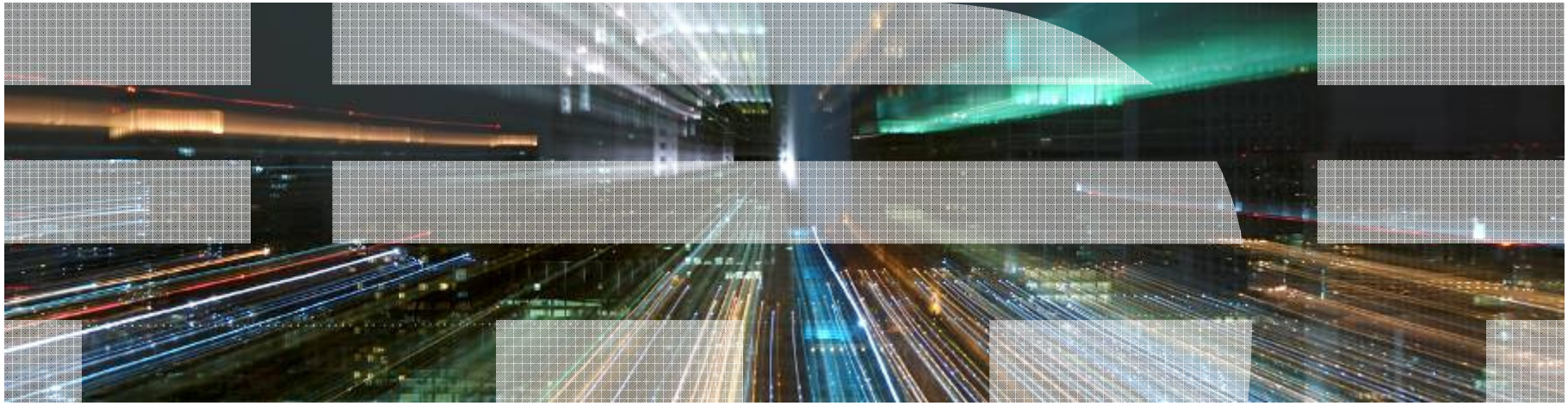
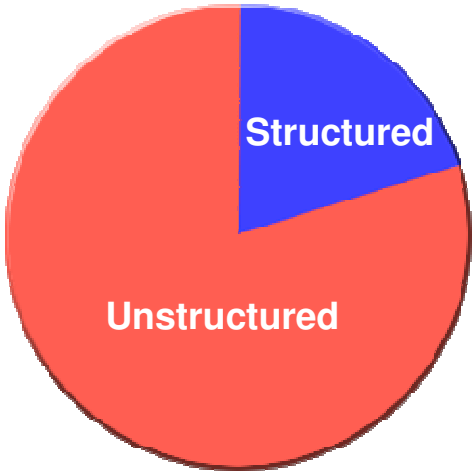
Gordon Arnold - Senior Technical Staff, Tivoli
04/22/2009

Storage Security Best Practices

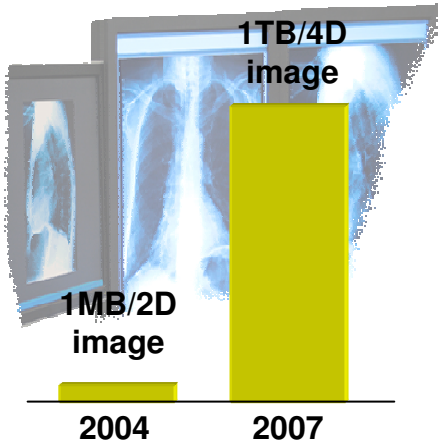


Information is Driving the Need for Infrastructure Transformation

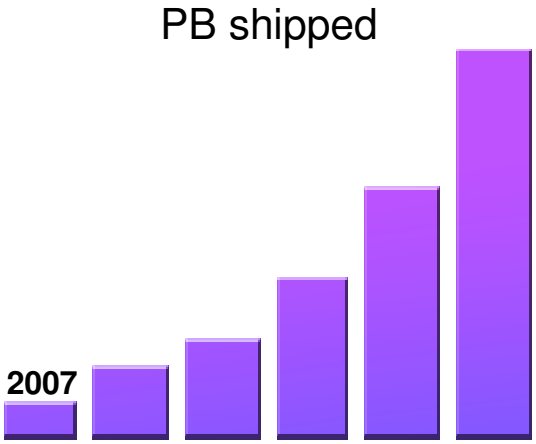
Data Types



Data Value



Data Growth



Today

80% unstructured data

By 2010...

