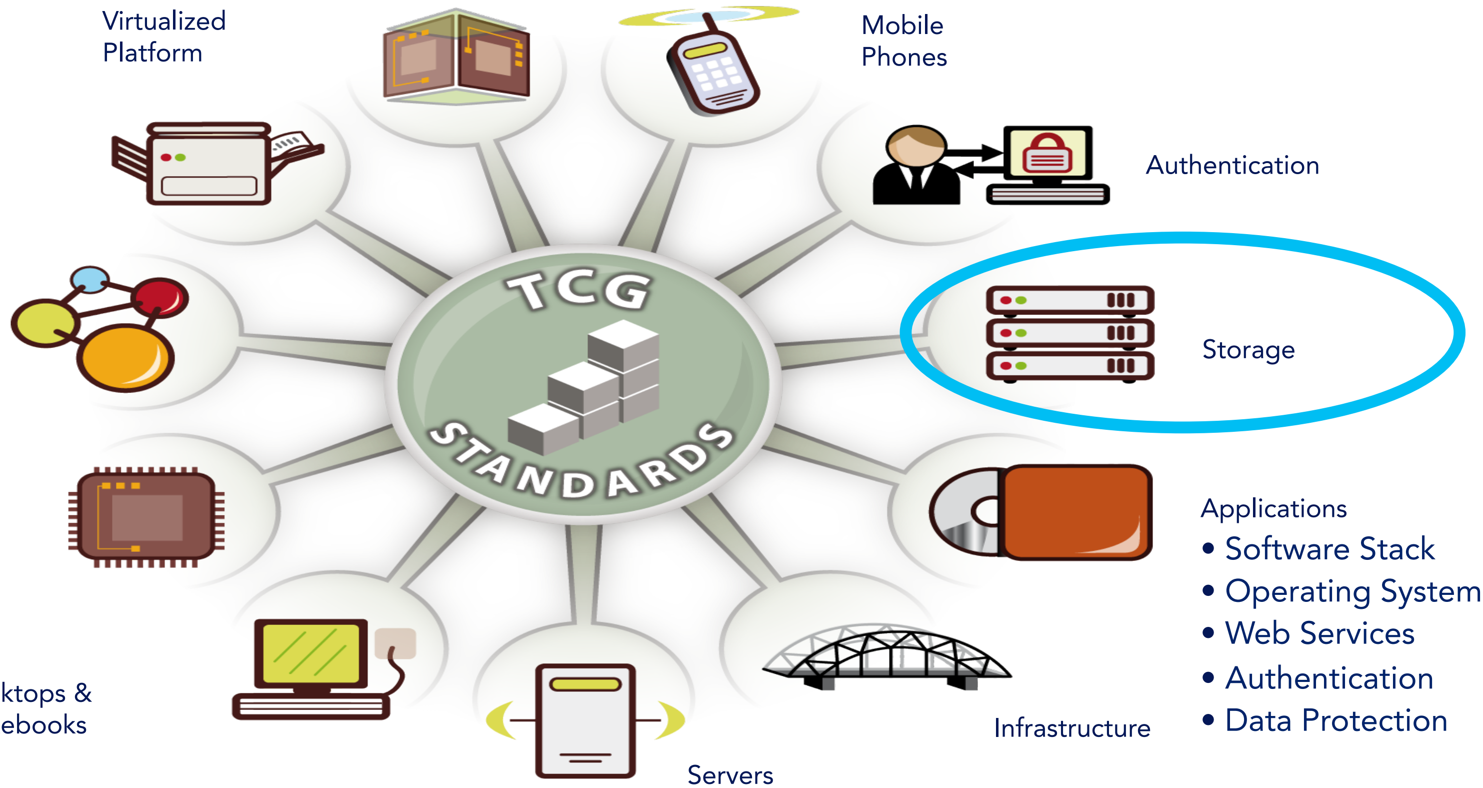
Self-Encrypting Storage: Simplest Security for Stored Data

