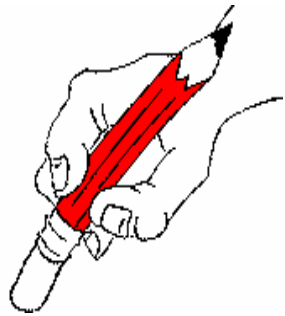




# What Storage Security Will Users Tolerate and What do they Need?

Tom Coughlin  
Coughlin Associates  
[www.tomcoughlin.com](http://www.tomcoughlin.com)



# Outline



- Security definition
- Data security trends and customer expectations
- Data erasure and data destruction
- Encryption
- Conclusions



# Security--Definitions

- 1) Freedom from danger, risk etc.
- 2) Freedom from care, apprehension, or doubt; well-founded confidence
- 3) Something that secures or makes safe; protection; defense
- 4) Precautions taken to guard against theft, sabotage, the stealing of military secrets, etc.

# Data security trends and customer expectations



# User Data Security Issues

- Laws protect user private data
- 1/3 of HDDs sold on eBay aren't erased
- Enterprise storage systems provide security
  - Until physical control of storage medium is lost
  - Examples are highly publicized losses of tapes in recent years
- RAID stripes aren't an answer
  - Transaction processing records often < 1 block
- Computers lost or stolen are usually easily broken into (see following slides)
- More and more devices are being networked with intrusion and data theft becoming more common
- How do you protect or eliminate multiple copies of data on different devices?
- These trends are becoming true in the home as well as in the enterprise

