Local Data Protection (LDP)

A Case Study
Laptop Encryption

Eric V. Leighninger
Chief Security Architect
Allstate Insurance Company

PD1

Agenda

- **Allstate and Information Security – A Snapshot View**
- **Laptop Encryption – Goals, Expectations, Priorities**
- **Technology Acquisition – Vendor Selection Process**
- **Vender Solution Deployment**
- **Lessons Learned**

Slide 2

PD1 As with the rest of this template, this is a suggested agenda that may or may not fit your situation. Please feel free to make changes as you see fit, including adding and changing pages - this is only a template. In general, the idea is to educate folks on the technology challenge you faced, how you addressed it, and the business benefits the project ultimately delivered - or failed to deliver, as the case may be. Keep in mind that people can learn a lot by hearing what went wrong with your project, so don't be afraid to mix the bad with the good.

Paul Desmond, 9/28/2006

PD2

Allstate – A Snapshot

- **Allstate Insurance Company**
  - Founded in 1931 as part of Sears, Roebuck & Co, and became a publicly traded company in 1993
  - Nation's largest publicly held personal lines insurer with nearly 40,000 employees
  - Providing personal financial services and managing risk for our customers
  - Providing insurance and financial products to more than 17 million households
    - More than 14,000 agents and financial specialists, and their licensed sales professionals
    - Over 1,000 exclusive financial specialists who provide life insurance and financial products

Allstate
You're in good hands.

Slide 3

PD2

As with all labels in this template, please replace these with your own. i.e.:

Manufacturing company

2,000 employess

Offices in 23 states

Conservative with respect to technology; low tolerance for risk

Paul Desmond, 9/28/2006

Allstate's Vision for Information Security

- **Aligned with Corporate and Technology Strategy**
- **Security Solutions Prioritized Based Upon Risk**
- **Operational Excellence**

Local Data Protection - Goals

- **Reduce Risk of Exposure**
- **Minimize Recovery and Support Costs**
- **Ensure Compliance**
- **Enable Productivity and Ease of Use**
- **Leverage Investment in Existing IT Infrastructure**

Local Data Protection Priorities

- Policy Holder and Applicant Data
- Employee Data
- PHI
- Credit Card Numbers
- Confidential Data
- Financial Information – Pre Earnings Release
- Communications to Competitors, Partners and Suppliers
- Source Code
- Competitive Sensitive Information

Local Data Protection – Multiple Facets

- **Full Disk Encryption**
  - Laptops
  - Desktops
- **Encryption of Removable Media**
  - USB-enabled Devices – Flash Drives, iPods, Bluetooth Devices, Thumb Drives, Hard Disks
  - CD/DVD Writers
- **Password and PIN Controls**
  - Blackberry
  - Other PDA Devices
- **Standards and Guidelines for Encryption**

Laptop – Full Disk Encryption Evaluation

- **Step 1: Using the local data protection goals and solution selection criteria**
  - Performed paper analysis of top Gartner Magic Quadrant full disk encryption vendors
  - Interviewed vendors regarding respective product functionality
- **Step 2: Performed hands-on product evaluation per our technology evaluation process at Allstate for candidate vendor Pointsec**
- **Step 3: Based on in-house evaluation results Allstate purchased the following Pointsec products:**
  - Pointsec for PC [now Check Point Endpoint Security Full Disk Encryption]
  - Pointsec Media Encryption (PME) [now Check Point Endpoint Security Media Encryption]
  - webRH

Allstate
You're in good hands.