Michael Willett, Ph.D.
VP Marketing

Bob Thibadeau, Ph.D
CEO

Drive Trust Alliance
www.drivetrust.com

Trusted Computing Group Standards



Virtualized Platform

Mobile Phones

Printers & Hardcopy

Authentication

Network Security

Storage

Security Hardware

Applications
- Software Stack
- Operating Systems
- Web Services
- Authentication
- Data Protection

Desktops & Notebooks

Servers

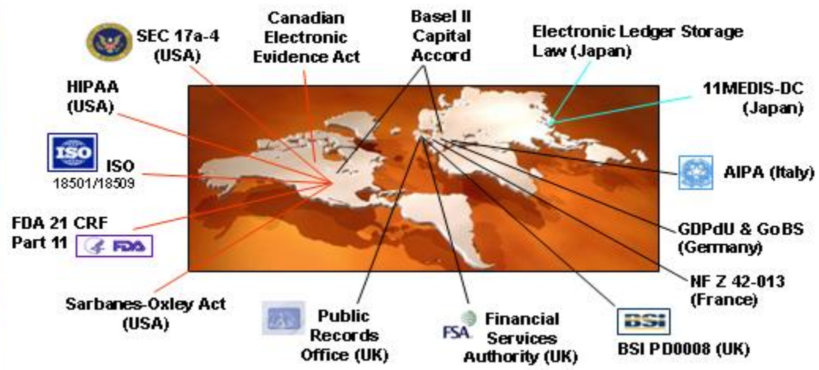
Infrastructure

The Problem…

2005-2013: over 864,108,052 records containing sensitive personal information have been involved in security breaches

In 2013, U.S. businesses paid an average cost of $5.4 million per data breach; that's $188 per record

- **$5.4 Million Per Incident**



http://www.privacyrights.org/ar/ChronDataBreaches.htm
http://www.symantec.com/about/news/resources/press_kits/detail.jsp?pkid=ponemon-2013

The Problem…

2005-2013: over 864,108,052 records
contai
been in

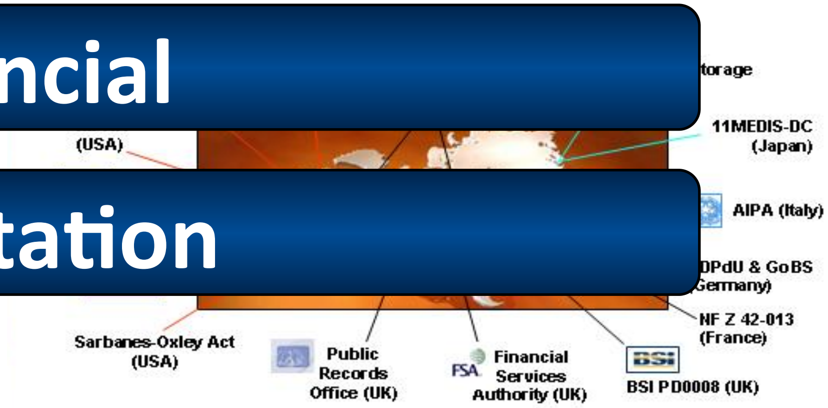
age cost of $5.4
er record

$5.4 Million Per Incident

Legal

Financial

Reputation



http://www.privacyrights.org/ar/ChronDataBreaches.htm
http://www.symantec.com/about/news/resources/press_kits/detail.jsp?pkid=ponemon-2013

Breach Notification Legislation

Example: California

"… any agency that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person…"

Encryption "safe harbor"