# Computers Lost and Stolen



**QUADRUPLE PROBLEM : LOSS OF INFORMATION  
LIABILITY / HARDWARE / SOFTWARE**

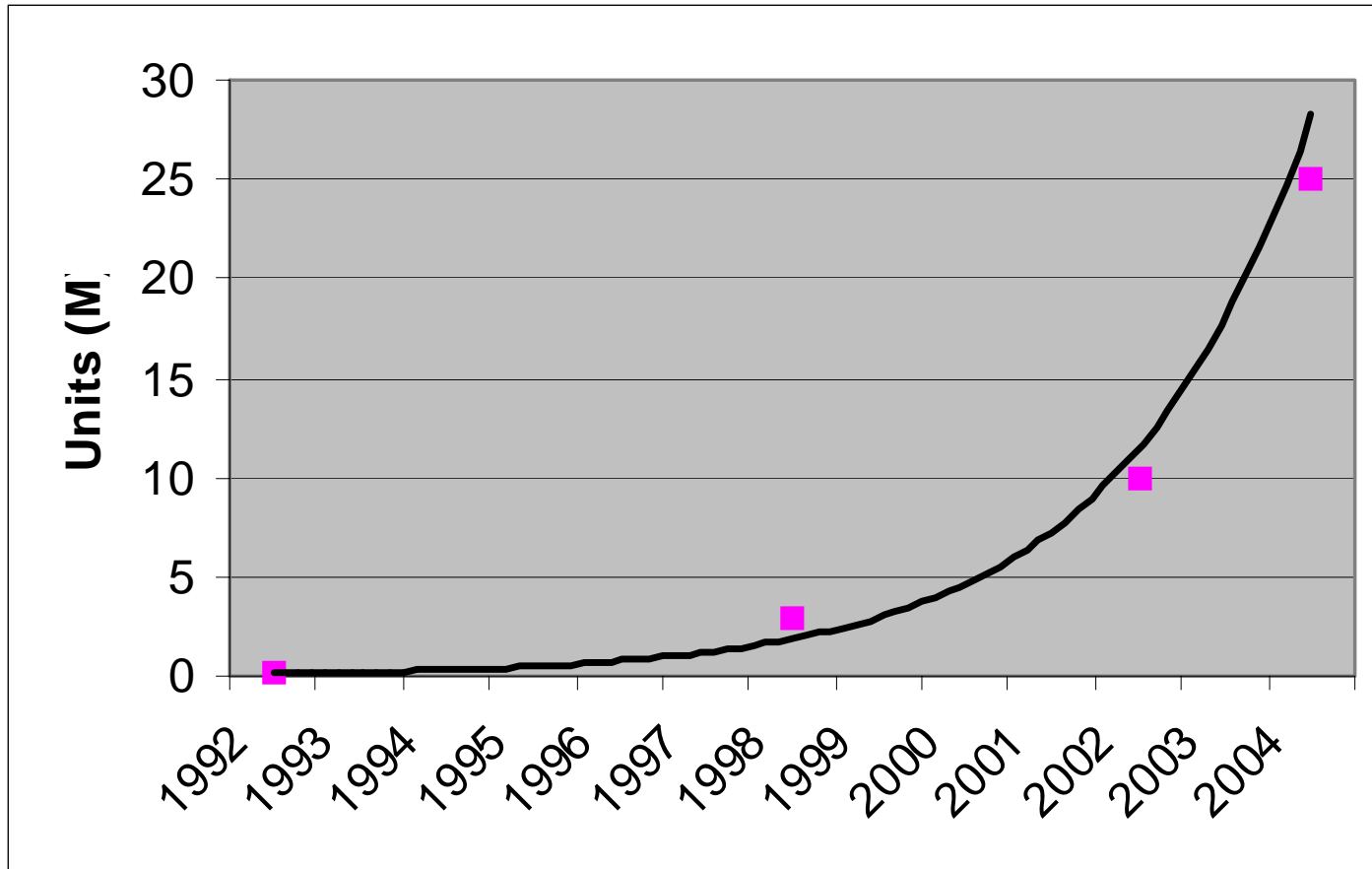
Source: zTrace Website

© 2006 Coughlin

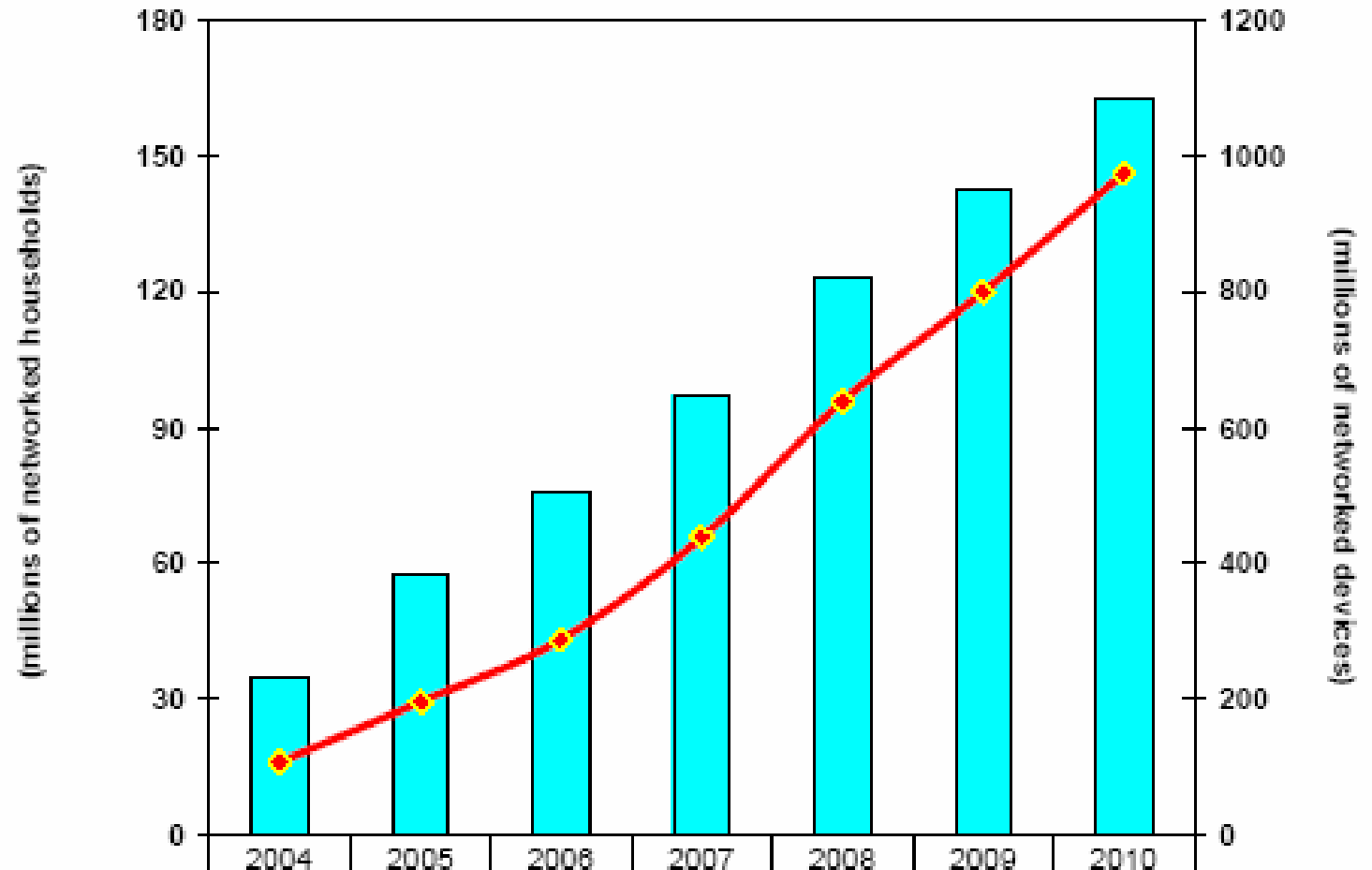
- **Statistics** show that **1 out of every 14 laptops is stolen**, and that **over 2,000 computers are stolen every day** in this country.
- A computer is **stolen every 43 seconds**
- Over 98% of stolen laptops are never recovered. (FBI)
- A survey of 769 corporate IT managers revealed that 64% had experienced laptop theft. (Tech Republic)



# Paper Shredder Projections

(Data in 1992 and 1998 from Royal)



# Global Home Network Deployment & Networked Devices



 # Networked Households (mil)	34.7	57.6	75.8	97.3	122.8	142.7	162.3
 # Connected Devices (mil)	107.6	195.8	288.0	437.9	638.6	799.1	973.8