Encryption Solution Selection Criteria

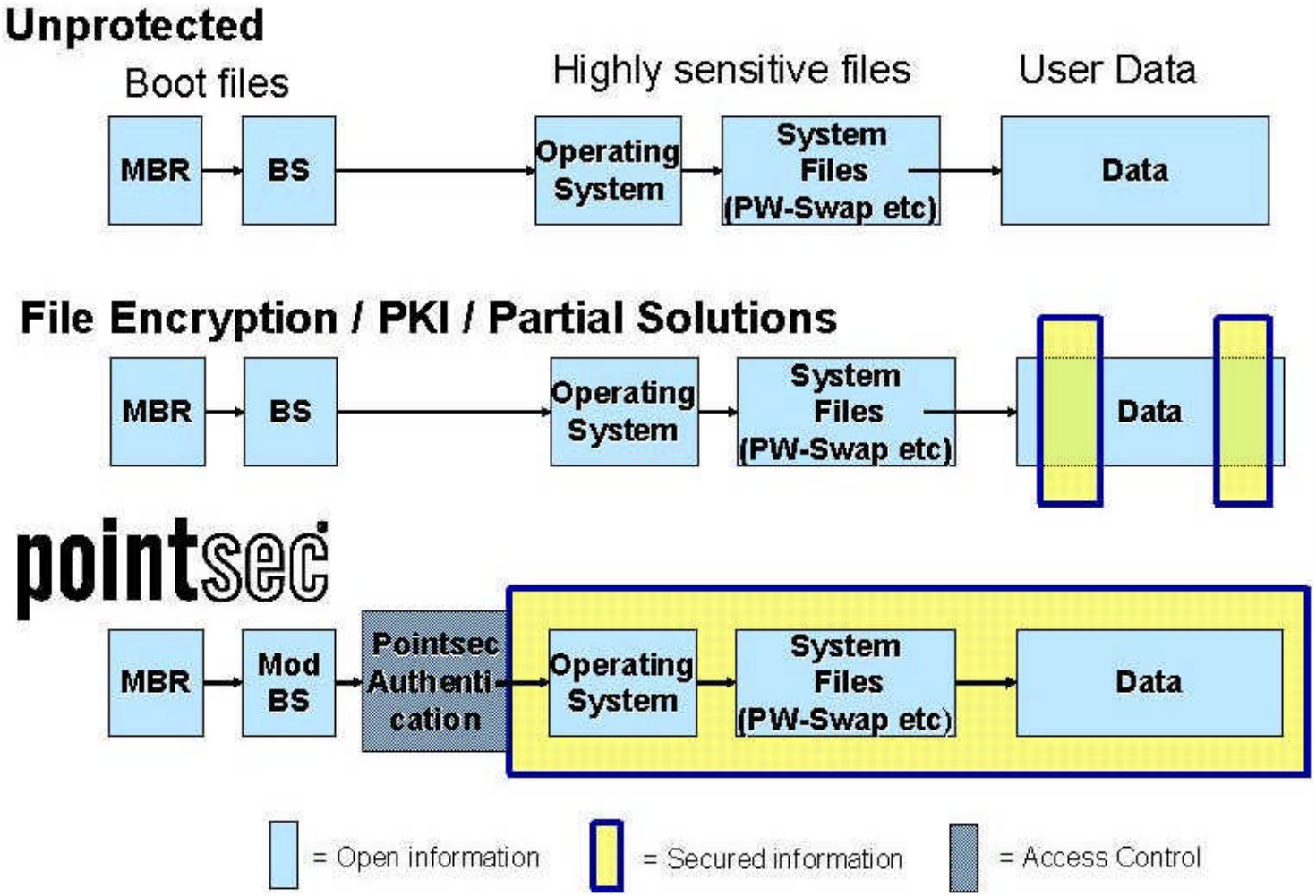
Selection Criteria

- ✓Strong approved cryptography algorithms (AES)
- ✓Encrypts entire disk (all disk sectors)
- ✓Strong Key (min 128 bits) storage & exchange methods
- ✓Meet Federal Standards Ability to control data viewing privileges of administrators and Contingent workers.
- ✓Separation of administrator's ability to access or manage encryption keys.
- ✓Storage of encrypted keys separately from the encrypted data.
- ✓Audit & Reporting Capabilities
- ✓Mandatory access control feature
- ✓Central Management (GUI)
- ✓Low performance degradation
  - *Encryption should take approximately 10 GB per hour regardless of amount of information on the hard drive*
  - *1-3% noticeable system performance degradation after disk is fully encrypted*
- ✓Key Recovery (primary (onsite), remote (offsite) and DR)
- ✓Interoperability with current Enterprise software
- ✓Support removable media
- ✓Fast robust, reliable initial encryption
- ✓Ease of Implementation (SMS Package)
  - *Guaranteed installation*
  - *User may not un-install without Administrator approval*
  - *Lowers total cost of ownership (configure and forget)*
- ✓Architected cryptographically secure Infrastructure
- ✓Integration into current environment easily
- ✓ Throttled background encryption service
  - *Low priority process*
  - *Allows other applications priority to access processor*
- ✓Fault tolerant
  - *User may shut down during encryption process*
  - *Power outage does not effect encryption process*
- ✓Suspend, hibernation, mouse support

Laptop – Full Disk Encryption Solution Rationale

- **Pointsec for PC provided the following advantages to Allstate:**
  - Strong security model
  - Leveraged our current SMS infrastructure for deployment and management
  - Supported Allstate's current Image and Break-Fix processes
  - Did not require alteration or replacement of key Windows components: Windows Master Boot Record and the Windows GINA
  - Size of installed base of users
  - Attractive product TCO

