Protecting Confidential Data: The Role of Tape Encryption

Heidi Biggar
Analyst
Enterprise Strategy Group

November 15, 2007
Agenda

• Tape encryption circa pre-/post-Breach era
• Change agents
  – Statistics
• Confidential data
• Technology evolution
  – Today’s encryption market
  – Options
  – Impediments
  – Key management
• LTO-4 encryption
  – Key management
  – Recap
• Summary
Does your company encrypt data as it is backed up to tape? (percent of storage professionals, N = 388)

- No: 60%
- Yes, always: 7%
- Yes, frequently: 9%
- Yes, but infrequently: 12%
- Don’t know: 12%
Does your organization encrypt or plan to encrypt data using tape backup encryption? (Percent of respondents, N = 227)

- Don't know, 24%
- Already deployed, 25%
- Plan to deploy within the next 12 months, 14%
- No plans to deploy, but interested, 21%
- No plans to deploy, 17%

Note: Figure reflects respondent interest in encryption approximately one year before tape drive encryption became available in the market.
Change Agents

• Regulatory compliance
  – Example: California Database Breach Act (CA SB1386)
  – Many, many more
• Publicly-disclosed breaches
  – Financial, banking, healthcare, other verticals
• Corporate governance
Scary Statistics

- Since 2000*
  - 70 data breach incidents involving lost/stolen tapes exposing at least 18 million records
  - 34% related to theft
  - 66% related to lost tapes
  - Largest breach
    - 3.9 million records exposed

*Source: Privacy Rights Clearinghouse (www.privacyrights.org)
Confidential Data

• ESG defines confidential data as information that can be categorized as follows:
  – Intellectual property
  – Information that is protected by government regulations
  – Non-public private information (NPPI)
  – Information that is protected by industry regulations
  – Information that is classified as company confidential or private
User Confidential Data Volumes

What percentage of your organization's total data would you consider confidential (Percent of respondents, N = 227)

- 8% of respondents said 1% to 10% of their data is confidential.
- 24% said 11% to 25% of their data is confidential.
- 17% said 26% to 50% of their data is confidential.
- 21% said 51% to 75% of their data is confidential.
- 26% said More than 75% of their data is confidential.
- 4% said they don't know. 

Copyright © 2007, The Enterprise Strategy Group, Inc.
Confidential Data Drivers

- Regulatory compliance-driven
  - 81% of users say that government regulations were the biggest motivator for protecting confidential information.
  - Motivator = disclosure laws

- Financial impact
Compliance Obligations

Number of regulatory compliance obligations (Percent of respondents, N = 227)

- None / don't know, 14%
- My organization must comply with 1 regulation, 29%
- My organization must comply with 2 regulations, 22%
- My organization must comply with 3 regulations, 11%
- My organization must comply with 4 or more regulations, 24%
Financial Impact

• Difficult to calculate – but can run companies in the millions of dollars

• Breakdown:
  – “Hard” costs
    • Correspondence-related cost, PR costs, fines, reparations
    • Data breach cost estimate
    • $25 to $150 per record
  – “Soft” costs
    • Damage to reputation
    • Loss of business/drop in stock price
  – Domino effect
    • Economic implications
    • Consumer Reports survey
Tape Loss/Theft Cost

Potential Cost of Data Breaches Related to Tape Loss/Theft, 2000 - 2007

Data breach @ $25 per lost record: $450,000,000
Data breach @ $150 per lost record: $2,700,000,000
Technology Evolution

- Performance Issue
- Scalability Issue
- Tape Encryption Ubiquity

2000 2003 2006
Market Realities

- Tape encryption penetration will grow over time
- Multiple solutions and technologies
- CIOs should prepare accordingly
  - Architectural approach
  - Key management
Implementing Encryption

• Where should encryption be done?
  – Application layer, database layer, system layer, or storage layer?
  – Tape encryption options (at the storage level):
    • With software
    • In the network on an appliance
    • In the library
    • In the tape drive
  – Users need to weigh options
What do you believe are the impediments-if any- to encrypting confidential data? (Percent of respondents, N = 227, multiple responses accepted)

- Performance implications: 64%
- Cost: 60%
- Concerns with key management: 37%
- Concerns regarding the implications of encryption on disaster recovery: 36%
- New programming required to add encryption capabilities into our applications: 32%
- We are concerned with using third-party tools for encryption: 8%
- I don't believe there are any major impediments: 6%
- Not familiar enough with encryption technology to answer this question: 5%
- Other: 4%

Source: ESG Research, 2006
Key Management

• “Fear factor” – the fear of the unknown
• What is key management?
  – The generation, exchange, storage, safeguarding, and use of encryption keys
  – Encryption key = long string of characters used to encrypt plain text into ciphertext and to decrypt
• Necessary evil
  – As data volumes grow, key management will become increasingly challenging
    • Applies to tape encryption as well as data encryption on laptops or desktop PCs
    • Need to back up
• Long-term answer
  – Centralized key management
Centralized Key Management

• Definition: Central control of key management for user-wide systems

• Idea is for on-board encryption products, such as LTO-4, to “hook” into this layer

• ESG Research:
  – 54% of users polled were either ‘extremely interested’ or ‘somewhat interested’ in centralized key management. Nearly one-fifth had already deployed one.

• Key management systems provided by a number of suppliers
LTO-4 Encryption

- Uses AES 256-bit industry standard encryption
- Done at the drive level
- Benefits:
  - Minimizes performance overhead
    - Virtually no impact to drive performance
  - Improves efficiency from a processing standpoint
    - Impact on “Time to DR”
  - TCO, maintenance, and training
    - Less “stuff” to buy, manage, and train IT staff on
  - Can compress then encrypt
    - Maximizes cartridge storage capacity
- Option with LTO-4 drives
  - Same drive can encrypt or write standard data
# LTO-4 Recap

<table>
<thead>
<tr>
<th>Feature</th>
<th>Benefit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encryption done in hardware</td>
<td>Minimizes performance overhead. Virtually no degradation to tape drive performance.</td>
</tr>
<tr>
<td></td>
<td>Helps avoid burden on servers. Less compute-intensive than software-based encryption alternatives</td>
</tr>
<tr>
<td>Encryption done at the tape drive level</td>
<td>Allows for more efficient processing since processing is done offline.</td>
</tr>
<tr>
<td></td>
<td>Can reduce “Time to DR” (versus in-line approaches).</td>
</tr>
<tr>
<td></td>
<td>Reduces the amount of hardware that needs to be purchased, managed and maintained. No need for separate encryption appliance.</td>
</tr>
<tr>
<td></td>
<td>Allows data to be compressed first and then encrypted, which helps maximize cartridge capacity.</td>
</tr>
<tr>
<td>Uses LTO-4 standard or WORM cartridges</td>
<td>Flexible support, depending on user environment (e.g., regulatory/corporate governance requirements).</td>
</tr>
</tbody>
</table>
Summary

• Confidential data is growing by leaps and bounds
• A breach of confidential data could be costly
• Customers need to secure data
• LTO-4 tape drive encryption
  – AES industry standard
  – Fast, transparent
  – Flexible
  – Variety of providers
  – Cost-effective

*ESG believes tape encryption with LTO-4 products has the potential to become ubiquitous.*
Q & A

Visit [www.ultrium.com/whitepaper](http://www.ultrium.com/whitepaper) for a copy of ESG’s paper on this topic.

Slides from this presentation will be available on [www.ultrium.com](http://www.ultrium.com)

Replays of the webinar will be available at:
http://go.techtarget.com/r/2515860/5392818