

Protecting Sensitive Information

Fred Kerby

NSWCDD Information Assurance
Manager



Roadmap (a work in progress)

- n Background
- n Current Situation
- n Way Ahead

Sensitive Information

- n Information that, when disclosed to unauthorized persons, may cause damage or harm to the organization and or its associated personnel. Sensitive information is not likely to be releasable under the terms of the Freedom of Information Act (FOIA).
- n Typical examples of unclassified sensitive information include and are not limited to: For Official Use Only (FOUO), information protected by the Privacy Act of 1974 (as amended), personally identifiable information (PII), and information related to technical and/or administrative programs.

Protection Envelope

- n Cyber Protection
 - n Individual accounts w/password
 - n Patches
 - n Network Firewall
 - n Network Intrusion Detection System
- n Physical Protection
 - n Buildings locked after hours
 - n Offices locked after hours
- n Loss of either or both mandates additional countermeasures (encryption)



Pushing the envelope

- n Travel
- n Telework
- n Outsourced IT

Not too distant history

- n ComputerWorld article (August 2006)
 - n 81% of US firms lost laptops w/sensitive info last year
 - n Handhelds; laptops; followed by USB memory sticks, desktops, and servers
 - n No way to determine what was actually lost
- n Laptop Hall of Shame (September 2006)
 - n Veteran's Affairs
 - n Several others mentioned

Might we have a problem?

- n Google "laptop loss"
 - n 660,000 hits in 0.18 seconds
- n SANS Newsbites
- n End of life computers in your organization?

Situation summary

- n Need to label (identify) all media
 - n Data ownership
 - n Sensitivity level?
- n Need to manage amount of sensitive data stored
 - n Volume (quantity)
 - n Duration (time)
- n Need to encrypt sensitive data
 - n Data outside your physical control at greatest risk



The Way Ahead



Awareness

- n Balancing Risk and Benefit
 - n Low hanging fruit
 - n Due Diligence
- n Operational Security (OPSEC)
- n Liability
- n Reputation



Policy

- n Labeling

- n IT owned or leased by your organization
- n All removable media

- n Protection

- n Minimize the amount of stored sensitive information commensurate with mission and operational requirements
- n Sensitive information must be protected when transmitted and stored
- n Stored encrypted data must be recoverable by authorized persons
- n Info must be erased prior to reassigning asset
- n Loss must be reported to cognizant person



Labels

- n DOD SF (700 series) available in e-mail
- n Understand the problem you are trying to solve...
- n Apply to all 'things' processing info that belongs to the organization



Minimizing stored info

- n Find
- n Erase
 - n Delete
 - n Empty Recycle Bin
 - n Overwrite free space

Protection

n Transmission

- n Downloading web pages
- n Sending email messages
- n Removable / transportable media
 - n USB drives, PDAs, laptops

n Storage

- n Hard disk on computer
- n Removable media

Physical security necessary, but not sufficient

Cryptography 101

- n Symmetric
 - n Shared keys
 - n WinZIP; TrueCrypt / TCexplorer
- n Asymmetric
 - n Public/private key pair
 - n PGP; CAC



Encrypting email

- n Outlook and Exchange have support for some PKI solutions (e.g., CAC)
- n OK to encrypt attachments only if message doesn't need encryption
- n Publish your certificate in the GAL



File / Disk Encryption

- n EFS
- n WinZIP
- n TrueCrypt / TCexplorer
- n Others

Recovering Encrypted Data

- n Asymmetric
 - n Key recovery available from CA
 - n Export and protect EFS certificate
- n Symmetric
 - n Escrow pass phrase (key) with line manager
 - n Write on opaque card
 - n Place in labeled envelope, seal, and sign
 - n Place envelope in lockable container
 - n PasswordSafe

Erasing Data prior to re-use

- n Examples
 - n Transferring computer to another user
 - n Disposing of computer (end of life)
- n Overwrite entire disk (DBAN)

Reporting Information Loss

- n Security for your organization
- n Your Supervisor
- n Organizational Missing / Lost / Stolen / Damaged report



Recap

- n Technology has changed – has protection?
- n What are your organization's risk vectors?
- n What can you do to make a difference?
 - n Policy
 - n Tools such as WinZIP and TrueCrypt / TCexplorer
 - n PasswordSafe

Questions?