



Encryption: The Good, the Bad, the Commonly Forgotten

Tom Bowers, Managing Director
Security Constructs, LLC

June 26, 2007

Introduction

- Business drivers
- Potential points of protection
- Encryption methods
- Managing the project
- Choosing a product
- Keys

Business Drivers

- **Business**

- Data Loss
- Outsourcing
- Mobile work force
- Maintain competitive advantage



- **Regulations**

- Privacy
- PCI
- FFIEC
- FERPA

Potential Data Leakage Points

- Laptops
- Portable storage
 - USB
 - CD / DVD
 - MP3
 - Cell phones / cameras
- Databases



Encryption Methods Overview

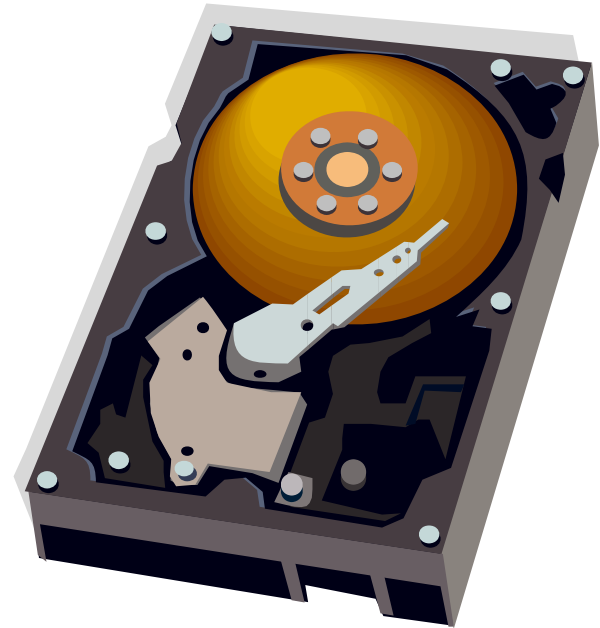
- Hard drive
 - Software
 - Hardware
- Trusted platform module (TPM)
- Digital rights management (DRM)
- Mobile methods

Hard Drive – Software Methods

- Policy server
- Client software component
- Integrated with USB or smart Card
- Hidden costs
 - Software is relatively inexpensive
 - Deployment costs – integrating encryption into business processes
 - Help desk costs - Is it the application / hard drive or is it the encryption?
 - Crashed hard drive recovery costs
 - Key recovery – more on this later
 - Companies have scaled back or stopped deployments because of these hidden costs

Hard Drive – Hardware Methods

- Fixed
 - Desktop methods - \$\$\$
 - PCMCIA - \$\$\$
- Portable
 - USB
 - Usually hardware key



Trusted Platform Module (TPM)

- All business class PCs - free
- Requires free client from PC vendor
- Integrates with biometrics
- Partial disk encryption only
- VERY secure
- U.S. courts following this technology closely
- Only one 3rd party central policy server available

Digital Rights Management (DRM)

- Encrypts the content (data) only
- Protection travels with the data
- New metadata controls
- Central policy server
- Requires client software
- Author determines rights
- Costs
 - Training (end user, administrator...)
 - Helpdesk
 - Business process mapping / integration

Mobile Products

- Software only
- Central policy server
- Application or platform specific
- Cross platform
- Portable encryption
- Challenges
 - Point solutions
 - Market inconsistency
 - Portable solutions around for a long time
 - Application solutions immature
 - Lose control of content after decryption



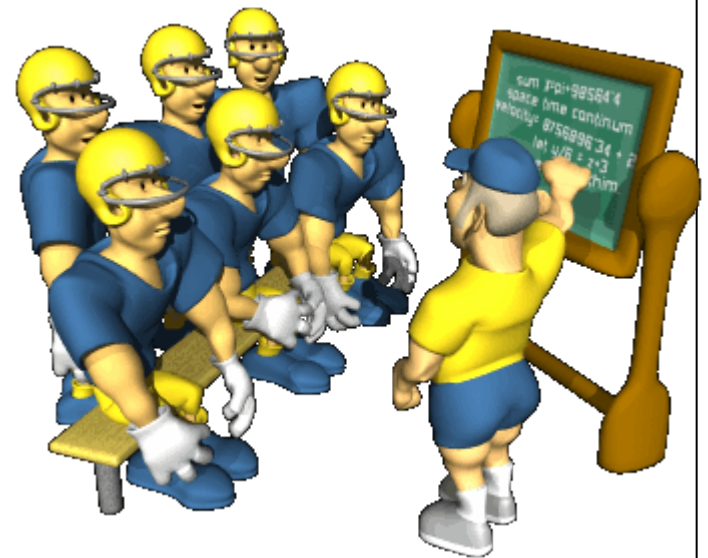
Keys

- Varies greatly by vendor
- **Greatest obstacle to encryption deployments**
- Types (Public/Private, Proprietary)
- Key management
- Key backup
- Key recovery
 - Employee quits
 - Administrator quits
 - Corrupted key
 - How fast can this be done



Managing the Project

- Team selection
 - Business unit(s) requesting encryption
 - Regulatory staff if requesting encryption
 - Help desk
 - Training
 - IT staff
- Choose encryption type
- Product testing
- Vendor selection
- Deployment
 - By business unit / process
 - By leakage point
 - Global



Choosing an Effective Solution

- What are you protecting?
- Have you had a breach recently?
- Where / how is your data flowing?
 - Outsourcing
 - Remote users
 - Mobile work force
- Usability / security
- Infrastructure capability
- Costs
 - Software
 - High availability / failover
 - Backup solution
 - Deployment
 - Administration



Conclusions

- While regulations may be the largest push, business concerns are also a cause for growth
- Wide range of leakage points to protect
- Full disk, partial, mobile devices or combinations
- Choosing a product should be a business decision -- not IT alone
- Key management is the greatest headache

Tom.bowers@securityconstructs.com

