



UCSF School of Medicine
Office of the Dean, Information Services Unit



SOM Encryption Project

Opinder Bawa, May 2009

IT Security is ...

- Devices
 - Laptops, Desktops, Blackberry, iPhone, Palm
- Servers
 - Sensitive or shared data, behind firewalls, secure data centers
- Applications
 - Developed by qualified staff, securely written, access
- Databases
 - Encryption of databases and backups

UCSF Recent Examples

- 3 Laptops January - March
 - No. 1) Timely reported, encryption verified, no action needed
 - No. 2) Unencrypted, patients notified (331); potential penalty \$250K+
 - No. 3) Timely reported, identifying IT owner took 4-6 hours; No reported sensitive data on hard drive, no encryption, unable to verify or audit data
- 1 Hand held device - March
 - Lost 9:00am
 - IT notified 2:30pm
 - “Wipe” command issued 3:30pm
 - “Wipe” successful confirm 5:35pm

Recent Industry Data Points

- Avg. cost of lost laptop \$49,246
 - Breached data \$39,297
 - Intellectual Property \$5,871
 - Other Costs \$4,078
- Average savings with encryption \$20,000
- Response time based avg. costs
 - Within 1 Day \$8,950
 - After 1 Week \$115,849

* Intel-sponsored study by Ponemon Institute: 138 laptops / 12 months / 29 organizations

Project Drivers

- AB-211 penalizes individuals and institutions that negligently disclose medical information
- SB-541 mandates prevention of unlawful, unauthorized access of patient information
- Price Waterhouse (PWC) Security Audit Report November 2008
- New UCSF technology standards
- Inconsistent implementation of encryption policies in the past
- Unable to track or audit the current installations

Scope and Funding

Scope

• Blackberry Devices	Completed	~320
• iPhone/other Devices	Fall '09	~300
• Univ. Laptops	Not complete	>2500
• Univ. Desktops	Not complete	>5000
• USB Drives/Memory Sticks	Need Stds.	Unknown
• Personal Laptops	Need Policy	Unknown
• Personal Desktops (homes)	Need Policy	Unknown

Funding Plan for Laptops

- Deans Office shares costs
 - ~\$100/device Dean provides software
 - ~\$225/device Department pays for labor
(Not flat rate, charge only for actual time expended)
- Annual costs paid by each respective department (~\$50/device/year)
- Department will have to also fund older system replacements (~3 years old)

Execution Options

- A) Department IT
 - Department managed rollout and funding, software choices
 - Learning curve for each IT team, inconsistency, gaps, lose efficiency, overall higher costs, duplicate setups
 - Dean's Office funds software (~\$100/device)
 - Department uses its own internal resources
 - ISU will only audit (\$92.20/hour)
- B) Focused project team approach by ISU
 - Lose some flexibility, new model for some
 - Consistency, inventory, lower overall costs, endorsed by STAC*, audit worthy
 - Dean's Office funds software (~\$100/device)
 - Department recharged labor (~\$225/device)

* **S**chool Of Medicine **T**echnology **A**dvisory **C**ommittee – members list in appendix

Execution Plan

- Phase 1
 - Inventory and analysis of devices
 - Which ones can be encrypted, need replacement, etc.
 - Encrypt SOM laptops or encrypted replacement
 - Develop USB Drive encryption standards
- Later Phases
 - Use Audit software to identify locations of sensitive data
 - Help users relocate sensitive data to secure servers
 - Encrypt SOM desktops where data cannot be relocated
 - Encrypt personal laptops & desktops (pending policy)

Logistics

- Leverages whatever we can from Campus & Medical Center
- Installing encryption is time intensive
 - for maximum efficiency and lowest cost, encrypt multiple computers in parallel at a central ISU staging area
- Over weekends as much as possible to minimize downtime during business hours

Risks

- **Can take up to 10 hours** (average is 3 hours)
 - Device labor costs higher (~\$225 + \$64.33/hour)
- **Disk crashes** (backups taken, spare hard drives)
- **Old systems** (need to retire or replace)
- **Repetitive scheduling or unavailability**

Communication Plan

- Present to Department Chairs May 4
- Email materials to SOM Managers May 5
- Publish materials on ISU Website May 5
- Review with SOM Managers May 15
- Meet with individual SOM Managers As Requested

Work Plan

- Identify all departments opting-into ISU Focused Project Team approach (finalize device count for this project)
- Identify full time Technical Project Manager
- Develop Project Schedule and Resource Plan
- Develop FY 09-10 Budget Plan
- Begin assembling the team targeting July 2009 initiation

Questions?