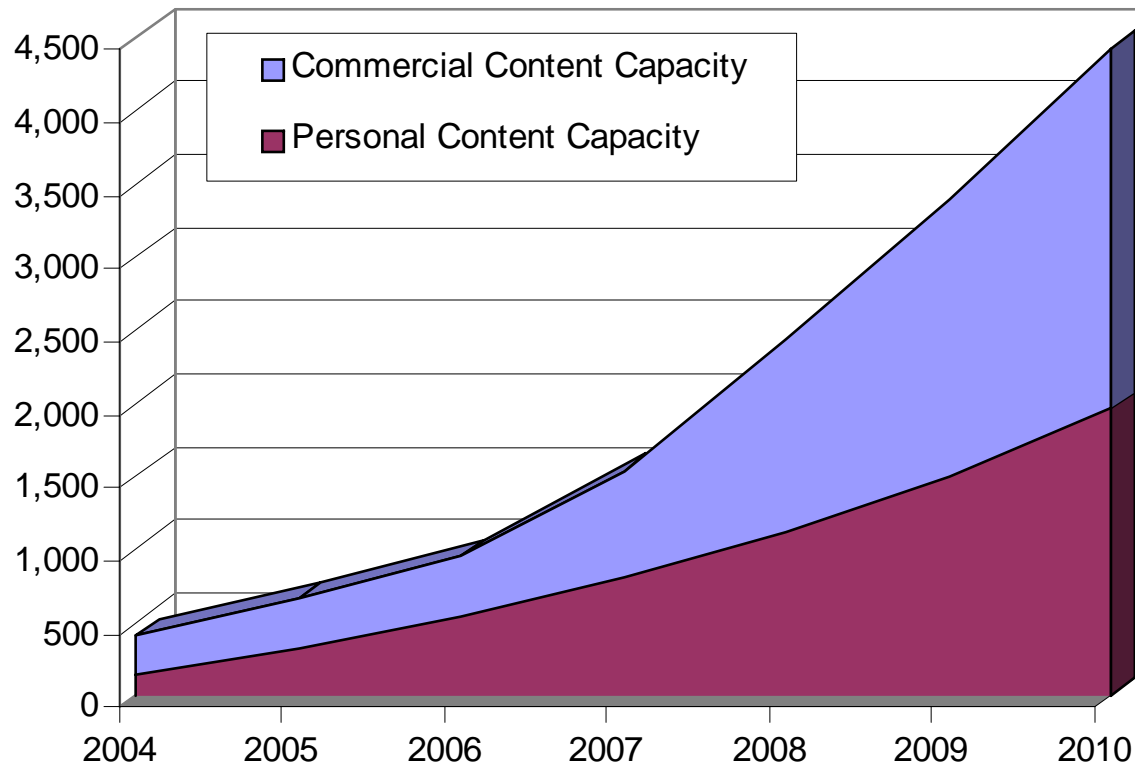
© 2005 TDG Research

© 2006 Coughlin Associates



# Cumulative Original-Instance Home Storage Capacity

Capacity (GB)



**Almost 5 TB of  
combined personal  
reference data and  
home commercial  
content  
by 2010**

# Higher Capacity Storage Products



PMR Hard  
Disk Drive



High Capacity  
Tape



Blu-Ray  
Disc



New External  
Storage



Next Generation  
SFF HDDs



Holographic  
Disc



New Flash  
Technology

# Consumer Products Using Digital Storage



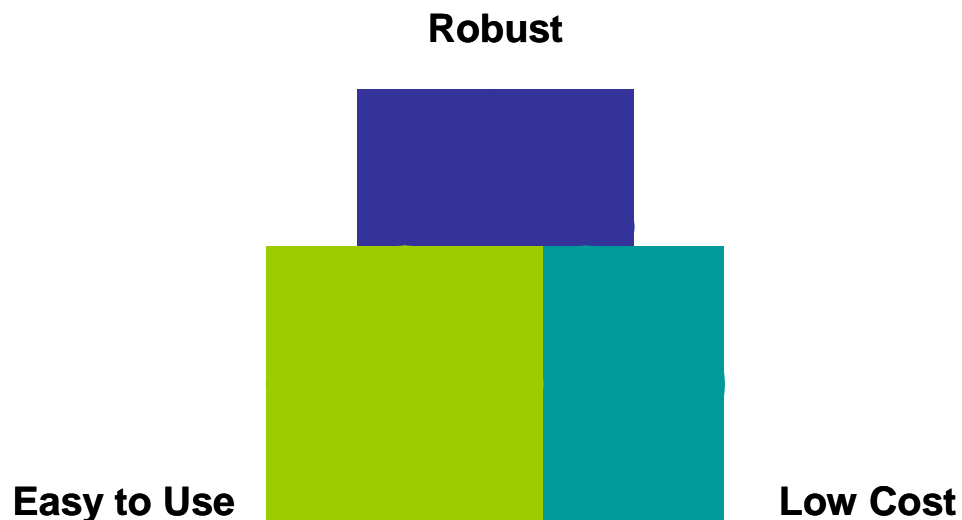
# Trends in the IT Industry

- Budget controls still relatively tight at many companies
- Storage demand is increasing for everything
- Greater regulatory requirements for long term data retention
- Greater concern by content owners for control of the use of their content
- More types of storage devices used for commercial and home purposes such as embedded disk drives, external disk drives, flash memory in many forms and optical disks.
- Fewer people are managing more storage
- Large numbers of older storage products, often containing recoverable data are being retired
- Greater numbers of non-technical people using storage products
- Greater expectations that storage should function like other common technologies (e.g. TVs, telephones or automobiles)

