Privacy and Mobile Security

Eric McMillen, CISSP CISM CISA

The McMillen Group, LLC

August 2006

Introduction

- Eric McMillen, CISSP CISM CISA
- The McMillen Group, LLC
  - Security Assessments
  - Penetration Testing
  - Compliance Assistance
  - Security Awareness Education

Session Objectives

- Discuss the security and privacy issues involving data on mobile devices.
- Present you with potential risk management approaches

Laptop Theft Fun Facts

- 10% of laptops will be stolen within the first 12 months of purchase.
- 90% are never recovered.
- 49% of companies have had laptops stolen with the last 12 months.
- 57% of corporate crimes are linked to stolen laptops.
- 73% of companies had no specific security policies for their laptops in 2003.

The Problem

- Identity Theft
  - Roughly 88 Million Americans Exposed since 2/2005
  - 25% of all “reported breaches” involved missing laptops
- Security Breach Notification Laws
  - 32 States since 2003
  - Most based upon California SB 1386

3 Phases of Mobile Data Security

- Planning
- Protection
- Response and Recovery

Planning Phase

- Planning Phase has Three Steps
  - Data Classification
  - Risk Assessment
  - Mobile Data Policy

Data Classification

- Not All Data is Created Equal
- Data Classification
  - What are you trying to protect?
  - What are you protecting it from?
  - What are the regulatory requirements to consider?
- Minimum of Three Classifications
  - Public
  - Internal Use Only
  - Sensitive

Compliance Related Data

Data Requiring Compliance Related Protection

Ordinary Personal Data

Data that is identifiable to an individual person but is not generally considered "Sensitive"

1. Name
2. Telephone # (work & home)
3. A ddress (work & home)
4. E-mail address (work and home)
5. Gender
6. Marital status
7. Number of children
8. Date of birth or age
9. Citizenship
10. Education
11. Income Range
12. Non-medical benefits information
13. Purchase history
14. Buying patterns
15. Hobbies and interests

Sensitive Personal Data

Data that is (1) identifiable to an individual person and (2) has the potential to be used to harm or embarrass the data subject.

16. Social Security Numbers
17. National ID Numbers
18. Driver's license number
19. Credit Card numbers
20. Account numbers
21. Passwords, including PINs*
22. Criminal arrests or convictions
23. Judgments in civil cases
24. Medical information
25. Administrative sanctions
26. Race, ethnicity, national origin
27. Data concerning sexual orientation or activity
28. Financial data (such as credit rating)
29. Salary & Compensation
30. Disability status

Risk Assessment Process

- Key Questions in the Process
  - What could happen?
  - If it happened, how bad could it be?
  - What can be done?
  - How much will it cost?
  - Is it cost-effective?

Establish a Policy

- 7 Items a Good Policy Should Contain
  - Objective
  - Scope
  - Risk Assessment
  - Security Measures
  - Notification Process
  - Enforcement
  - Employee Sign-off

Protection Phase

- 5 Essential Aspects to Protect Mobile Data
  - Physical Security
  - Authentication
  - Encryption
  - Backup
  - Education

Physical Security

- Easiest to implement - Most often ignored.
- Minimum Physical Security Guidelines
  - Don’t take data out of the office unnecessarily.
  - Maintain positive control of your laptop.
  - Utilize laptop locking cables.
  - Keep laptops out of sight when not in use.
  - Don’t leave your laptop in the backseat.
  - Attach ID Tags or engrave your firm information on your laptops.
  - Use a laptop bag that doesn’t look like one and place a conspicuously colored luggage tag on it.

Authentication

- Types of Authentication
  - Something You Know
  - Something You Have
  - Something You Are
- The Problem with Passwords
- Two Factor Authentication Products
  - SecuriKey (http://www.securikey.com/)
  - PointSec (http://www.pointsec.com)
  - Various built-in biometric devices

Encryption

- Whole Disk Encryption vs.. Targeted Encryption
- Issues
  - Cipher Strength
  - Key Management
  - Bad Pass Phases
  - Performance
- Products
  - PGP (http://www.pgp.com)
  - Credant Mobile Guardian (http://www.credant.com/)
  - PointSec Media Encryption (http://www.pointsec.com/)

Backup

- Don’t Take Your Only Copy of the Data
- Backup Encryption Keys
- Help Identify What Information May Be Accessible.
- Get Staff Back to a Productive State.

Education

- Using it is different then installing it.
- Sample Curriculum
  - Contents of the Mobile Security Policy
  - Why the Policy is necessary
  - Best Practices to follow
  - How to handle an Incident

Response and Recovery

- Incident Response
- Breach Notification
- Laptop Tracking Technology
- Poison Pill Technology

Incident Response

- Written Incident Response Plan
  - Team members
  - Escalation Process
  - Action / Reaction Steps
    - What Data was Impacted
    - Assess Relevant Legal Requirements
    - Necessary Notification
  - Post-Mortem

Breach Notification

- Determine who to notify
- Timing of a breach notice
  - In general, notify as soon as reasonably possible
  - Possible delays for law enforcement investigations
- Required Channels for communicating

Breach Notification Cont'd

- Content of breach notice communication
  - Date & details of the incident
  - Remedial actions taken
  - A toll-free number for further information, if possible
  - How to protect against the possibility of ID theft
  - Contact information for major credit reporting agencies
  - Consider adding other helpful & pertinent information
- Consider posting additional information on your website
  - FTC or other government resources
  - Consumer-focused ID theft resources

Tracking Technology

- Benefits
  - Reduce Internal Theft
  - Relatively Low Cost
- Tracking Myths
  - Thief will connect to the Internet right away
  - High Recovery Rate
- Tracking Products
  - CyberAngel (http://www.sentryinc.com/)
  - CompuTracePlus (http://www.absolute.com/)

“Poison Pill” Technology

- The Laptop “Fail Safe” Solution
- Trigger Mechanisms
  - Remote
  - Check-in Timer
- Often bundled with other products.

Questions??

Thank You!

Contact Information

Eric McMillen, CISSP CISM CISA
The McMillen Group, LLC
http://www.mcmillengroup.com
emcmillen@mcmillengroup.com
Phone:214.329.9730
Mobile: 214.663.1563
Fax: 866.375.6006