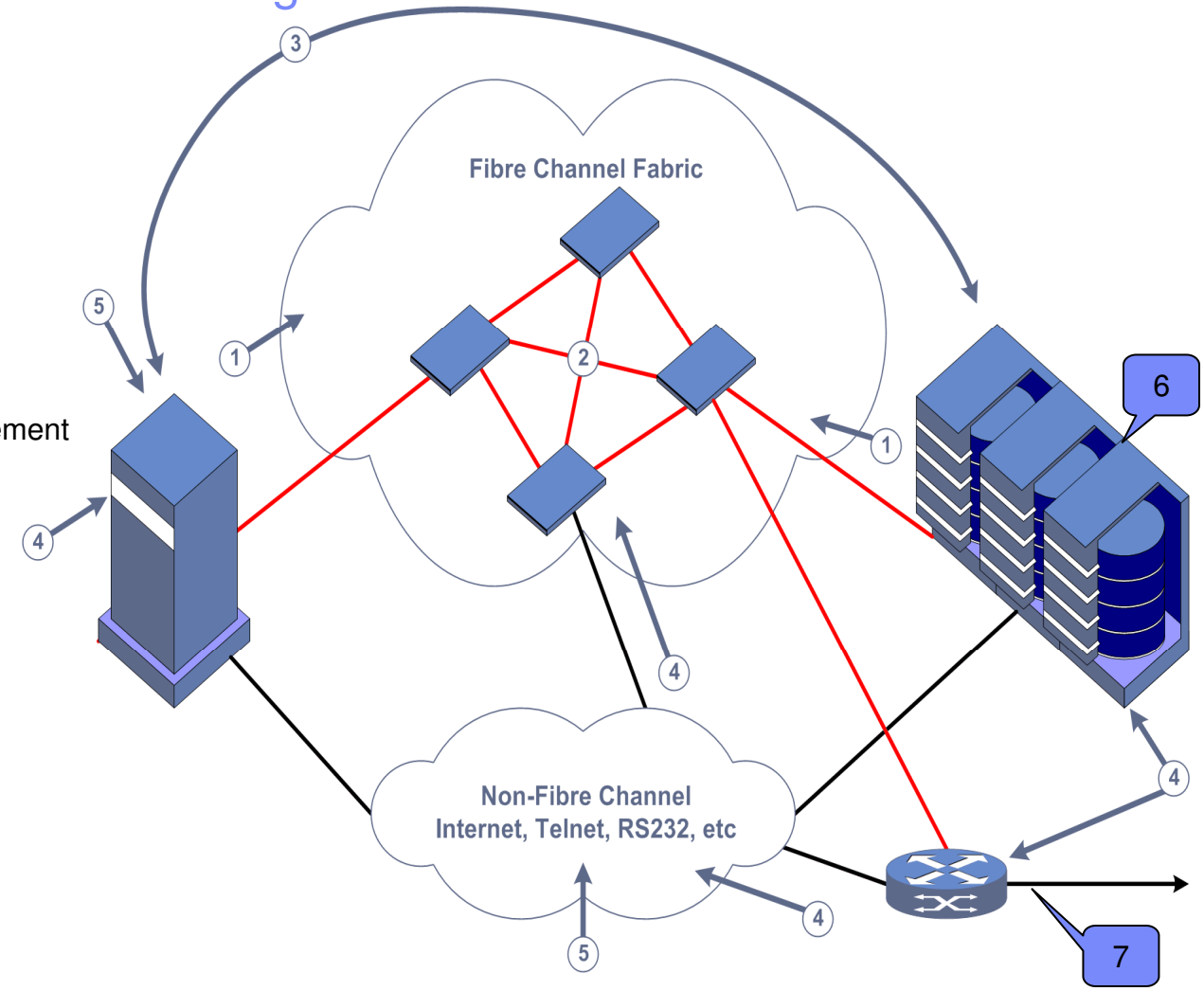
> 1000x storage per image

Through 2012...