Additional Information Slides

Current Project Overview

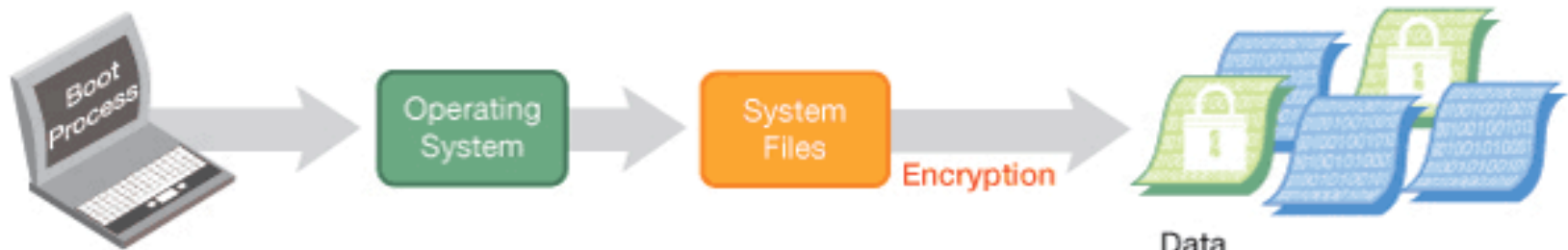
- Encryption prevents unauthorized access to PHI and other sensitive data stored on computer hard drives
- For multiple compliances and data security reasons, we need to encrypt SOM devices
- Phased approach due to cost, beginning with highest risk computers

Detailed Size

- **SOM ISU Supported** (includes SFGH & Fresno)
 - Deans Offices 750 Devices
 - Several Departments 2000 Devices
- **SOM Depts with some known IT Support**
 - Estimated 4000+ Devices
- **SOM Depts with no known IT Support**
 - E.g. Labs 2000+? Devices

How it works

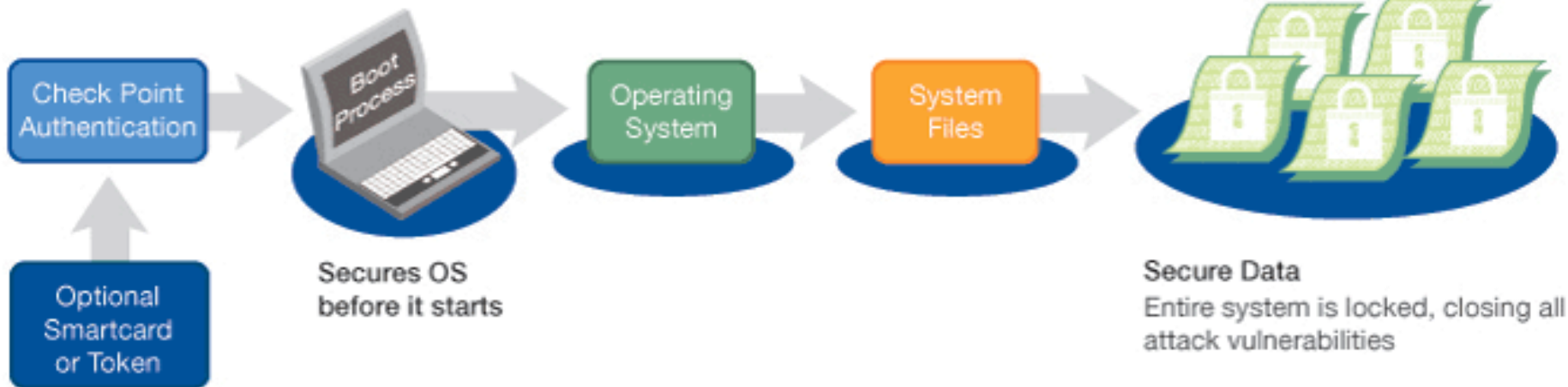
Unprotected System or File and Folder Protection



Data

Full access to system information through unsecured operating system means data is vulnerable to multiple attacks

Check Point Endpoint Security Full Disk Encryption



Costs For Encrypting Laptops

- One Time
 - New Campus Software - ~\$100/device
 - Labor - ~\$225/device
- Annual on going
 - Software - ~\$50/device
 - Labor - Part of normal support by ISU or Dept IT

SOM Technology Advisory Committee

- Brad Immanuel Department of Anesthesia
- Todd Bazzill Department of Radiology
- Issac Sato Department of CVRI
- Erik Wieland Department of Medicine
- Tim Greer San Fran. General Hospital
- Joe Hesse Department of Neurology
- Jenny Broering Department of Urology
- Opinder Bawa Dean's Office, SOM (Chair)

California Assembly Bill 211 (AB-211)

January 2009

- AB 211 fines and civil penalties against any individual
 - negligently discloses or knowingly and willfully obtains, discloses, or uses medical information in violation of state / federal laws.
- Enforced by Office of Health Information Integrity (CalOHii)
- Penalties
 - various fines per violation, one of which has a maximum of US\$250,000
 - misdemeanor if the patient suffers economic loss or personal injury
 - potential for civil action by the patient with statutory damages (\$1,000) in addition to actual damages
 - notify the licensing board for further investigation or discipline of individual providers
- May apply to institutions or to individuals or to both

California Senate Bill 541 (SB 541)

January 2009

- SB 541 imposes penalties upon institutions
 - failure to prevent or report for unauthorized access use, or disclosure of medical information.
- Enforced by Calif. Department of Public Health (CDPH).
- Penalties:
 - up to US\$25,000 per patient
 - up to \$17,500 per subsequent access, use, or disclosure
 - \$100 per day that the violation is not reported within the 5-day reporting period
- Applies to institutions, not to individuals.