# Some forms of Storage Security

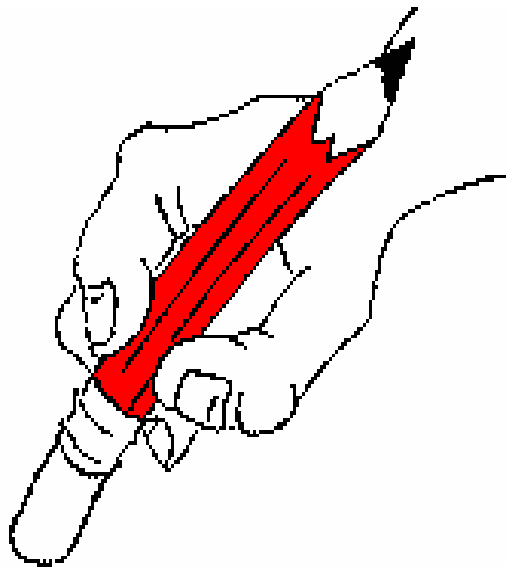
- Drive data erasure—drive still usable
  - Secure erase of all blocks of data on disk drive
    - Supported by all ATA disk drives
  - Single file erasure
- Drive destruction (e.g. Dead on Demand)
- Data transfer encryption (data is encrypted during transport)
  - Protection of data while in transport
- Drive encryption (data is encrypted on the storage device)
  - Access level dependent upon key or password used to decrypt the data

# General Requirements for a Storage System



- Customers will not be satisfied unless
  - The system is robust enough for normal use
  - Is easy to use and completes its intended operations in the time available and expected
  - The price and operating costs are deemed reasonable

# Data Erasure and Data Destruction



# Disk Erasure Technology

Type of Erasure	Average Time (100 GB)	Security	Comments
DoD 5220 Block Erase	Several Days	High	3 writes + verify, cannot erase reassigned blocks
Enhanced Secure Erase	Several Hours	High	LF Overwrites reassigned sectors, 2 off-track overwrites
Secure Erase	Less than an hour	Better	Low frequency overwrite of user accessible sectors
Fast Secure Erase	Minutes	Good	Drive is set to secure erase with a password and turned off, when turned on again secure erase must complete. Can be broken by sophisticated forensic techniques
Normal File Deletion	Minutes	Poor	Deletes only file entries, not the data itself



# Drive Secure Erase

- When HDDs sold on eBay, user data is sold as well
- File/folder delete or HDD reformat still leaves recoverable data
- This is true for enterprise storage as well as PC HDDs
- ATA & SATA HDDs have internal SE command
- SCSI and Fibre Channel drives have not implemented SE erase

# Classes of File Erasure

- 5 classes of single file and sensitive data erasure:
  - Class 1: File and all copies of a file are erased
  - Class 2: Including class 1 but also eliminating information that the erased files had been on the computer as well as all prior versions of the erased file
  - Class 3: Classes 1 & 2 but also erasure of all references to the erased file or sensitive information in other files
  - Class 4: Classes 1-3 but also eliminating any information on the drive showing that an erasure occurred
  - Class 5: Extension of Classes 1-4 into associated storage systems
- For all these file erasure classes the remaining data on the disk drive or storage system that was not erased should remain useable in the usual way
- Ideally this file level erasure should use the techniques developed for drive level security erase to ensure non-recoverability of the erased data