54% annual storage growth

Storage Threats in Networked Storage

1. End device to network
2. Switch to Switch
3. Server to Storage Array
4. Management Interface
5. Denial of Service
   Hijacking
   Man-in-middle
   Spoofing
6. Loss of media or media replacement
7. Storage array replication



Why Encrypt Data-At-Rest?

- Co
  - 4(
  - Ne
  - PC
- Expo
- Data
  - Nea
  - The

And no

The Cost of Data Loss

- The impact of data loss is significant
  - Totaling $66.9M in 2007±
  - Average data breach costs a company $5M†
  - Average annual loss per company is $350,000 ±
  - Breaches costs companies an average of $185 per record
  - 327 data breaches were reported in 2006*
  - More than 100M data points exposed in 2006*
- Requirement for data privacy and encryption is becoming mandatory

±Computer Security Institute 2007

†Network World Magazine

**Source: privacyrights.org*

Information Risk

- Average cost of a privacy breach is around $200 per compromised record

Information Security

- 63% IT executives rate compliance with regulations a top challenge

Information Compliance

- Average legal discovery request can cost an organization from $150k to $250k

Information Retention

- Downtime costs can amount up to 16% of revenue in some industries

Information Availability

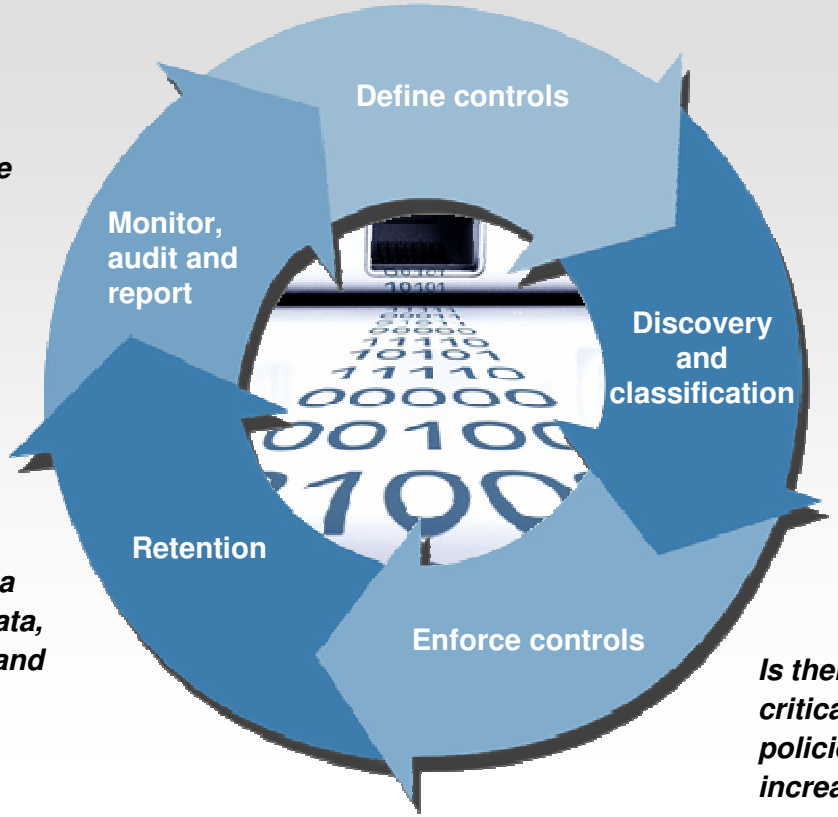
Sources: CIO Magazine survey 2007; IBM Tivoli Market needs and profiling study 2005;
The Costs of Enterprise Downtime: NA Vertical Markets 2005" Information Research; IBM Market Intelligence

Not an effective strategy…

Information Security Requires a Repeatable Process for Safeguarding Information

Over 80% of enterprise information is unstructured – requiring classification, protection and monitoring

Is there a way to streamline reporting and tracking information so I can easily sift through the false positives to target the real violations?



Do I have intellectual property, confidential records or personally identifiable information that violates policy or government regulations and/or is on the verge of being comprised?

Are there sophisticated ways to categorize my data, standardize my policies and manage my data protection issues?

