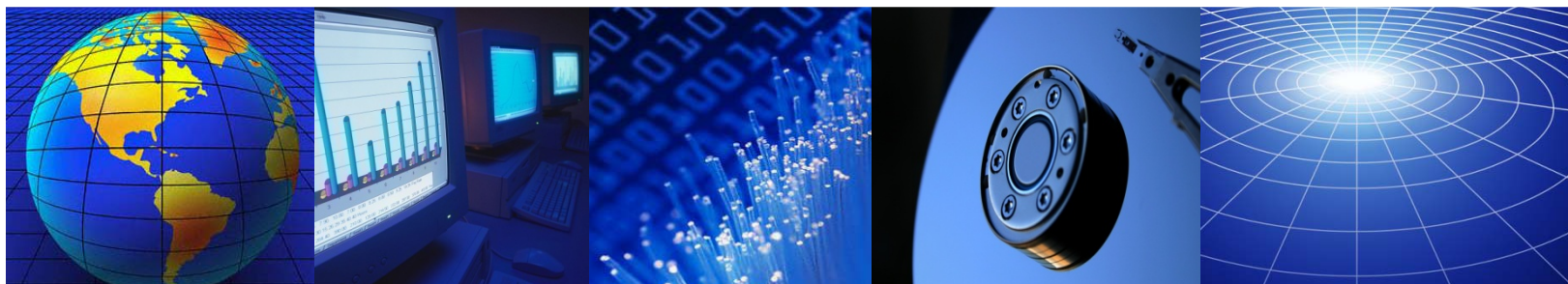




Protecting Confidential Data: The Role of Tape Encryption



Heidi Biggar
Analyst
Enterprise Strategy Group

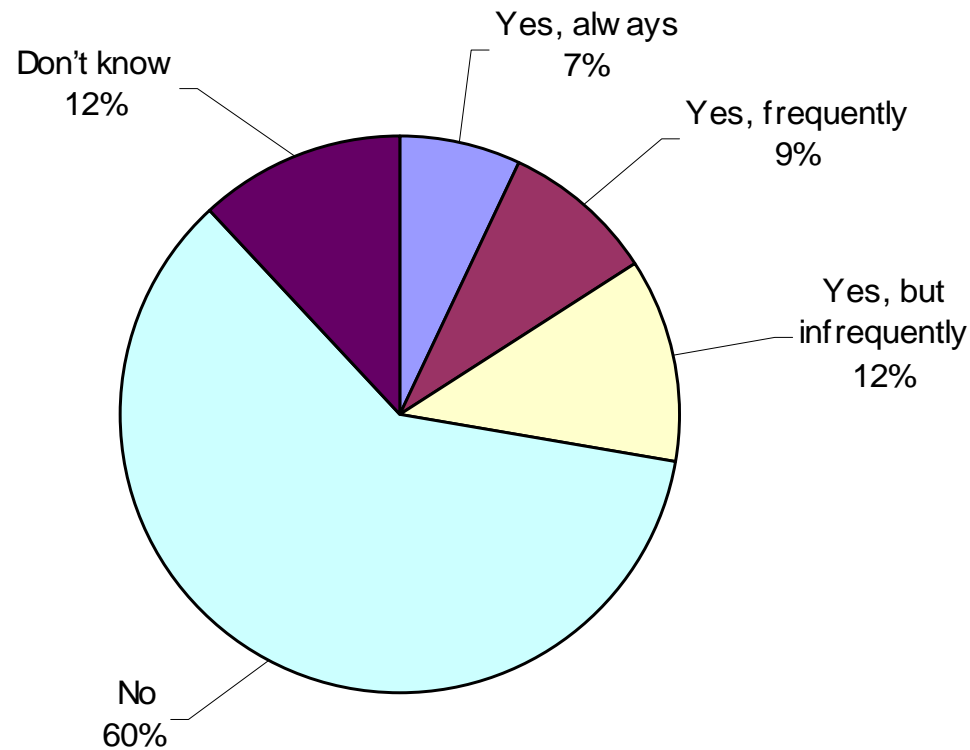
November 15, 2007

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

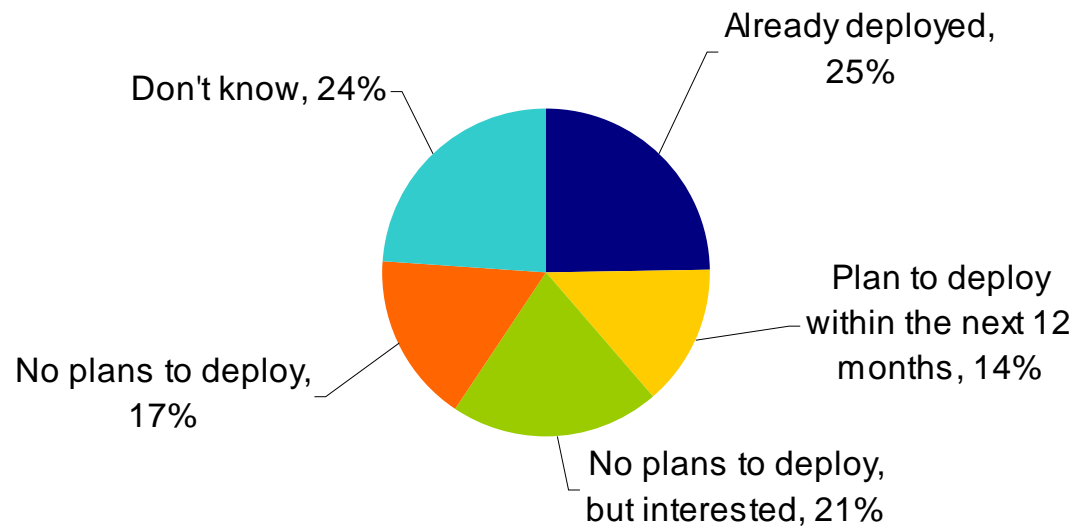
Tape Encryption Circa 2004

Does your company encrypt data as it is backed up to tape?
(percent of storage professionals, N = 388)



Tape Encryption Circa 2006

Does your organization encrypt or plan to encrypt data using tape backup encryption? (Percent of respondents, N = 227)