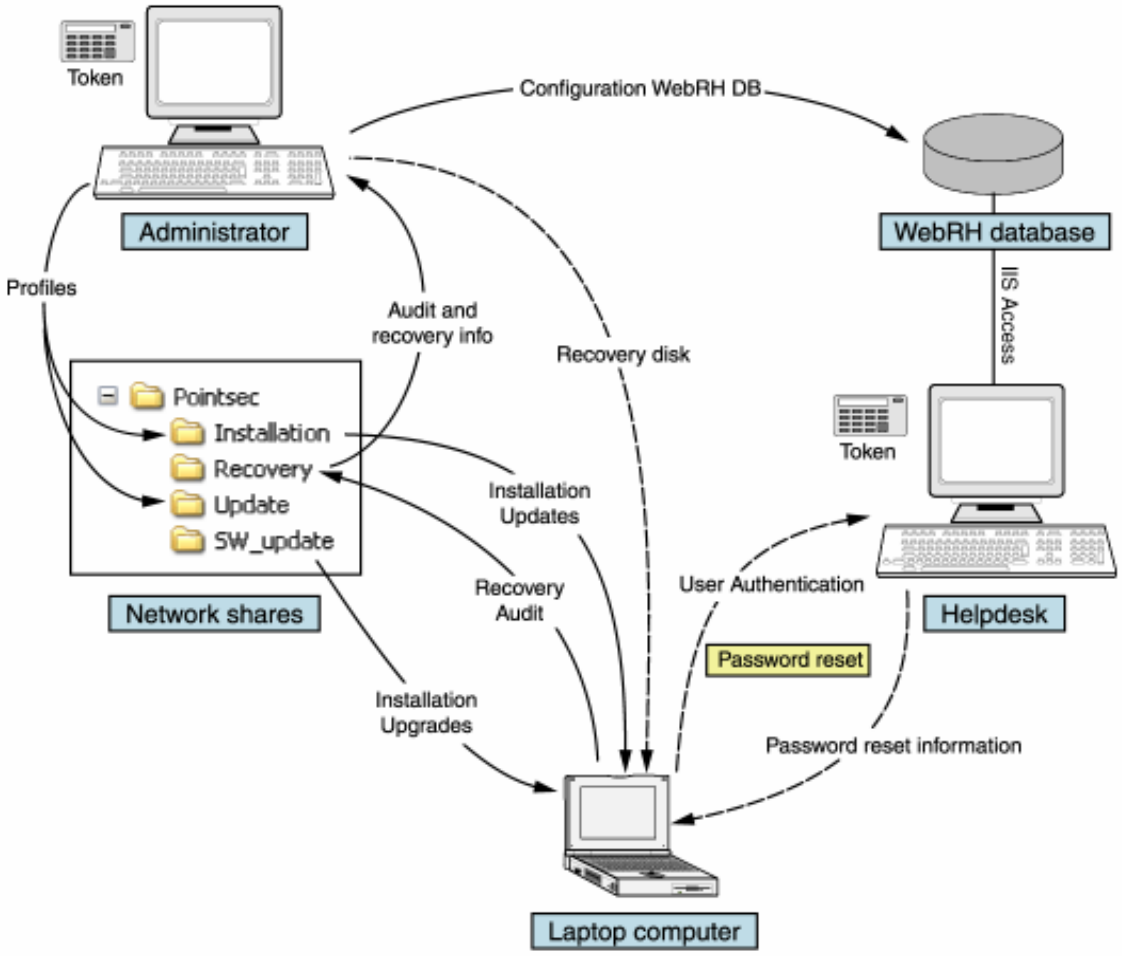
Pointsec Security Model



Pointsec – Full Disk Encryption Features

- Pointsec for PC is a Full Disk Encryption (FDE) product operating on a Full Volume Encryption (FVE) principle, therefore ensuring that all data stored on the laptop is encrypted
- Encryption is done at the Window's Filter Driver level and is seamless to the applications running on the laptop
- Any access to the laptop from a network connection will see the data in clear text
- Initial encryption of the hard drive averages about 15GB/hour and is done in the background as the user performs normal activity
- This process can be interrupted and will restart where it left off
- Pointsec will throttle the resources needed for initial encryption based on available CPU
- Additional overhead once the volumes are encrypted is negligible
- When a laptop goes into sleep mode or standby, initial volume encryption will stop

Pointsec Installation Model



Pointsec Installation – Key Considerations

- Pointsec administration requires the set up of the centralized file server as well as the creation of profiles for user configuration
- MSI installation, 10MB package
- Management of files will be in a flat hierarchy file share environment
- Each machine will act as an intelligent client that stores and gathers information to and from a centralized location while being transparent to the end user
- Unique key for each device that's created automatically at installation
- Information transferred between the client and the file share server is encapsulated in very small files which are approximately 10k-40K in size, and encrypted with the specified algorithm
- Administrators will be capable of managing security settings, update software versions, and view user logs from the central location
- To ensure recovery information is available to Help desk staff, it is essential that this directory be regularly backed up