How can I keep track of which data retention policy applies to what data, what data needs to be encrypted and how long I need to retain it?

Is there a way to share and guard critical data with manageable policies to mitigate against increasing internal threats?

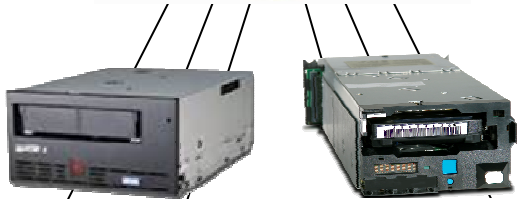
Our Response Is Self-Encrypting Storage for Securing Data At Rest

IBM Self-Encrypting Storage

- ***Why the Need for Encryption of data at rest?***
  - Datacenter tape and disk drives are all mobile
  - Lost data breaches are not just embarrassing but tremendously costly

- ***The industry's first self-encrypting tape drive***
  - IBM System Storage TS1100 tape drive family
  - IBM LTO Gen 4 drives offer encryption for open format
  - Standards-based Tivoli Key Lifecycle Manager

- ***Benefits***
  - Protect sensitive data when storage media are physically removed from secure data center
  - Self-encrypting media and key management enables simple deployment
    - Requires less planning and management
    - Saves time and money
  - Integration with z/OS security features for enterprise class security



Advanced, Software-based Encryption Key Management

Key management components

- Key store – customer choice of using existing key stores or installing new key stores, standards –based
- Key serving – transparent detection of media and assignment of keys
- Key management – backup and synchronization, life cycle, audit, and long term retention

Leverage existing high availability and disaster recovery configurations

- Fit with server management rather than introduce a separate appliance

Encryption built into the storage device

- No performance loss
- Transparent – no application changes
- Simple and secure key management

Multinational Financial Services Provider

IBM Information Infrastructure Improves Information Security

- *Security breached when Delivery service misplaced a box of tapes*
- *High cost to recover lost data*
- *Encryption overhead must not impact application performance*
- *High media costs*

Solution

- New Media Encryption Solution
- Total Solution components:
  - System z comprehensive key, policy and security management system
  - Hardware: 371 IBM TotalStorage 3592 Enterprise Tape Drives and 41 controllers, 10 IBM TotalStorage 3584 Ultrium UltraScalable Tape Libraries and 60 library expansion frames, IBM directors and new FICON channels

Result

- Reduced business risk; less security breach exposure
- Fast, reliable, 256-bit encryption
- Able to encrypt many tapes in parallel
- Able to compress before encryption, reducing media expenses

Large US-Based Healthcare Provider

IBM Information Infrastructure Improves Information Security

- *Needed to ensure security of storage media leaving the data center*
- *Solution needed to support mainframe and distributed platforms*
- *Required simple, secure encryption key management*
- *Needed reduced operational costs*

Solution

- TS3500 (3584) Tape Library
- TS1120 Model E05 Tape Drives w/ encryption
- IBM Encryption Key Manager (EKM)
- Tivoli Storage Manager
- IBM Services