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

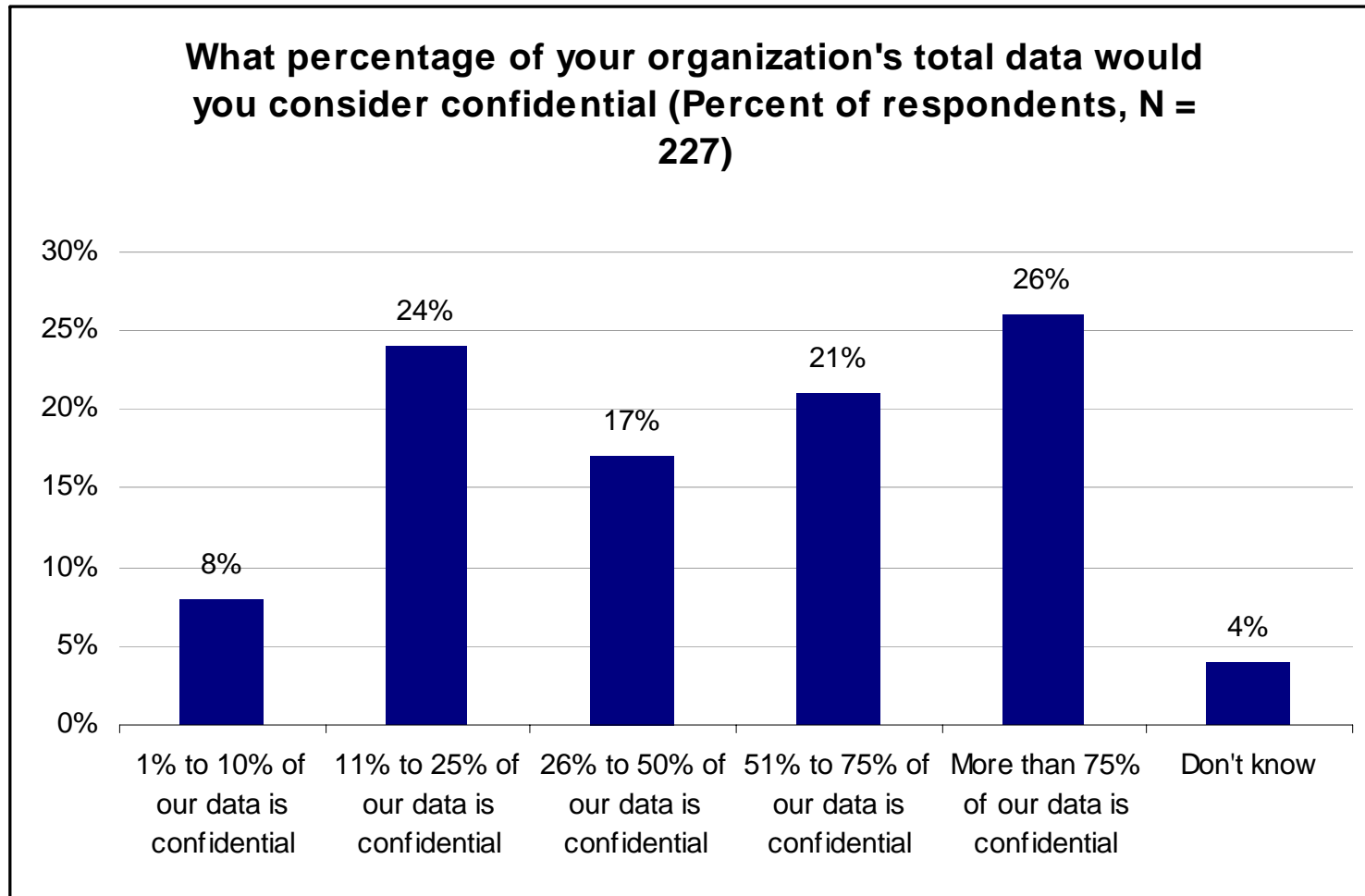
- Since 2000*
 - 70 data breach incidents involving lost/stolen tapes exposing at least 18 million records
 - 34% related to theft
 - 66% related to lost tapes
 - Largest breach
 - 3.9 million records exposed