Trusted Storage Standardization

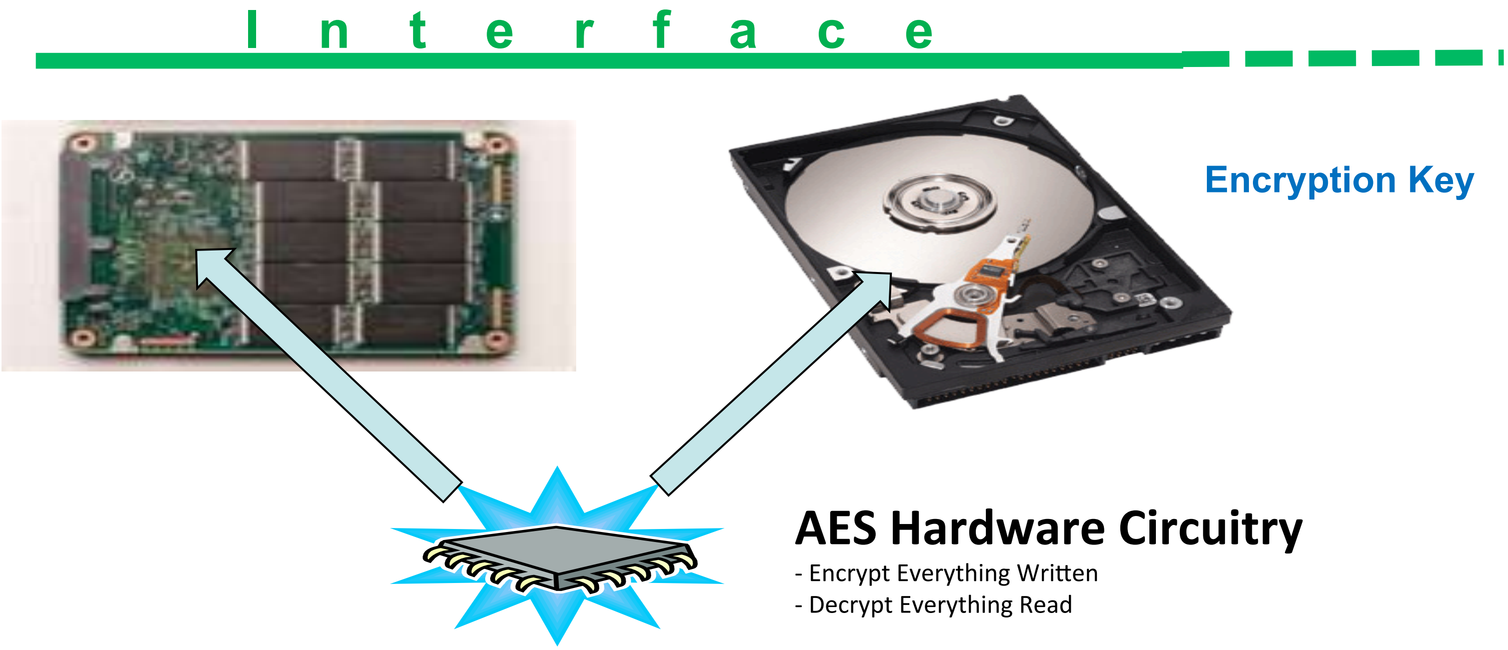
TRUSTED COMPUTING GROUP™

Published Storage Specifications

Self-Encrypting Drives (SED)

What is a Self-Encrypting Drive (SED)?

Trusted Computing Group
SED Management Interface



Interface

Authentication Key

Encryption Key

AES Hardware Circuitry

- Encrypt Everything Written
- Decrypt Everything Read

SED Superiority

- Simplified Management
- Robust Security
- Compliance “Safe Harbor”
- Cuts Disposal Costs

- Scalable
- Interoperable
- Integrated
- Transparent

Crypto Erase

www.drivetrust.com

Flash SSDs
iPhones, iPads,
Android
All of Google
etc.
All Printers

Protecting
“USER” Data

There Should Be No Encryption Backdoors, Only Front Doors

"In two sentences: iPhones and iPads have always had front door central encryption management using international standards. The government needs to learn how to legally employ the solutions that companies have employed for over a decade."

READ MORE

Drive Trust Alliance on Apple/FBI Security Debate
Happening NOW
FOX NEWS LIVE
WSJ: FBI WANTS TO UNLOCK PHONES IN A DOZEN CASES NOT TERROR-RELATED
STILITIES IN SYRIA" ... ANNOUNCEMENT CAME HOURS AFTER U
S&P 21.94

Automotive Use Cases

(Parallel Already Adopted Use Cases)

0. Purpose Protect the Privacy of “User” Data (when the “user” isn’t using it.)

1.Your car key (phone, whatever) that starts you car should cryptographically unlock all the data you and your passengers need.

2.When you sell your car (repurpose a corporate vehicle, whatever) you should be able to cryptographically erase all “user” data very quickly (logging into your car’s web site).