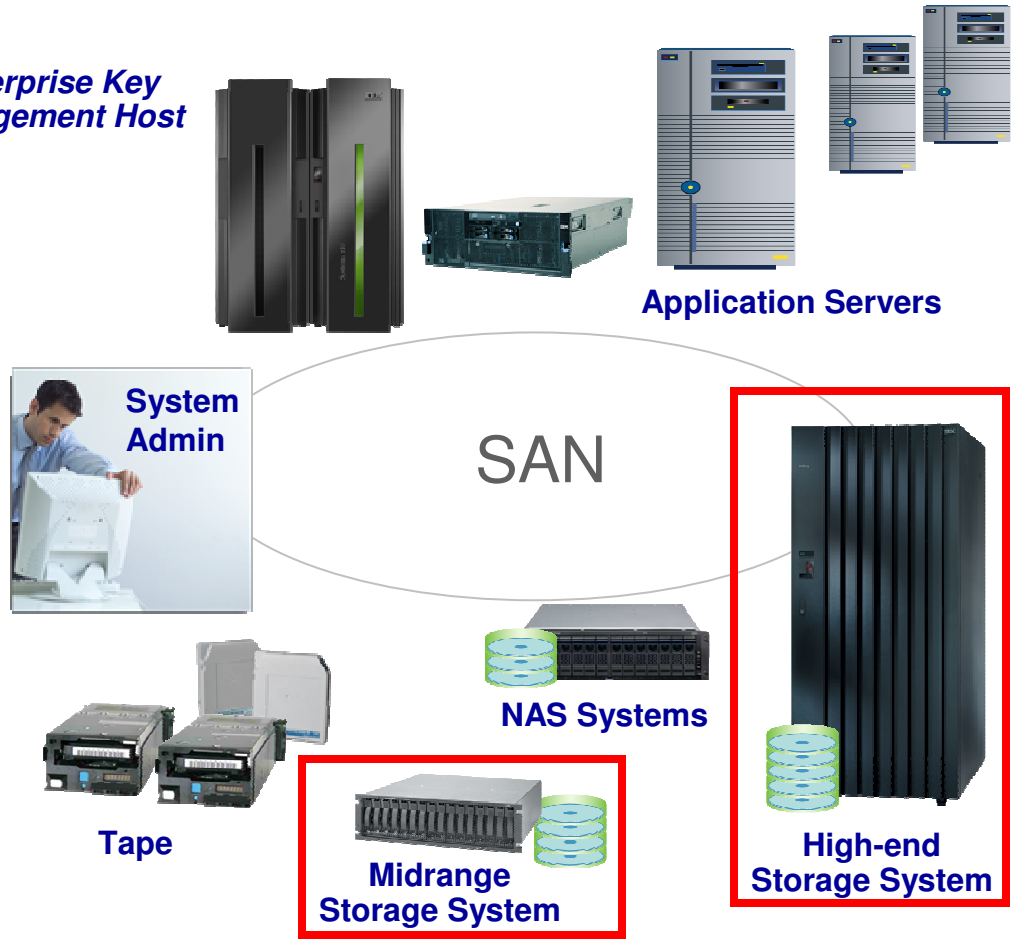
Result

- Secured critical customer information
- Reduced overall operational costs
- Improved compliance with industry regulations

Expanding from Tape to Disk Systems

IBM System Storage DS8000 series now offers Full Disk Encryption solution (DS5000 preview)

- ***Full disk encryption (FDE) drives***
  - Encrypt data-at-rest with embedded encryption key and password authentication
- ***Storage system***
  - Define secure volume groups, authenticate with the key source, and pass authentication key to the drive
- ***Key management service***
  - Uses same proven key management as TS1130 tape drive to easily and securely manage keys
- ***Standards for interoperability***
  - FDE management support via Trusted Computing Group security protocol
  - Working to create industry standards for the authentication key management protocol



IBM System Storage DS8000 series

Enterprise Disk for the World's Most Demanding Clients

- Performance, resiliency, and security to satisfy the world's most demanding clients
  - *Performance* – **Architected for highest total throughput**
  - *Availability* – **Designed for 24X7 environments**
  - *Resiliency* – **Outstanding Copy and Mirroring Capability**
  - *Security* – ***Full Disk Encryption and other security enhancements***
  - *Scalability* – **Up to 1024 TB physical capacity**

- **Built on 50+ years of enterprise class innovation**
  - Server/Storage Integration – POWER5™ Technology
  - Market share leader for System z environments
  - Exploitation of IBM Virtualization Engine™ Technology
  - IBM technology leadership and innovation