*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

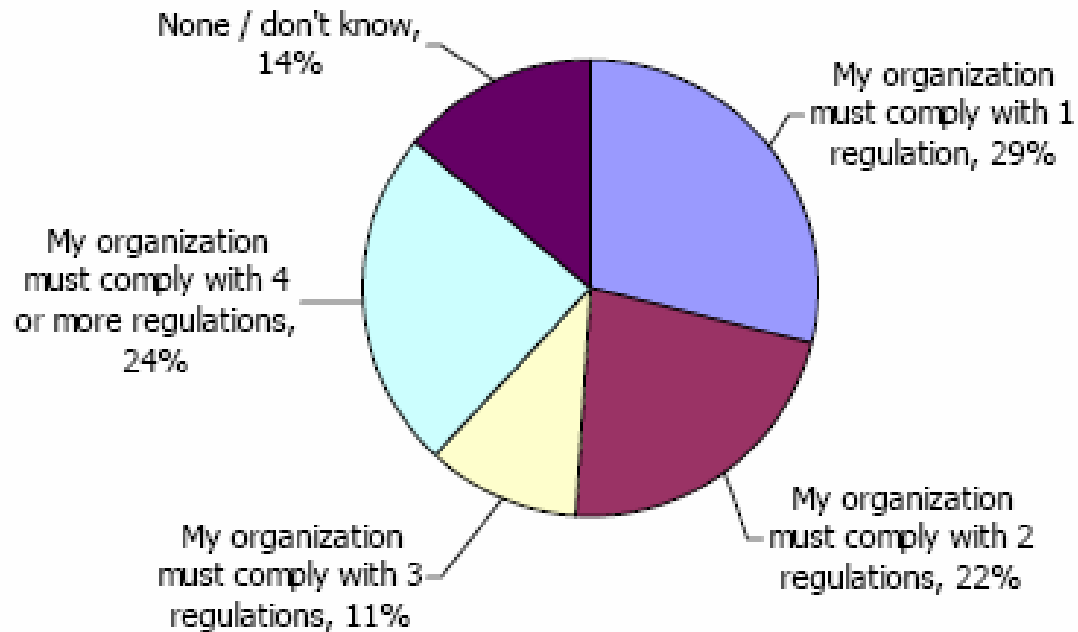


Confidential Data Drivers

- 