# Prior Work on File Level Erasure

- Several commercial programs are marketed to remove files from computers, including copies and evidence that the files existed
- As shown in a 2005 CMU study (Mathew Geiger) all of these programs have various defects in their file erasure effectiveness or their ability to remove traces of the existence of the erased file or that the file was erased
- CMU study of following programs
  - Cyberscrub
  - Window Washer
  - SecureClean
  - Evidence Eliminator
  - Windows & Internet Cleaner
  - Acronis Privary Expert



# Drive Destruction

**REMOTEY DESTROY  
HARD DRIVE DATA  
BEYOND  
FORENSIC RECOVERY**



- Quick and Dirty—Hammer and Screwdriver
- Long and torturous—Grind and Dissolve
- Fast chemical destruction of the disk media—perhaps multiple triggers
- In all cases the storage device is no longer usable—not retired but destroyed



# Encryption in Drives and in Transport

# Encryption of Storage Devices

- Does it slow down storage device data access noticeably?
- Is it invisible to the user?
- What happens when the user wants to migrate his data or upgrade his system?
- Does it get in the way of backup?
- Does it get in the way of common disk array approaches?

# Encryption of Transport

- Will it noticeably slow down data delivery?
- Will it be standardized so it can be recognized by heterogenous systems?
- Will it be robust and fault tolerant?
- How will it know that it is secure?
- Are there back doors through which content can be viewed?

# Data Security that Works?





# Passwords—An example of how not to do data security

- Who can remember all of them?
- To be effective they must be cryptic and changed often—very few people can keep track of such passwords
- In practice most password systems offer only token security since they must allow folks to use passwords that they can remember such as a date or name

# DRM—An example of how not to do data security

- Digital Rights Management (DRM) is a form of security for content sold to customers to prevent unauthorized copying of content
- In practice DRM has stood in the way of making technology and content access more wide-spread and hence has limited the potential market for selling content
- If it does not include some reasonably acceptable “fair use” or if it is used to prop up unreasonable prices (as perceived by the customers) it helps create a vast underground market for “stolen” content
- Case in point: Sony DVDs and the rootkits problem
  - customers didn’t get the usage they expected and
  - DRM scheme may have left their systems vulnerable to attack)

# Do customers want data security?

- Maybe yes, but not if it takes too much time or cuts down on their performance or enjoyment of life
- Data security may be perceived like buying life insurance, taking bitter medicine or making a will--a good idea but somehow not very pleasant to think about and thus often put off
- How will customers know if it works until it is too late?

# Some ideas on how to do data security that people can use

- Sell positive rather than negative
  - E.g. sell content exclusivity rather than content protection
  - Sell security as part of a better performance package
- A challenge: Can data security be combined with better overall system performance?
  - My computer/PDA/toaster etc. is used to me and the way that I work and always works better for me than for others that use it or attempt to use it—it protects others from my personal stuff
- Can data security be based on idiosyncratic principles (recognizing characteristics that make you—you?)
  - Biometric recognition could be part of this and if it works well should be easy to use
  - Shouldn't our digital devices pay attention to how we do things and couldn't these individual usage characteristics be part of system security and access

# Cautions for implementation of data security

- Follow the Hippocratic Oath: First, do no harm
- Make it simple and easy to use
- Make it robust under normal expected usage
- Price of solution should be reasonable
- Don't hamstring your customers and make things so complicated that even you can't manage them—this leads to interminable service calls
- Combine data security as part of overall better system performance—can you do this?

# Conclusions

- User data security becoming an ever larger problem as storage devices proliferate and more content is stored in more places
- Security can be provided by erasure of data files, entire drive or by destruction of the drive
- Security can also be provided by encryption in the storage device or during transport
- Forms of data security in use today such as DRM and passwords work poorly
- Can data security be part of a positive rather than a negative message?
- New security features such as encryption in the drive or during data transport may be better but not if they compromise system performance
- Data security that is tied to authorized users using biometrics or perhaps idiosyncratic usage patterns of users could be much more effective
- A challenge to the data security industry—can better security add to system performance rather than detract from it



*Thank  
you!*