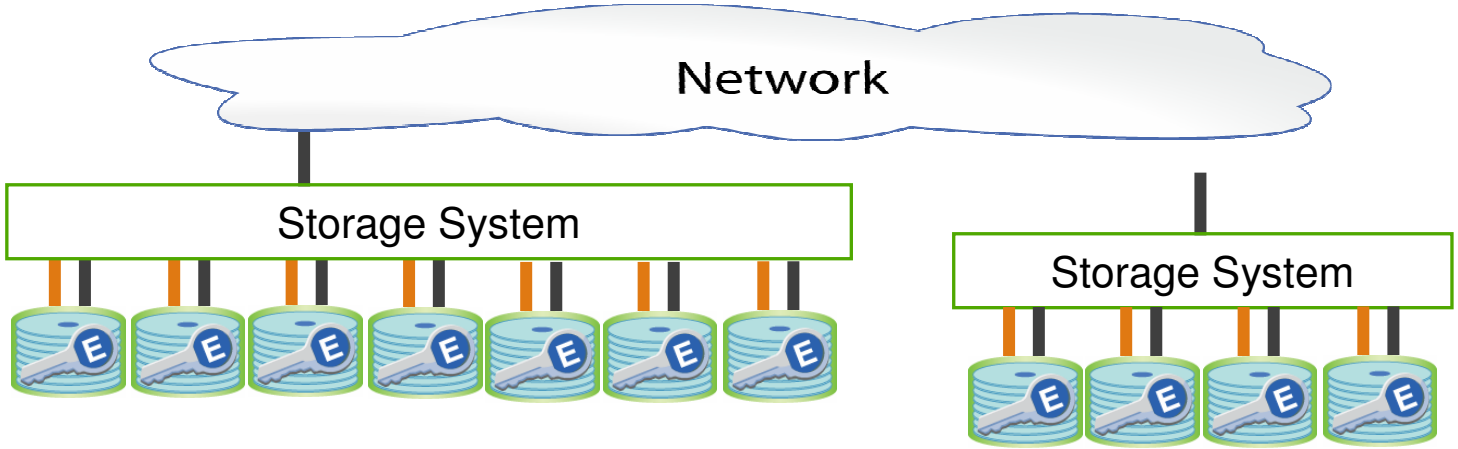
Like Tape, Self-Encrypting Drives Have No Performance Degradation

Encryption engine speed
Matches

Port's max speed

The encryption engine is in the controller ASIC

Scales Linearly, Automatically



All data can be encrypted, with no performance degradation
No need to classify which data to encrypt