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

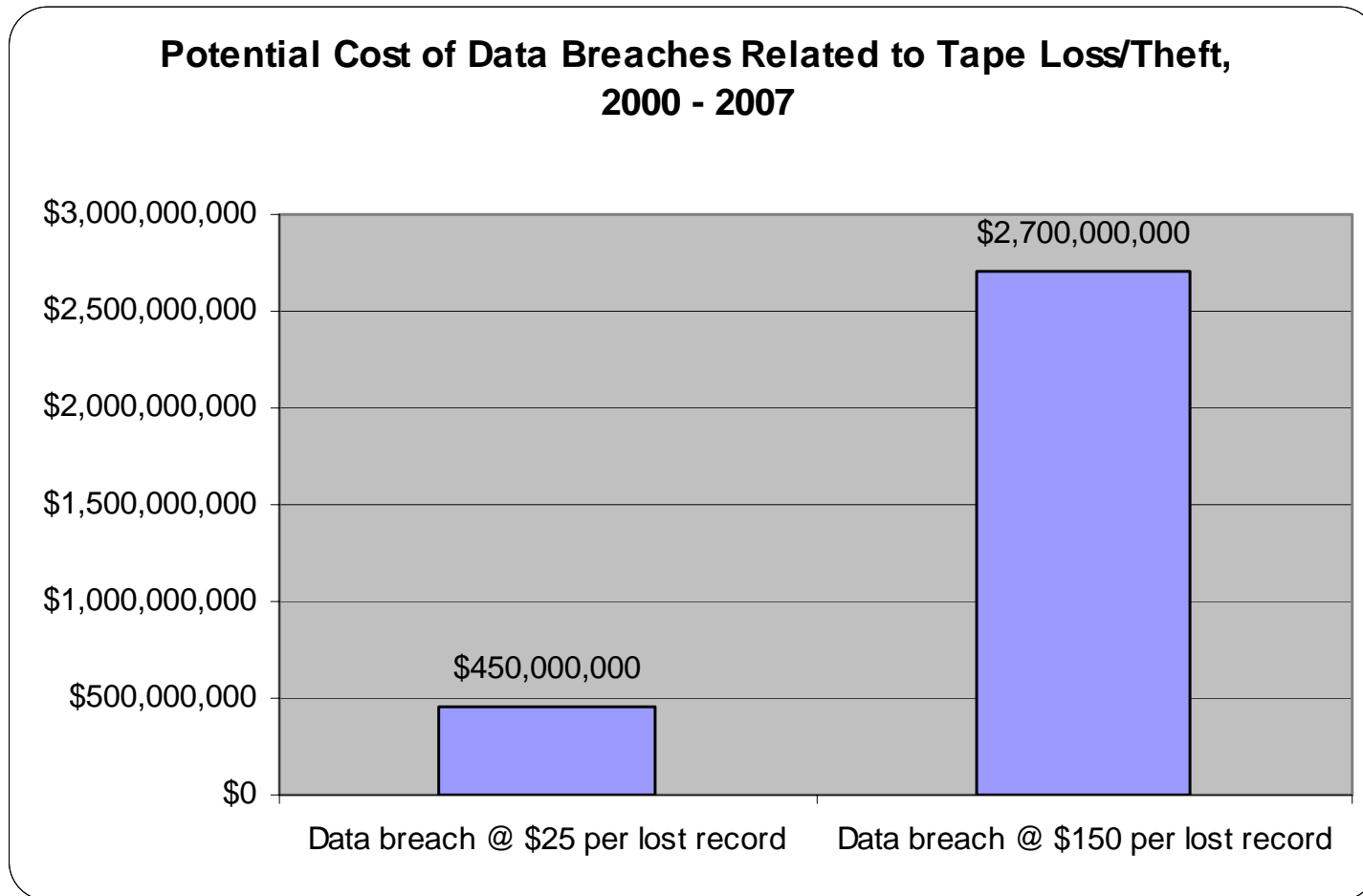
Number of regulatory compliance obligations (Percent of respondents, N = 227)



