Local Data Protection (LDP)

A Case Study
Laptop Encryption

Eric V. Leighninger
Chief Security Architect
Allstate Insurance Company
Agenda

• Allstate and Information Security – A Snapshot View
• Laptop Encryption – Goals, Expectations, Priorities
• Technology Acquisition – Vendor Selection Process
• Vendor Solution Deployment
• Lessons Learned
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
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
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
## Encryption Solution Selection Criteria

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

Unprotected
 Boot files

| MBR | BS |

Highly sensitive files
 System Files (PW-Swap etc)

| Operating System |
| System Files (PW-Swap etc) |

User Data

Data

File Encryption / PKI / Partial Solutions

| MBR | BS |

| Operating System |
| System Files (PW-Swap etc) |

Data

pointsec

| MBR | Mod BS |

| Pointsec Authentication |
| Operating System |
| System Files (PW-Swap etc) |

Data

Open Information

Secured Information

Access Control
**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, approximately 18,500 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

- 2/1/2007: Testing/Integration begins
  - Updated package integration testing begins
  - PCCSO application/performance testing begins
  - Testing the latest update with the Build process
  - Testing the latest update with the Break/Fix process
  - Testing 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
- 3/14/2007: Mini PCCSO
- 3/21/2007: Full PCCSO pilot begins
- 3/28/2007: PCCSO rollout (dependant on pilot results) begins
- 4/2/2007: Enterprise rollout by business unit continues
- 6/29/2007: Laptop rollout complete

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
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**