Encryption Planning & Management Made Simple

IBM Self-Encrypting Storage and Key Management

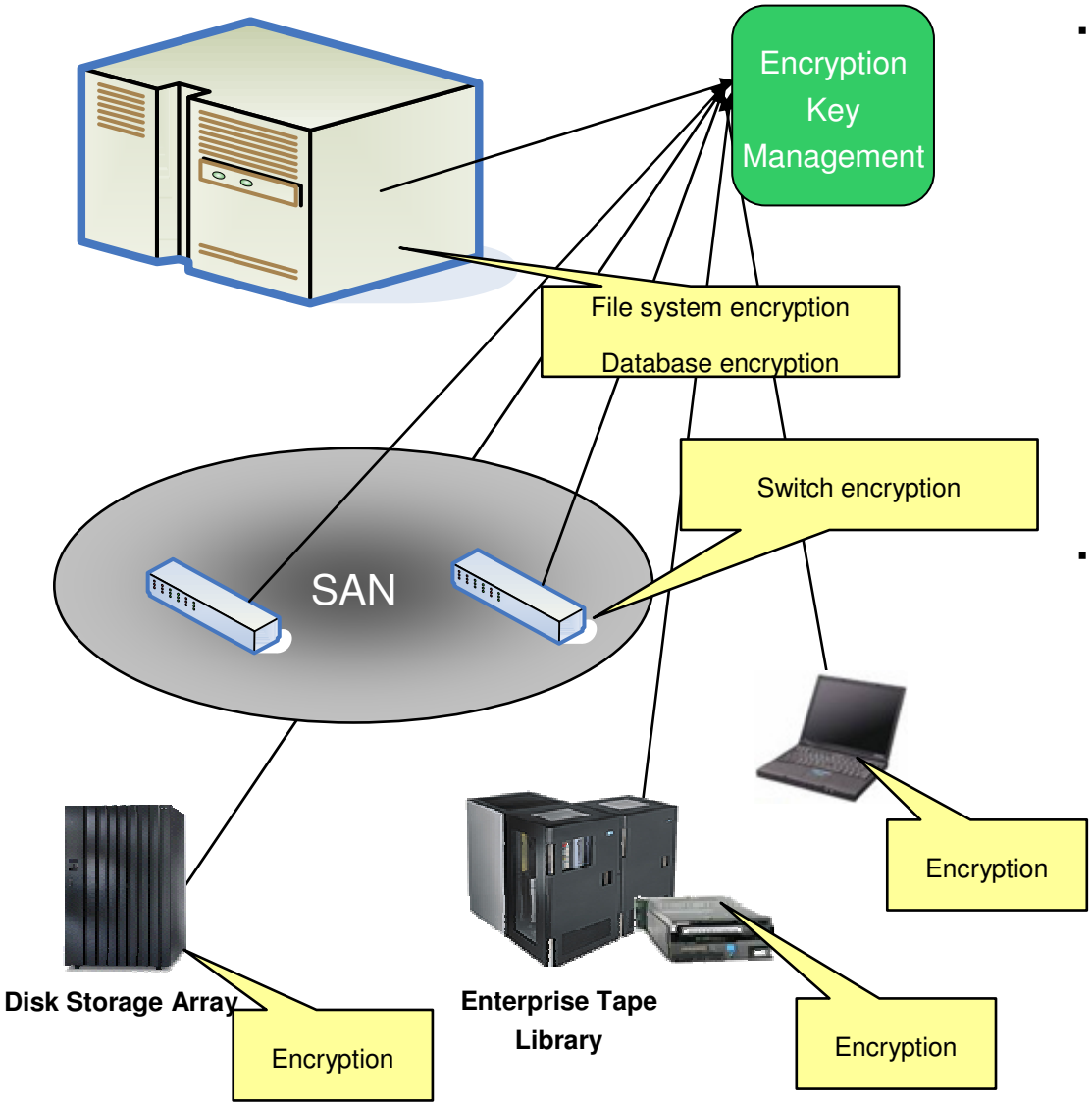
Less Planning and Management

- ✓ **Less Data Classification granularity needed**
- ✓ **No application changes are required Implementation doesn't require software chances and support**
- ✓ **Encryption is transparent to system administrators and end-users**
- ✓ **Much less complex to track keys and plan for data recovery**
- ✓ **Don't need to think about performance Performance automatically scales linearly**
- ✓ **Integrated in standard products Key Management and Key Stores software imbedded in pre-existing equipment, leveraging pre-existing backup protocols**

More Capabilities

- ✓ **Able to easily decommission drives with secure erase**
- ✓ **Able to easily repurpose drives securely**
- ✓ **Recovering from a disaster is much simpler since clients need only the pre-existing authentication keys and the pre-existing drive**
- ✓ **Drives can encrypt data that has been compressed and de-duplicated, which improves capacity utilization and reduces hardware costs**
- ✓ **Standard-based for optimal manageability and interoperability All of the major players are participating in standards**

View of the Future – Encryption Everywhere



- **Encryption choices – why should encryption be built into storage**
  - Performance – cryptography can be computationally intensive
  - Efficiency - encrypted data is not able to be compressed or de-duplicated
  - Security - Data in transit should use temporary keys, data at rest should have long term retention and robust management
  - Scalability – best to distribute cryptography across many devices
- **We started with encrypting tape systems, moving to encrypting storage arrays, with plans to extend to the rest of the infrastructure**

Why Wouldn't You Encrypt Data at Rest?

Customer Concern:

1. Performance
   - Encryption that isn't built into the storage infrastructure could cause serious performance penalties
2. Potential to Lose data
   - If you encrypt the data and lose the key then the data is lost
3. Complexity
   - Some solutions add extra boxes on the wire, classification, constant configuration, application changes
4. Total cost of ownership
   - Some solutions can double the cost of the storage solution

IBM's Response:

Our encrypting storage solutions have an impact on performance that is less than 1%

Our key management is proven with thousands of customers today

Our solution is simple to install, configure, with no application or server changes required