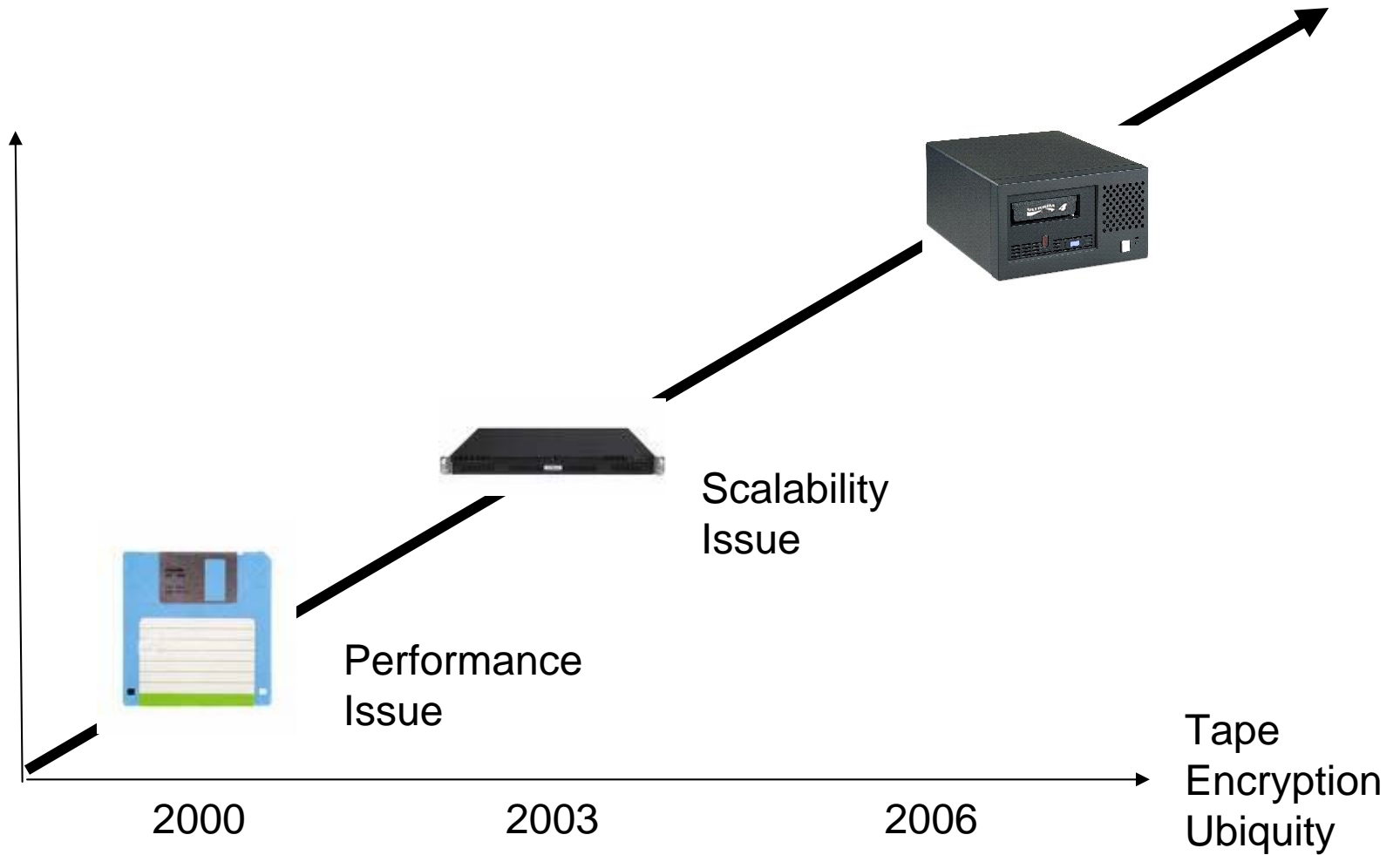
Financial Impact

- 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



Technology Evolution



Market Realities

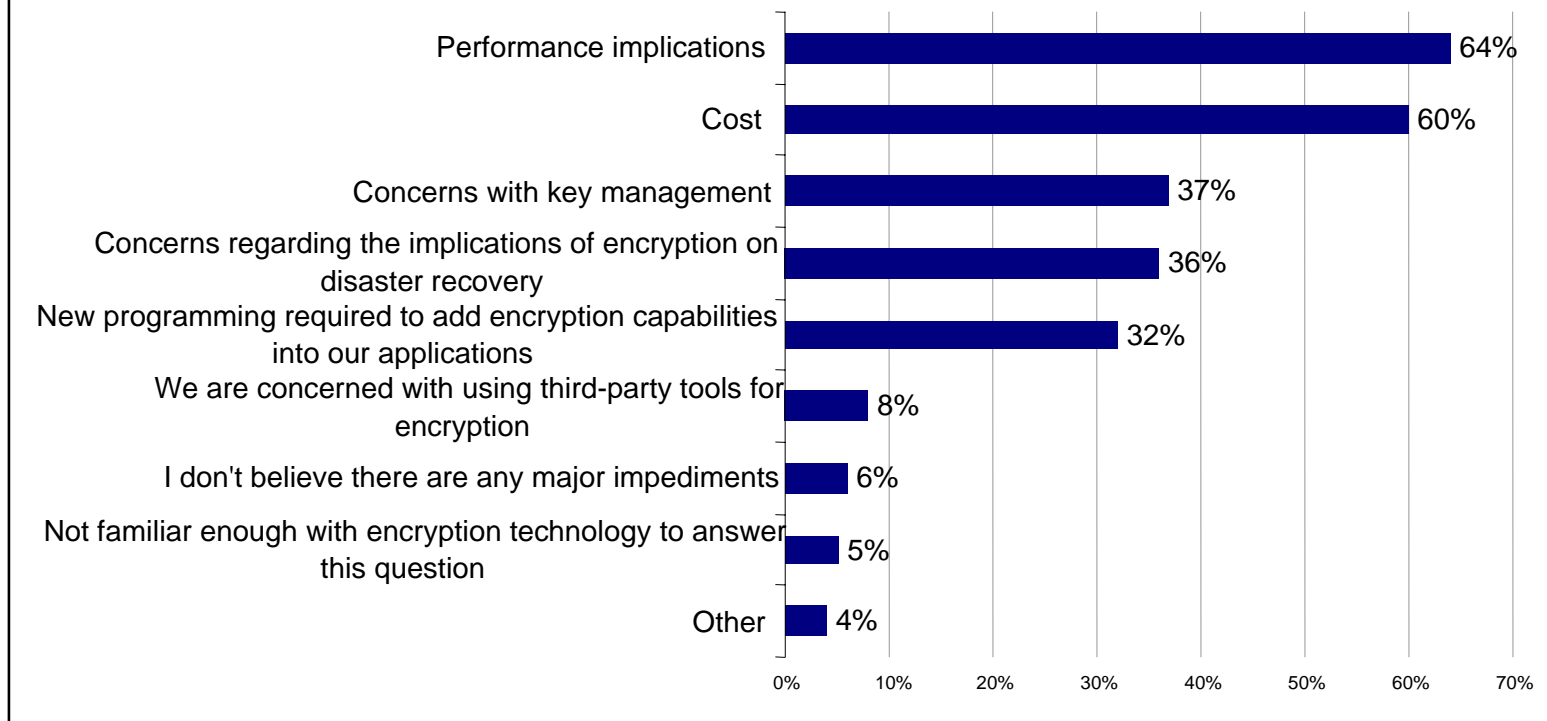
- Tape encryption penetration will grow over time
- Multiple solutions and technologies
- CIOs should prepare accordingly
 - Architectural approach
 - Key management

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

Adoption Impediments

What do you believe are the impediments-if any- to encrypting confidential data? (Percent of respondents, N = 227, multiple responses accepted)



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

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

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
for a copy of ESG's paper on this topic.

Slides from this presentation will be available on
www.ultrium.com

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