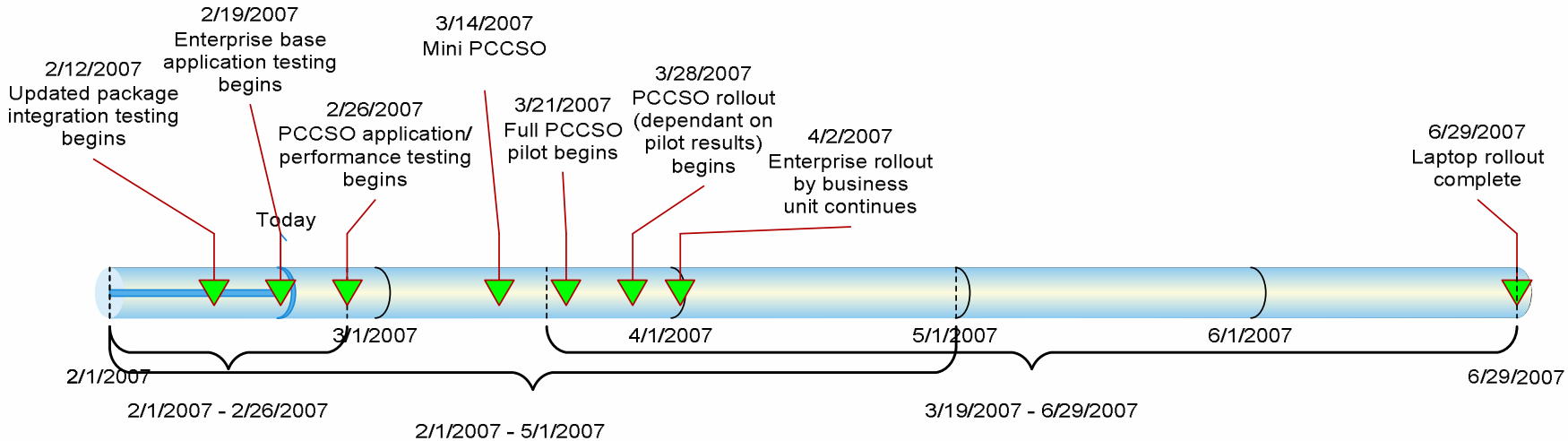
Laptop – Full Disk Encryption Deployment

- A pilot was completed successfully for over 60 users from Information Security, Internal Audit, Treasury & Planning, Privacy, Protection, Enterprise Technology, Enterprise Infrastructure, and Senior Officer Group
- The following Pointsec products were purchased by Allstate: Pointsec for PC, Pointsec Media Encryption (PME), and webRH
- Final pre-deployment enterprise testing was conducted to test product enhancements and updates requested by Allstate
- Allstate Claims organization was the first production rollout group

Laptop – Full Disk Encryption Deployment

- **Full disk encryption was first deployed to approximately 10,000 laptops in areas within the company identified as handling high value data**
  - Claims
  - Executive
  - Agency
  - Law & Regulation
  - Finance & Treasury
  - HR
  - Litigation
  - Investments
- **Full disk encryption is in the process of being deployed to all Allstate owned and managed laptops running latest base image, approximately18,500 laptops**
- **Laptops running earlier base image and Desktops, an approximate total of 70,000 machines, will be addressed this year**

Laptop – Full Disk Encryption Timeline



Testing/Integration:

- ☐ Test the latest update with the Build process
- ☐ Test the latest update with the Break/Fix process
- ☐ Test the latest update with the delta process
- ☐ Retest the Pointsec product with the base OS
- ☐ Retest the Pointsec product with the base applications
- ☐ Determine deployment methodology

Rollout planning:

- ☐ Identify target business units
- ☐ Identify target laptops
- ☐ Coordinate testing with business units
- ☐ Business unit IO testing
- ☐ Determine rollout schedule
- ☐ Create support processes for rollout support
- ☐ Create rollout communications plan

Product Rollout:

- ☐ Execute rollout communications plan
- ☐ Rollout product
- ☐ Support rollout
- ☐ Monitor rollout
- ☐ Review rollout results

Allstate
You're in good hands.

Lessons Learned

- **Timely and beneficial technology**
  - Laptop encryption capability has provided increased assurance and has reduced the risk associated with laptop loss or compromise
- **Three suggestions**
  - Establish clear data protection goals, criteria and policies particularly for encryption and key management
  - Establish a communications plan for systematic and smooth deployment of encryption software
  - Do your homework on vendor capabilities versus organizational needs
- **Most significant lesson: Rapid pilot to production deployments are possible when requirements are clear and there is clear alignment of technology strategy and management objectives**