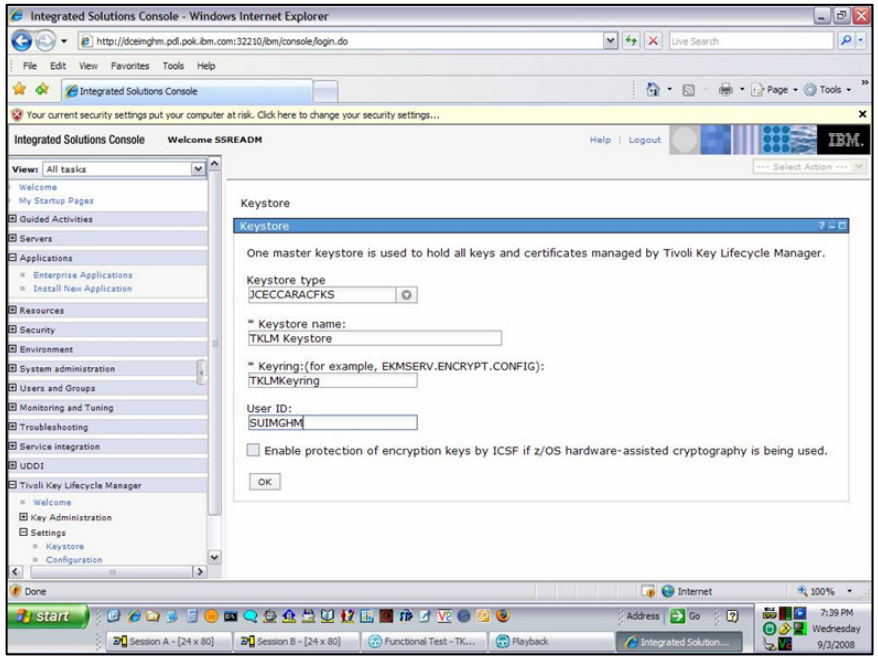
Our Encryption and key management adds small incremental cost

Our solution is high performance, robust, safe, simple, and cost effective

IBM Tivoli Key Lifecycle Manager v.1.0

- Focused on device key serving
  - IBM encrypting tape – TS1120, TS1130, LTO gen 4
  - IBM encrypting disk (when available)
  - Client reference implementation
- Lifecycle functions
  - Notification of certificate expiry
  - Automated rotation of certificates
  - Automated rotation of groups of keys
- Designed to be Easy to use
  - Provide a Graphical User Interface
    - Initial configuration wizards
- Easy backup and restore of TKLM files
  - One button operation
- Installer to simplify installation experience
  - Simple to use install for Windows, Linux, AIX, Solaris
  - Can be silent install

- Platforms for V1
  - AIX 5.3, 6.1 64 bit
  - Red Hat AS 4.0 x86 - 32 bit and 64 bit
  - Suse Linux 9.0 and 10 x86 - 32 bit and 64 bit
  - Solaris 10 Sparc -64 bit.
  - Windows Server 2003 - 32 bit.
  - Windows Server 2008 – 32 and 64 bit
  - z/OS 1.9



Lessons Learned

- Storage Security has to built into the infrastructure
  - Should fit into existing server management
  - Should leverage existing high availability and disaster recovery solutions
- Adding security has to be:
  - Simple
  - Transparent to existing applications
  - Cost effective
  - Leverage existing investments

Trademarks and disclaimers

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries./ Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both. Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both. IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce. ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office. UNIX is a registered trademark of The Open Group in the United States and other countries. Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both. Other company, product, or service names may be trademarks or service marks of others. Information is provided "AS IS" without warranty of any kind.

The customer examples described are presented as illustrations of how those customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics may vary by customer.

Information concerning non-IBM products was obtained from a supplier of these products, published announcement material, or other publicly available sources and does not constitute an endorsement of such products by IBM. Sources for non-IBM list prices and performance numbers are taken from publicly available information, including vendor announcements and vendor worldwide homepages. IBM has not tested these products and cannot confirm the accuracy of performance, capability, or any other claims related to non-IBM products. Questions on the capability of non-IBM products should be addressed to the supplier of those products.

All statements regarding IBM future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

Some information addresses anticipated future capabilities. Such information is not intended as a definitive statement of a commitment to specific levels of performance, function or delivery schedules with respect to any future products. Such commitments are only made in IBM product announcements. The information is presented here to communicate IBM's current investment and development activities as a good faith effort to help with our customers' future planning.

Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput or performance that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput or performance improvements equivalent to the ratios stated here.

Prices are suggested U.S. list prices and are subject to change without notice. Starting price may not include a hard drive, operating system or other features. Contact your IBM representative or Business Partner for the most current pricing in your geography.

Photographs shown may be engineering prototypes. Changes may be incorporated in production models.

Thank You for Joining Us today!

Go to **www.ibm.com/software/systemz** to:

- Replay this teleconference
- Replay previously broadcast teleconferences
- Register for upcoming events